行列式の冪の展開，Alon-Tarsi 予想の一般化，超行列式

行列式の冪の展開, Alon–Tarsi 予想の一般化, 超行列式

鹿児島大学大学院 理工学研究科
数理情報科学専攻
下吉　仁平

2020 年 1 月 31 日

序文

本論文では行列式の冪, つまり $(\det X)^m$ の展開係数について論じる. Glynn は「m が素数 p を用いて $m = p - 1$ と表せるとき, この展開係数に 0 は現れない」ということを示した. 本論文では実はこの逆もなりたつことを明らかにする.

Glynn の結果からは Alon–Tarsi 予想という未解決問題が特別な場合に解決される. 実際には Glynn の結果は, より一般的な正則二部グラフの完全マッチングへの分割の個数についての定理を証明したことになる. 本論文の結果から, このグラフに関する定理はその逆もなりたつことが明らかになる.

行列式の冪の展開とその係数

まず本論文の主定理, つまり行列式の冪の展開係数に関する定理を述べよう.

$n \times n$ 行列 $X = (x_{ij})_{1 \le i,j \le n}$ に対して, 行列式の冪 $(\det X)^m$ は次の形に展開できる. この展開に現れる係数 C_L に注目する.

$$(\det X)^m = \sum_{L \in \Psi(m)} C_L x^L.$$

ただし, $\Psi(m)$ は各行, 各列の和が m となる非負整数成分の $n \times n$ 行列全体を表す. また $L = (l_{ij})_{1 \le i,j \le n}$ に対して x^L を次のように定める.

$$x^L = \prod_{1 \le i,j \le n} x_{ij}^{l_{ij}}.$$

展開係数 C_L に関する次の定理が本論文の主定理である.

定理 I (主定理)**.** $n \ge 3$ のとき, 自然数 m に関する次の 2 つの条件は同値である.

(1) ある素数 p が存在して, $m = p - 1$.
(2) 任意の $L \in \Psi(m)$ に対して, $C_L \neq 0$.

以下,「ある素数 p が存在して $m = p-1$」を単に「$m = p-1$」とかく. また「$m = p-1$ をみたす素数 p が存在しない」を単に「$m \neq p - 1$」とかく.

Glynn の超行列式

主定理の (1) $\Rightarrow$ (2) がなりたつことは Glynn が超行列式を用いて示した.

行列式は行列に対して定まる値だが, 超行列式は 1 次元以上の超行列に対して定義される行列式の類似物である（超行列とは 0 次元的, 1 次元的, 2 次元的, 3 次元的, ... に数を並べた行列の一般化である）.

Glynn は正標数 p の体上の可換代数 $\mathbb{A}$ の元を成分とする超行列に対し超行列式を定めた. 以下, この Glynn の超行列式を $\det_p$ とかく.

通常の行列（つまり 2 次元の超行列）A に対して超行列式 $\det_p A$ を考えるとどうなるのだろうか？実は $\det_p A$ は行列式 $\det A$ の $p-1$ 乗と等しい.

定理 II. $\mathbb{A}$ 上の $n \times n$ 行列 A に対して次の等式がなりたつ.

$$\det_p A = (\det A)^{p-1}.$$

また $\det_p A$ は次のように展開できる.

定理 III. $\mathbb{A}$ 上の $n \times n$ 行列 A に対して, $\det_p A$ は次のように表せる.

$$\det_p A = \sum_{L \in \Psi(p-1)} \frac{(-1)^n}{L!} a^L.$$

ただし, $L = (l_{ij})_{1 \le i,j \le n}$ に対して $L! = \prod_{1 \le i,j \le n} l_{ij}!$ と定める.

この定理は一般の次元の超行列に拡張できる（定理 3.0.1）. 定理 II と定理 III から $(\det A)^{p-1}$ の展開がわかる. これから任意の $L \in \Psi(p-1)$ に対して次がなりたつ.

$$L! C_L \equiv (-1)^n \pmod{p}.$$

とくに $C_L \neq 0$ がなりたつので主定理の (1) $\Rightarrow$ (2) が導かれたことになる.

注意. 主定理の (1) $\Rightarrow$ (2) は, 現在は超行列式を用いない証明もある [K2]（[K1] も参照のこと）.

$C_L = 0$ をみたす L が存在するのはどんな m か

$m = p-1$ のとき任意の $L \in \Psi(m)$ に対して $C_L \neq 0$ であることがわかったが, 逆に $m \neq p-1$ の場合は $C_L = 0$ をみたす $L \in \Psi(m)$ は常に存在する（つまり, 主定理の (2) $\Rightarrow$ (1) がなりたつ）. これは本論文で初めて明らかにすることである.

この事実は $n = 3$ のときが本質的であり, $C_L = 0$ となる $L \in \Psi(m)$ は次のように具体

的に与えられる.

$$L = L^{ab}(3) = \begin{pmatrix} ab+b-1 & a & 1 \\ a & ab & b \\ 1 & b & ab+a-1 \end{pmatrix}.$$

ただし, a, b は $m+1 = (a+1)(b+1)$ をみたす自然数である ($m+1$ は合成数だからこのような a, b は存在する). この L に対し, 実際に $C_L = 0$ となることは多項係数の計算ですぐわかる（行列式を Sarrus の公式で与えてやればあとは高校レベルの計算）.

$n \geq 4$ のとき $C_L = 0$ をみたす $L \in \Psi(m)$ は $L^{ab}(3)$ を用いて簡単に構成できる（詳しくは第 5 章）.

この発見に至った経緯も記しておく. 「$m = p-1$ のとき, 任意の $L \in \Psi(m)$ に対して $C_L \neq 0$」という Glynn の主張を読んで $m \neq p-1$ のときはどうなるかが気になり, 計算機実験を行った（具体的には $n = 3, m \leq 68$ の計算をした）. $m = p-1$ が単なる十分条件ではなく必要条件でもあることは初めから予想していたわけでなく. この計算機実験を通じてその可能性に気づかされた. 一旦予想してみると, その証明は案外楽だった.

正則二部グラフの完全マッチングへの分割に関する問題

展開係数 C_L が 0 か否かという問題は, 正則二部グラフの完全マッチングへの分割に関する問題と自然に同一視できる.

このグラフの問題を説明する. $\Psi(m)$ の各元は m-正則二部グラフと自然に同一視できる. ただし, 本論文では多重グラフ（2 つの頂点間に複数の辺がありうるグラフ）を単にグラフとよぶことにする.

$L \in \Psi(m)$ に対して, n 文字の置換 $\sigma_1, \ldots, \sigma_m$ が $L = P_{\sigma_1} + \cdots + P_{\sigma_m}$ をみたすとき $\Sigma = (\sigma_1, \ldots, \sigma_m)$ を L の置換行列への分割（以下, 単に L の分割）とよぶ. ただし, P_σ は置換 σ に対応する置換行列である. この L の分割は m-正則二部グラフの完全マッチングへの分割と自然に同一視できる. L の分割 Σ の符号, つまり偶奇を $\operatorname{sgn}\Sigma = \operatorname{sgn}\sigma_1 \cdots \operatorname{sgn}\sigma_m$ と定める. また L の偶分割全体を $\mathrm{EP}(L)$, 奇分割全体を $\mathrm{OP}(L)$ と表す. これらの集合の大きさ $|\mathrm{EP}(L)|$ と $|\mathrm{OP}(L)|$ が等しいか否かという問題を考えよう. 言い換えると m-正則二部グラフの完全マッチングへの分割で偶分割のものと奇分割のものの個数を比較することになる. $|\mathrm{EP}(L)|$ と $|\mathrm{OP}(L)|$ の差は展開係数 C_L と等しい, つまり

$$|\mathrm{EP}(L)| - |\mathrm{OP}(L)| = C_L$$

となる. よって, このグラフの問題は C_L が 0 か否かを考えることと同値である. Glynn

は主定理の (1) ⇒ (2) を示すことで, このグラフの問題に関する次のような定理を与えたことになる.

定理 IV. $m = p - 1$ のとき, 任意の $L \in \Psi(m)$ に対して, $|\mathrm{EP}(L)| \neq |\mathrm{OP}(L)|$.

また本論文では主定理の (2) ⇒ (1) の証明を与えるが, これはこの定理の裏, つまり次の定理を示したことになる.

定理 V. $m \neq p - 1$ のとき, ある $L \in \Psi(m)$ が存在して, $|\mathrm{EP}(L)| = |\mathrm{OP}(L)|$.

Alon–Tarsi 予想

このグラフの問題は Alon–Tarsi 予想という未解決問題の自然な一般化とみなせる.

Alon–Tarsi 予想はラテン方陣の個数についての予想である. n 次ラテン方陣とは各行, 各列に 1 から n の自然数が 1 回ずつ現れる $n \times n$ 行列のことである. n 次ラテン方陣はすべての成分が 1 である正方行列 $L'(n) = (1)_{1 \leq i,j \leq n} \in \Psi(n)$ の分割と自然に同一視できる. ラテン方陣の符号をそれに対応する $L'(n)$ の分割の符号と定める. 以下, n 次の偶ラテン方陣全体を $\mathrm{ELS}(n)$, 奇ラテン方陣全体を $\mathrm{OLS}(n)$ とかく. これらの個数の比較に関する次の予想は Alon–Tarsi 予想とよばれている [AT].

予想 VI (Alon–Tarsi 予想)**.** n が偶数のとき, $|\mathrm{ELS}(n)| \neq |\mathrm{OLS}(n)|$.

なお, n が 3 以上の奇数のとき $|\mathrm{ELS}(n)| = |\mathrm{OLS}(n)|$ であることは比較的やさしい.

偶ラテン方陣の個数と奇ラテン方陣の個数はそれぞれ

$$|\mathrm{ELS}(n)| = |\mathrm{EP}(L'(n))|, \quad |\mathrm{OLS}(n)| = |\mathrm{OP}(L'(n))|$$

と表せるので, 先ほどのグラフの問題は Alon–Tarsi 予想の一般化とみなせる. $|\mathrm{ELS}(n)|$ と $|\mathrm{OLS}(n)|$ の差は展開係数 $C_{L'(n)}$ と等しいから Alon–Tarsi 予想は「自然数 n が偶数のとき $C_{L'(n)} \neq 0$」という予想と同値である. 定理 IV から Glynn は $n = p - 1$ の場合の Alon–Tarsi 予想を解決したことになる [G2].

実際は定理を得た経緯は逆であり, この Glynn の Alon–Tarsi 予想に関する結果がまずあり, これを本論文でまとめ直したのが定理 IV である. つまり [G2] の証明は主定理の (1) ⇒ (2) が鍵であり, これを素直に読むとラテン方陣というよりグラフの話と解釈するのが自然だという認識にいたり, 定理 IV という形にまとめ直したのである. そして, このグラフの話としては本論文で示した (2) ⇒ (1) は定理 V という形に言い換えられるので

ある.

注意. 今定めたラテン方陣の符号は印符号とよばれるものであり, 通常採用されるラテン方陣の符号とは異なる. しかし, Alon–Tarsi 予想を考える上でこの違いは問題にならない. なぜなら, この 2 つの符号は n のみで決まるスカラー倍の違いしかないためである（詳しくは第 7 章）.

各章について

第 1 章から第 4 章で超行列式に関する Glynn の結果 [G1] をまとめる. 具体的には通常の行列における超行列式と通常の行列式との関係（定理 II）, 超行列式の展開公式（定理 III）, 超行列式の積公式についてまとめる. 第 4 章では超行列式の積公式について扱うが, これは本論文の主題である行列式の冪の展開係数とは論理的に関係はなく, 読まなくても他の章を読む際に支障はない. しかし, Glynn の超行列式が積を保つという性質は興味深かったためここでまとめる.

第 5 章では主定理（定理 I）について, つまり $(\det X)^m$ の展開係数が 0 を含まないための m の条件（$m = p - 1$）について論じる. この十分性は第 3 章までの Glynn の議論からわかる. また必要性は本論文ではじめて示すことである.

第 6 章では, 第 5 章の定理を正則二部グラフの完全マッチングへの分割に関する定理（定理 IV, 定理 V）に翻訳する. Glynn はラテン方陣に関する Alon–Tarsi 予想の部分的解決をした [G2] が, このグラフについての定理はその一般化とみなせる.

第 7 章では, ラテン方陣の符号に関する補足説明をする.

謝辞

最後に, 伊藤稔先生は学部 4 年生から 3 年間, 非常に熱心に丁寧にご指導してくださいました. 心より感謝申し上げます. また, 学部, 大学院を通してご指導してくださった数理情報科学科の先生方, 苦楽を共にした同期の皆様にも感謝の意を表します.

目次

1　超行列式

通常の行列は 2 次元的に数が並んでいるが, これを一般の次元に拡張した超行列を考える. 通常の行列には行列式が定まるが, 実は超行列にも同じような概念がある. それが超行列式である. 様々な研究者が様々な超行列式を定義してきたが, 本論文では [G1] で Glynn が定めた超行列式を考える.

1.1　超行列と超行列式

この節では超行列と超行列式を説明しよう.

通常の行列は平面的に数が並んでいる. 立体的に数が並んだ「3 次元行列」や絵には描けないが 4 次元的に数が並んだものを考えてもよさそうである. このように 0 次元的, 1 次元的, 2 次元的, 3 次元的, ... に数が並んだ「行列」を超行列と よぶ. 以下, n は自然数, r は非負整数とし, R は可換環とする.

定義 1.1.1. $[n]^r$ から R への写像を R 上の n^r 超行列とよぶ. ただし, $[n]$ は n 以下の自然数全体とする. 以下, n^r 超行列を単に n^r 行列や r 次元行列とよぶ. また R 上の r 次元行列全体を $\mathrm{Mat}(n^r, R)$ とかく.

以下, $(i_1, \ldots, i_r) \mapsto a_{i_1 \cdots i_r}$ という対応で決まる n^r 超行列を次のようにかく.

$$(a_{i_1 \cdots i_r})_{1 \leq i_1, \ldots, i_r \leq n}.$$

超行列同士の積を通常の行列同士の積と同様に次のように定める.

定義 1.1.2. R 上の r 次元行列 $A = (a_{i_1 \cdots i_r})_{1 \leq i_1, \ldots, i_r \leq n}$ と s 次元行列 $B = (b_{j_1 \cdots j_s})_{1 \leq j_1, \ldots, j_s \leq n}$ に対して, それらの積 AB を次のように定める.

$$AB = \left(\sum_{1 \leq k \leq n} a_{i_1 \ldots i_{r-1} k} b_{k j_2 \ldots j_s} \right)_{1 \leq i_1, \ldots, i_{r-1}, j_2, \ldots, j_s \leq n}.$$

ただし, r, s は自然数である. このとき, AB は $r + s - 2$ 次元行列である.

注意 1.1.3. 通常の行列では正方行列以外にも 3×5 行列などのように長方形の行列を考えることがある. 超行列でも $3 \times 5 \times 7$ という型のように各辺の長さが異なるものを考えることが可能であり, 一定の条件がなりたてば積も考えられる. ただし, 本論文では定義 1.1.1 で定めたようにすべての辺の長さが同じもののみを考える.

通常の行列に行列式が考えられるのと同様に, 超行列にも行列式のような概念がある. これを超行列式という. 超行列式を定義するためにいくつか記号を用意しよう.

定義 1.1.4. R 上の n^1 行列 $A = (a_i)_{1\leq i\leq n}$ に対して, $\widetilde{A}$ を次のように定義する.

$$\widetilde{A} = a_1 a_2 \cdots a_n.$$

$t_1, \ldots, t_n$ という n 個の不定元を成分とする n^1 行列 $t = (t_i)_{1\leq i\leq n}$ を考える. またこの n 個の不定元の R 係数の多項式環 $R[t_1, \ldots, t_n]$ を $R[t]$ と表す.

定義 1.1.5. 自然数 k と $f(t) \in R[t]$ に対して, $\langle f(t)\rangle_k$ を次のように定義する.

$$\langle f(t)\rangle_k = \text{「}f(t) \text{ における } \prod_{1\leq i\leq n} t_i^k \text{ の係数」}.$$

これらの記号を用いて超行列式を定義しよう. ただし, 正標数の体上の可換代数の元を成分とする超行列のみに超行列式が定まる. 以下, $\mathbb{F}$ を正標数 p の体とし, $\mathbb{A}$ は $\mathbb{F}$ 上の可換代数 [M] とする.

定義 1.1.6. r を自然数とする. $\mathbb{A}$ 上の n^r 行列 A に対して, A の超行列式を次のように帰納的に定義する.

$$\det_p A = \begin{cases} \widetilde{A}^{p-1} & (r = 1) \\ \langle \det_p(At)\rangle_{p-1} & (r \geq 2). \end{cases}$$

つまり, r 次元行列 A に対して, $\det_p A$ は $r-1$ 次元行列 At の超行列式 $\det_p(At)$ における $\prod_{1\leq i\leq n} t_i^{p-1}$ の係数である.

1.2 例

簡単な行列に対して, 超行列式を具体的に計算してみよう.

まず $r = 2$, つまり通常の行列に対する超行列式をいくつか計算しよう.

例 1.2.1. $p = 3$ のとき, 次の $A \in \mathrm{Mat}(2^2, \mathbb{A})$ の超行列式を計算しよう.

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

定義 1.1.6 を適用すると

$$\det_3 A = \langle \det_3(At)\rangle_{3-1} = \langle \widetilde{At}^2 \rangle_2$$

である. $\widetilde{At}^2$ は展開すると次のようになる.

$$\begin{aligned}\widetilde{At}^2 &= \{(at_1+bt_2)(ct_1+dt_2)\}^2 \\ &= a^2c^2t_1^4 + (2a^2cd+2abc^2)t_1^3t_2 \\ &\quad + (a^2d^2+4abcd+b^2c^2)t_1^2t_2^2 + (2abd^2+2b^2cd)t_1t_2^3 + b^2c^2t_2^4.\end{aligned}$$

この $\widetilde{At}^2$ における $t_1^2t_2^2$ の係数が $\det_3 A$ である. つまり

$$\det_3 A = a^2d^2+4abcd+b^2c^2 = a^2d^2+abcd+b^2c^2$$

がなりたつ. また $p=5$ のときの $\det_5 A$ も同様に計算できる.

$$\begin{aligned}\det_5 A &= a^4d^4+16a^3bcd^3+36a^2b^2c^2d^2+16ab^3c^3d+b^4c^4 \\ &= a^4d^4+a^3bcd^3+a^2b^2c^2d^2+ab^3c^3d+b^4c^4.\end{aligned}$$

これらの結果から $\det_3 A = (\det A)^2$, $\det_5 A = (\det A)^4$ であることがわかる. 実は一般の p で 2 次元行列 A に対して, $\det_p A = (\det A)^{p-1}$ がなりたつ. この事実は第 2 章で示す.

次に $r=3$, つまり 3 次元行列の超行列式を $n=2$ のときに計算しよう.

例 1.2.2. $p=3$ のとき, 次の $A \in \mathrm{Mat}(2^3, \mathbb{A})$ の超行列式を計算しよう.

$$A = (a_{ijk})_{1\le i,j,k\le 2}.$$

定義 1.1.6 を適用すると

$$\det_3 A = \langle \det_3(At) \rangle_2$$

である. At は次のようにな 2 次元行列になる.

$$At = \begin{pmatrix} a_{111}t_1+a_{112}t_2 & a_{121}t_1+a_{122}t_2 \\ a_{211}t_1+a_{212}t_2 & a_{221}t_1+a_{222}t_2 \end{pmatrix}.$$

例 1.2.1 の結果から $\det_3 At$ は次のように表せる.

$$\begin{aligned}\det_3(At) &= (a_{111}t_1+a_{112}t_2)^2(a_{221}t_1+a_{222}t_2)^2 \\ &\quad + (a_{111}t_1+a_{112}t_2)(a_{121}t_1+a_{122}t_2)(a_{211}t_1+a_{212}t_2)(a_{221}t_1+a_{222}t_2) \\ &\quad + (a_{121}t_1+a_{122}t_2)^2(a_{211}t_1+a_{212}t_2)^2.\end{aligned}$$

この $\det_3(At)$ における $t_1^2 t_2^2$ の係数が $\det_3 A$ である．つまり

$$\begin{aligned}
\det_3 A = {} & (a_{111}^2 a_{222}^2 + 4a_{111}a_{112}a_{221}a_{222} + a_{112}^2 a_{221}^2) \\
& + (a_{111}a_{121}a_{212}a_{222} + a_{111}a_{122}a_{211}a_{222} + a_{111}a_{122}a_{212}a_{221} \\
& + a_{112}a_{121}a_{212}a_{222} + a_{112}a_{122}a_{211}a_{222} + a_{112}a_{122}a_{212}a_{221}) \\
& + (a_{121}^2 a_{212}^2 + 4a_{121}a_{122}a_{211}a_{212} + a_{122}^2 a_{211}^2) \\
= {} & a_{111}^2 a_{222}^2 + a_{112}^2 a_{221}^2 + a_{121}^2 a_{212}^2 + a_{122}^2 a_{211}^2 \\
& + a_{111}a_{112}a_{221}a_{222} + a_{111}a_{121}a_{212}a_{222} + a_{111}a_{122}a_{211}a_{222} + a_{111}a_{122}a_{212}a_{221} \\
& + a_{112}a_{121}a_{212}a_{222} + a_{112}a_{122}a_{211}a_{222} + a_{112}a_{122}a_{212}a_{221} + a_{121}a_{122}a_{211}a_{212}
\end{aligned}$$

がなりたつ．

1.3 超行列式の歴史

ここまで Glynn の超行列式について述べてきたが, Glynn 以外の研究者も超行列に対して定義できる超行列式を考えていた．この節ではそのような超行列式に関する歴史を振り返る．なお, この節の内容は, [N] で述べられていた [C], [S], [GKZ] に関する内容と Glynn の超行列式に関する内容 [G1] をまとめたものである．

最初に 1845 年に Cayley が $2 \times 2 \times 2 = 2^3$ 行列に対して超行列式を定義した [C]. Cayley はその後一般化を試みたが成功しなかった．次に 1852 年に Schläfli が 2^4 行列に超行列式を定義した [S]. 以降, 約 150 年ものあいだ超行列式の研究に大きな進展はなかったようだ．1994 年, ついに Gelfand, Kapranov, Zelevinsky が Cayley, Schläfli の超行列式を一般化した [GKZ]．しかし, その数年後の 1997 年に Glynn がこの系列とはちがう超行列式を発見した [G1]．ただし, 正標数のときにしか考えられない．これこそが本論文で扱う今回の超行列式だ．

これらの超行列式の中で Glynn の超行列式だけが積を保つという特徴を持つ．この特徴は第 4 章で示される．

2　通常の行列に対する超行列式

超行列式は超行列に対して定義したわけだが, 通常の行列（2 次元行列）も超行列の一種なので超行列式が考えられる. それは一体どんな値になるだろうか. 実は $\mathbb{A}$ の元を成分とする 2 次元行列 A に対して $\mathrm{det}_p\, A = (\det A)^{p-1}$ がなりたつ. これは主定理の $(1) \Rightarrow (2)$ を示すための鍵の 1 つである. もう 1 つの鍵である超行列式の展開公式は第 3 章で述べる.

この等式は実質的に位数 p の有限体 $\mathbb{F}_p$ 上の主張だが, これをまず $\mathbb{F}_p$ の代数閉包 $\bar{\mathbb{F}}$ 上の主張に帰着させ, それをさらに標数 p の任意の有限体 $\mathbb{F}_q$ 上の主張に帰着させて証明する. 具体的にはまず $\bar{\mathbb{F}}$ 上で det_p と $\det$ の零点集合が一致するという主張に帰着させる. さらにこれらの零点集合が $\mathbb{F}_q$ 上でも一致するという主張に帰着させる. そして, この主張は $\mathbb{F}_q$ 上の射影空間における $\widetilde{At}$ の零点の個数を数えることで示される. $\bar{\mathbb{F}}$ 上ではこのような零点の個数は無限個になってしまうが, $\mathbb{F}_q$ 上なら有限の値となり, このような個数の議論に帰着できるのである.

2.1　正標数の体

本題に入る前に正標数の体に関する記号や性質を説明する. 以下, この章では p を素数とする.

位数 p の有限体を $\mathbb{F}_p$ と表す. またその代数閉包を $\bar{\mathbb{F}}$ と表す. 標数 p の有限体に関して次の定理がなりたつ [Y].

定理 2.1.1. 標数 p の有限体の位数は p の冪である. 逆に任意の p の冪 $q = p^i$ に対して位数 q の有限体は存在し, 同型を除いてただ 1 つに決まる. またこの位数 q の体は $\bar{\mathbb{F}}$ のある部分体と同型である（以下, この $\bar{\mathbb{F}}$ の位数 q の部分体を $\mathbb{F}_q$ とかく）. $\bar{\mathbb{F}}$ は次のように表せる.

$$\bar{\mathbb{F}} = \bigcup_{i=1}^{\infty} \mathbb{F}_{p^i}.$$

以下, この章でのみ $\mathbf{1}$, $\mathbf{0}$ をそれぞれ $\mathbb{F}_p$ の単位元, 零元とする. 前の章に引き続き $\mathbb{F}$ は標数 p の体, $\mathbb{A}$ は $\mathbb{F}$ 上の可換代数とする. $\mathbb{F}_p$ は $\mathbb{F}$ の素体だから $\mathbf{1}$, $\mathbf{0}$ はそれぞれ $\mathbb{F}$ の単位元, 零元とみなせる.

注意 2.1.2. 上で述べたように, この章では有限体上の射影空間において元の個数を数えることが鍵となる. そのため非負整数と有限体の元が同時に現れる. どちらの元かわかり

やすくするために, この第 2 章では $\mathbb{F}_p$ の単位元, 零元を意図的に $\mathbf{1}$, $\mathbf{0}$ とかく.

2.2 $\det_p A = (\det A)^{p-1}$

超行列式は超行列に対して定まるが, ここからは通常の行列（2 次元行列）の超行列式について考えてみよう. 実は例 1.2.1 で述べたようにこれは行列式の $p-1$ 乗となる.

定理 2.2.1. $A \in \mathrm{Mat}(n^2, \mathbb{A})$ に対して次の等式がなりたつ.

$$\det_p A = (\det A)^{p-1}.$$

以降, この章ではこの定理を証明する. まずこの節ではその方針を述べる.

この定理を示すには実際は $\mathbb{F}_p$ 係数の多項式環における次の定理を示せばよい.

定理 2.2.2. 不定元を成分とする行列 X に対して次の等式がなりたつ.

$$\det_p X = (\det X)^{p-1}.$$

ここで X は x_{ij}（ただし, $1 \leq i, j \leq n$）という n^2 個の不定元を成分とする n^2 行列 $X = (x_{ij})_{1 \leq i,j \leq n}$ とする. ただし, この不定元は $\mathbb{F}_p$ 係数の多項式とみなす（$\mathbb{F}_p$ は $\mathbb{F}$ の素体だから $\mathbb{F}$ 係数の多項式ともみなせる）. この n^2 個の不定元の $\mathbb{F}$ 係数の多項式環 $\mathbb{F}[x_{11}, x_{12}, \ldots, x_{nn}]$ を $\mathbb{F}[X]$ とかく. よって, X は $\mathrm{Mat}(n^2, \mathbb{F}[X])$ の元とみなせる.

定理 2.2.2 の x_{ij} に A の (i, j) 成分を代入すれば定理 2.2.1 を得る（つまり定理 2.2.2 から定理 2.2.1 が得られる）.

以下, この章の残りで定理 2.2.2 を示す. 具体的には次のような手順で示す.

$$\text{定理 2.2.5} \Rightarrow \text{定理 2.2.4} \Rightarrow \text{定理 2.2.3} \Rightarrow \text{定理 2.2.2}.$$

定理 2.2.3, 定理 2.2.4, 定理 2.2.5 は次のような定理である.

定理 2.2.3. $\bar{\mathbb{F}}[X]$ において次のイデアルの包含関係がなりたつ.

$$(\det X) \subset \sqrt{(\det_p X)}.$$

定理 2.2.4. $A \in \mathrm{Mat}(n^2, \bar{\mathbb{F}})$ に対して次がなりたつ.

$$\det A = \mathbf{0} \iff \det_p A = \mathbf{0}.$$

定理 2.2.5. 任意の p の冪 q と $A \in \mathrm{Mat}(n^2, \mathbb{F}_q)$ に対して次がなりたつ.

$$\det A = \mathbf{0} \iff \det_p A = \mathbf{0}.$$

この定理 2.2.3 に現れる記号は 2.3 節で説明する.

定理 2.2.5 から定理 2.2.2 が導かれる流れをもう少し詳しく説明する. まず $\mathbb{F}_q$ 上の主張である定理 2.2.5 から $\bar{\mathbb{F}}$ 上の主張である定理 2.2.4 が導かれる. これは定理 2.2.5 に定理 2.1.1（つまり $\bar{\mathbb{F}} = \bigcup_{i=1}^{\infty} \mathbb{F}_{p^i}$）を適用することですぐにわかる. 次に定理 2.2.4 から定理 2.2.3 を導く. これは定理 2.2.4 に Hilbert の零点定理を適用して証明することになる（詳しくは 2.4 節）. さらに定理 2.2.3 から定理 2.2.2 を導く. この証明では行列式の既約性, 次数, 係数の比較が鍵となる（詳しくは 2.5 節）.

よって, 定理 2.2.2 は定理 2.2.5 に帰着されたわけだが, この定理 2.2.5 は 2.6 節から 2.8 節で示すことになる. この定理 2.2.5 の証明では斉次多項式 $\widetilde{At}$ の射影空間における零点の個数に関する議論を経由する. 具体的には次の 4 つの条件の同値性を示すことになる.

$$\begin{aligned} \det_p A = \mathbf{0} &\Leftrightarrow |\bar{N}(\widetilde{At})| \equiv 0 \pmod{p} \\ &\Leftrightarrow |N(\widetilde{At})| \equiv 1 \pmod{p} \\ &\Leftrightarrow \det A = \mathbf{0}. \end{aligned}$$

ただし, $N(\widetilde{At})$ は斉次多項式 $\widetilde{At}$ の射影空間における零点集合であり, $\bar{N}(\widetilde{At})$ はこの $N(\widetilde{At})$ の射影空間における補集合である（詳しくは 2.6 節）. 第 2 の同値性は 2.6 節で証明する. また第 1 と第 3 の同値性はそれぞれ 2.7 節と 2.8 節で証明する.

本論文におけるこの定理 2.2.5 の証明は, 大まかな流れは [G1] と [FM] による証明を参考にしつつ, 詳細部分は独自に与えたものである. この定理は [G1] で初めて証明が与えられ, [FM] でも [G1] の解説という形で証明が述べられている. しかし, [G1] の証明は 13 行のみ, [FM] の証明も 17 行のみで, どちらも理解できなかった. ただ, [G1] では

$$|N(\widetilde{At})| \equiv 1 \pmod{p}$$

という条件を経由していること, [FM] では包除原理（Inclusion–Exclusion Principle [SV]）が鍵を握っていることは読み取れた. これらの鍵を手掛かりに証明を構築したのが本論文の証明である. 2.6 節から 2.8 節まで約 11 ページかけて証明することになる.

このように定理 2.2.1（実質的に定理 2.2.2）は $\mathbb{F}_p$ における主張なのに, その証明は $\mathbb{F}_p$ の代数閉包 $\bar{\mathbb{F}}$ における主張に帰着させ, さらにそれを標数 p の任意の有限体 $\mathbb{F}_q$ における主張に帰着させる. そして, この $\mathbb{F}_q$ における主張は $\mathbb{F}_q$ 上の射影空間で $\widetilde{At}$ の零点の個数を数えることで示される. 有限体だからこそ個数が数えられるのである. 有限体 $\mathbb{F}_p$ の話が一度無限体 $\bar{\mathbb{F}}$ の話に帰着され, それが再び有限体 $\mathbb{F}_q$ の話に戻って証明されることになるのはおもしろい.

2.3 Hilbert の零点定理

まずこの節では定理 2.2.3 の証明の際に鍵となる Hilbert の零点定理（正確には [CLO] でいうところの強形の零点定理）を説明しよう.

定理 2.3.1 (Hilbert の零点定理)**.** $\mathbb{K}$ が代数閉体のとき, 多項式環 $\mathbb{K}[x] = \mathbb{K}[x_1, \ldots, x_n]$ のイデアル I に対して次がなりたつ.

$$\mathbf{I}(V(I)) = \sqrt{I}.$$

ただし, 本論文ではこの定理の証明は省略する.

ここからは Hilbert の定理に現れた記号の説明をしよう. まず $\sqrt{I}$ を次で定める (この $\sqrt{I}$ を I の根基という). 以下, $\mathbb{K}$ を代数閉体とは限らない一般の体とする. また $\mathbb{K}$ の零元を $\mathbf{0}$ とかく. さらに $f(x) = f(x_1, \ldots, x_n)$ をしばしば f とかく.

定義 2.3.2. $\mathbb{K}[x]$ のイデアル I に対して, $\mathbb{K}[x]$ の部分集合 $\sqrt{I}$ を次のように定義する.

$$\sqrt{I} = \{f \in \mathbb{K}[x] \mid \text{ある } m \in \mathbb{N} \text{ が存在して}, f^m \in I\}.$$

この $\sqrt{I}$ はイデアルである.

命題 2.3.3. $\mathbb{K}[x]$ のイデアル I に対して, $\sqrt{I}$ は $\mathbb{K}[x]$ のイデアルである.

証明. $\mathbf{0} \in \sqrt{I}$ は明らか.

まず $\sqrt{I}$ が和について閉じていることを示す. $f, g \in \sqrt{I}$ とする. つまり, ある $s, t \in \mathbb{N}$ が存在して, $f^s, g^t \in I$ である. $(f+g)^{s+t}$ を二項展開すると各項は $f^s \in I$ または $g^t \in I$ で割り切れるので $(f+g)^{s+t} \in I$, すなわち $f + g \in \sqrt{I}$ である.

次に $f \in \sqrt{I}, h \in \mathbb{K}[x]$ とし, $hf \in \sqrt{I}$ であることを示す（これは $-f \in \sqrt{I}$ であることも主張している）. $f \in \sqrt{I}$ よりある $s \in \mathbb{N}$ が存在して, $f^s \in I$ がなりたつ. $f^s \in I$ だから $(hf)^s = h^s f^s \in I$ である. したがって, $hf \in \sqrt{I}$ がなりたつ.

以上より $\sqrt{I}$ は $\mathbb{K}[x]$ のイデアルである. □

次に $V(f)$ は f の零点集合を表す.

定義 2.3.4. $f \in \mathbb{K}[x]$ に対し, $\mathbb{K}^n$ の部分集合 $V(f)$ を次のように定義する.

$$V(f) = V_{\mathbb{K}}(f) = \{b \in \mathbb{K}^n \mid f(b) = \mathbf{0}\}.$$

また $\mathbb{K}[x]$ の部分集合 J に対し, $\mathbb{K}^n$ の部分集合 $V(J)$ を次のように定義する.

$$V(J) = V_{\mathbb{K}}(J) = \{b \in \mathbb{K}^n \mid \text{任意の } f \in J \text{ に対して}, f(b) = \mathbf{0}\}.$$

これらの記号に関して次の等式がなりたつ.

命題 2.3.5. $f \in \mathbb{K}[x]$ に対し, $V((f)) = V(f)$ がなりたつ. ただし, $f \in \mathbb{K}[x]$ に対して (f) は f から生成される単項イデアルを表す. つまり $(f) = \{gf \mid g \in \mathbb{K}[x]\}$ と定める.

証明. $V((f)) \subset V(f)$ は明らか. だから, $V((f)) \supset V(f)$ を示す. $b \in V(f)$ とする. あとは $g \in (f)$ に対して, $g(b) = \mathbf{0}$ であることを示せばよい. $b \in V(f)$ より $f(b) = \mathbf{0}$ がなりたつ. また $g \in (f)$ よりある $h \in \mathbb{K}[x]$ が存在して, $g = hf$ がなりたつ. したがって, $g(b) = h(b)f(b) = \mathbf{0}$ である. □

最後に $\mathbf{I}(V)$ は V の元を零点とする多項式のなすイデアルである.

定義 2.3.6. $\mathbb{K}^n$ の部分集合 V に対して, $\mathbb{K}[x]$ のイデアル $\mathbf{I}(V)$ を次のように定義する.

$$\mathbf{I}(V) = \{f \in \mathbb{K}[x] \mid \text{任意の } b \in V \text{ に対して}, f(b) = \mathbf{0}\}.$$

この $\mathbf{I}(V)$ が $\mathbb{K}[x]$ のイデアルであることはすぐわかる. このイデアルついて次の包含関係がなりたつ.

命題 2.3.7. $f \in \mathbb{K}[x]$ に対して次がなりたつ.

$$(f) \subset \mathbf{I}(V(f)).$$

証明. $g \in (f)$ とする. つまり, ある $h \in \mathbb{K}[x]$ が存在して, この g は $g = hf$ をみたす. したがって, 任意の $b \in V(f)$ に対して, $g(b) = h(b)f(b) = \mathbf{0}$ である. よって, $g \in \mathbf{I}(V(f))$ である. □

以上で Hilbert の零点定理に現れた記号を説明した.

2.4 イデアル $(\det X)$ と $(\det_p X)$ の関係

この節では定理 2.2.4 が成立すれば定理 2.2.3, つまり $\bar{\mathbb{F}}[X]$ において次のイデアルの関係がなりたつことを示そう.

$$(\det X) \subset \sqrt{(\det_p X)}.$$

以下, とくに断りがなければイデアル (f) や $I(V)$ は $\bar{\mathbb{F}}[X]$ において考える.

まず定理 2.2.4 は次のように言い換えられる.

補題 2.4.1. 次の等式がなりたつ.

$$V_{\bar{\mathbb{F}}}(\det X) = V_{\bar{\mathbb{F}}}(\det_p X).$$

この補題を用いて定理 2.2.3 を示す.

定理 2.2.3 の証明. $\bar{\mathbb{F}}[X]$ において次のイデアルの関係がなりたつ.

$$(\det X) \subset \mathbf{I}(V_{\bar{\mathbb{F}}}(\det X)) = \mathbf{I}(V_{\bar{\mathbb{F}}}(\det_p X)) = \sqrt{(\det_p X)}.$$

最初の包含関係は命題 2.3.7 から成立. 次の等号は補題 2.4.1 からわかる. 最後の等号は命題 2.3.5 に注意すれば, $\bar{\mathbb{F}}$ が代数閉体であることと Hilbert の零点定理からわかる. □

2.5 イデアルの関係からの $\det_p X = (\det X)^{p-1}$ の導出

この節では定理 2.2.3 から定理 2.2.2, つまり

$$\det_p X = (\det X)^{p-1}$$

がなりたつことを証明しよう. この証明の鍵は次の 4 つの補題と行列式の既約性である. [G1] ではこの 4 つの補題と定理 2.2.5 から定理 2.2.2 を導いているようであるが, 行列式の既約性 [GW] については触れておらず, よく理屈が理解できない箇所がある. ここでは行列式の既約性を使って独自の説明を与えた.

$\det X$ に関する次の 2 つの補題はすぐわかる.

補題 2.5.1. $\det X$ は n 次斉次多項式である.

補題 2.5.2. $(\det X)^{p-1}$ の $\prod_{1\leq i\leq n} x_{ii}^{p-1}$ における係数は **1** である.

次に $\det_p X$ に関する次の 2 つの補題は例 1.2.1 と同じような計算をすればわかる.

補題 2.5.3. $\det_p X$ は $n(p-1)$ 次斉次多項式である.

補題 2.5.4. $\det_p X$ の $\prod_{1\leq i\leq n} x_{ii}^{p-1}$ における係数は **1** である.

次に通常の行列式が既約多項式であることを示す [GW].

命題 2.5.5. $\det X$ は既約多項式.

証明. $\det X$ が $g(X), h(X) \in \bar{\mathbb{F}}[X]$ を用いて次のように表せるとする.

$$\det X = g(X)h(X).$$

以下, $g(X)$ のある項に x_{11} が含まれると仮定して, $h(X) = \mathbf{1}$ であることを示す. 仮定より $h(X)$ に x_{11} を含む項が存在しないので, x_{1j}, x_{j1} $(2 \leq j \leq n)$ を含む項も存在しない. これより $h(X)$ には x_{ii} $(2 \leq i \leq n)$ を含む項が存在しないので, x_{ij}, x_{ji} $(i+1 \leq j \leq n)$ も存在しない. 以上で $h(X)$ は x_{ij} $(1 \leq i, j \leq n)$ を含む項が存在しないので $h(X) = \mathbf{1}$ である. □

これらの準備の下, 定理 2.2.3 から定理 2.2.2 が導ける.

定理 2.2.2 の証明. $\bar{\mathbb{F}}$ において $\det X \in (\det X)$ だから定理 2.2.3 から $\det X \in \sqrt{(\det_p X)}$ が成立する. したがって, ある $k \in \mathbb{N}$ と $f(X) \in \bar{\mathbb{F}}[X]$ が存在して,

$$(\det X)^k = f(X) \det_p X$$

がなりたつ. ここで $\det X \in \bar{\mathbb{F}}[X]$ は既約多項式 [GW] だからある $l \in \mathbb{Z}_{\geq 0}$ と $b \in \bar{\mathbb{F}} \setminus \{\mathbf{0}\}$ が存在して,

$$\det_p X = b(\det X)^l$$

がなりたつ. 補題 2.5.1 より $\det X$ は n 次斉次多項式であり, 補題 2.5.3 より $\det_p X$ は $n(p-1)$ 次斉次多項式だから $l = p-1$ である. また補題 2.5.2, 補題 2.5.4 より $\det_p X$, $(\det X)^{p-1}$ の $\prod_{1 \leq i \leq n} x_{ii}^{p-1}$ における係数はともに $\mathbf{1}$ だから $b = \mathbf{1}$ である. したがって, $\det_p X = (\det X)^{p-1}$ である. □

以上で定理 2.2.3 から定理 2.2.2 を導いた. ただし, 定理 2.2.3 は定理 2.2.4 から導かれたが, その定理 2.2.4 を導く際に使った定理 2.2.5 はまだ示していない. これはこの章の残りで示すことになる

2.6 斉次多項式の射影空間における零点集合

この章の残り（2.6 節から 2.8 節）で定理 2.2.5, つまり $A \in \mathrm{Mat}(n^2, \mathbb{F}_q)$ に対して次の等式が成立することを証明しよう.

$$\det A = \mathbf{0} \Leftrightarrow \det_p A = \mathbf{0}.$$

以下, この章の終わりまで $q = p^h$ とし, $\mathbb{F}_q$ を単に $\mathbb{F}$ と表す. 2.2 節でも述べたが, この証明は斉次多項式 $\widetilde{At}$ の射影空間における零点の個数に関する議論を経由する. 具体的には次の 3 つの定理を示せばよい. ここからこの章の終わりまで A を $\mathrm{Mat}(n^2, \mathbb{F})$ の元とし, $H_A = H_A(t) = \widetilde{At}$ とする.

定理 2.6.1. 次がなりたつ.

$$\det_p A = \mathbf{0} \Leftrightarrow |\bar{N}(H_A)| \equiv 0 \pmod{p}.$$

定理 2.6.2. 次がなりたつ.

$$|\bar{N}(H_A)| \equiv 0 \pmod{p} \Leftrightarrow |N(H_A)| \equiv 1 \pmod{p}.$$

定理 2.6.3. 次がなりたつ.

$$|N(H_A)| \equiv 1 \pmod{p} \Leftrightarrow \det A = \mathbf{0}.$$

ただし, $N(H_A)$ は斉次多項式 H_A の射影空間における零点集合であり, $\bar{N}(H_A)$ はこの $N(H_A)$ の射影空間における補集合である.

この節ではこの斉次多項式の射影空間における零点集合を説明した上で定理 2.6.2 を証明する. 残りの定理 2.6.1 と定理 2.6.3 の証明はそれぞれ 2.7 節と 2.8 節で与える.

最初に射影空間の説明をしよう [Y]. 以下, n は自然数とし, $\mathbb{F}^\times = \mathbb{F} \setminus \{\mathbf{0}\}$ と定める. また, ここからこの節の終わりまで $\mathbf{0}$ は $\mathbb{F}^n$ の零ベクトルとする.

定義 2.6.4. $n-1$ 次射影空間 $\mathbb{F}P_{n-1}$ を次で定める.

$$\mathbb{F}P_{n-1} = (\mathbb{F}^n \setminus \{\mathbf{0}\})/\sim.$$

ただし, $\mathbb{F}^n$ 上の同値関係を次で定める.

$$b \sim c \underset{\text{def}}{\Longleftrightarrow} \text{ある } d \in \mathbb{F}^\times \text{ が存在して, } b = dc.$$

$\mathbb{F}^n$ の零ベクトル $\mathbf{0}$ が属する同値類は $\{\mathbf{0}\}$ だから, これは $\mathbb{F}^n \setminus \{\mathbf{0}\}$ 上の同値関係ともみなせる.

まず $\mathbb{F}P_{n-1}$ の大きさを見ておこう.

命題 2.6.5. $\mathbb{F}P_{n-1}$ の大きさは

$$|\mathbb{F}P_{n-1}| = 1 + q + \cdots + q^{n-1}$$

である. とくに $|\mathbb{F}P_{n-1}| \equiv 1 \pmod{p}$ である.

証明. この命題は次の等式からわかる.

$$|\mathbb{F}P_{n-1}| = \frac{|\mathbb{F}^n \setminus \{\mathbf{0}\}|}{q-1} = \frac{q^n - 1}{q-1} = 1 + q + \cdots + q^{n-1}. \qquad \square$$

$\mathbb{F}^\times$-閉な $\mathbb{F}^n$ の部分集合は $\mathbb{F}P_{n-1}$ の部分集合に自然に対応する. ただし, $\mathbb{F}^\times = \mathbb{F} \setminus \{\mathbf{0}\}$ とし, $W \subset \mathbb{F}^n$ が $\mathbb{F}^\times$ の元の積で閉じているとき W を $\mathbb{F}^\times$-閉な集合とよぶ.

定義 2.6.6. $\mathbb{F}^\times$-閉な集合 $W \subset \mathbb{F}^n$ に対して, $\mathbb{F}P_{n-1}$ の部分集合 $W^\dagger$ を次で定める.

$$W^\dagger = (W \setminus \{\mathbf{0}\})/\sim.$$

この記号を用いると $\mathbb{F}P_{n-1}$ は $\mathbb{F}P_{n-1} = (\mathbb{F}^n)^\dagger$ と表せる. W に対し $W^\dagger$ を対応させる写像が和集合や共通部分, 補集合をとる操作を保つことはすぐわかる.

命題 2.6.7. $\mathbb{F}^\times$-閉な集合 $W, W' \subset \mathbb{F}^n$ に対して, 次の等式がなりたつ.

$$(W \cup W')^\dagger = W^\dagger \cup W'^\dagger, \quad (W \cap W')^\dagger = W^\dagger \cap W'^\dagger, \quad \overline{W^\dagger} = \bar{W}^\dagger.$$

ただし, $\bar{W}$ は W の $\mathbb{F}^n$ における補集合, $\overline{W^\dagger}$ は $W^\dagger$ の $\mathbb{F}P_{n-1}$ における補集合である.

$\mathbb{F}^n$ の m 次元部分空間 W に対する $W^\dagger$ の大きさは次のとおりである（もちろん W は $\mathbb{F}^\times$-閉な集合である）. このことは W が $\mathbb{F}^m$ と線型同型であることからわかる.

命題 2.6.8. $\mathbb{F}^n$ の m 次元部分空間 W に対して,

$$|W^\dagger| = 1 + q + \cdots + q^{m-1}$$

がなりたつ. とくに p を法として

$$|W^\dagger| \equiv \begin{cases} 0 & (m = 0) \\ 1 & (m \geq 1) \end{cases}$$

である.

また $\mathbb{F}^\times$-閉な集合 W が零ベクトルを含まないとき, $|W|$ と $|W^\dagger|$ に次の関係があることはすぐわかる.

命題 2.6.9. $\mathbb{F}^\times$-閉な集合 $W \subset \mathbb{F}^n \setminus \{\mathbf{0}\}$ に対して次の等式がなりたつ.

$$|W| = (q-1)|W^\dagger|.$$

ここからは斉次多項式 H の $\mathbb{F}P_{n-1}$ における零点集合 $N(H)$ を定義する. 以下, H は $\mathbb{F}^n$ 上の m 次斉次多項式とする. H は $\mathbb{F}P_{n-1} \sqcup \{\{\mathbf{0}\}\}$ から $\mathbb{F}P_{n-1} \sqcup \{\{\mathbf{0}\}\}$ への写像とみなせる.

定義 2.6.10. $Z \in \mathbb{F}P_{n-1}$ としたとき, $H(Z)$ を次で定める.

$$H(Z) = \mathrm{cl}(H(z)).$$

ただし, z は Z の元であり, $\mathrm{cl}(H(z))$ は $H(z)$ の属する同値類である. また $H(\{\mathbf{0}\}) = \mathrm{cl}(H(\mathbf{0}))$ とする.

この $H(Z)$ は $z \in Z$ の選び方によらず一意に定まる（つまりこの定義は well defined である）. つまり, $Z \in \mathbb{F}P_{n-1}$ としたとき

$$z_1, z_2 \in Z \Longrightarrow H(z_1) \sim H(z_2)$$

がなりたつ. 実際ある $c \in \mathbb{F} \setminus \{\mathbf{0}\}$ が存在して, $z_1 = cz_2$ がなりたつので,

$$H(z_1) = H(cz_2) = c^m H(z_2).$$

よって, $H(z_1) \sim H(z_2)$ である.

$H(Z) = \{\mathbf{0}\}$ をみたす $Z \in \mathbb{F}P_{n-1}$ を H の射影空間における零点とよぼう. これらを集めたのが $N(H)$ である.

定義 2.6.11. $\mathbb{F}P_{n-1}$ の部分集合 $N(H)$ を次で定める.

$$N(H) = \{Z \in \mathbb{F}P_{n-1} \mid H(Z) = \{\mathbf{0}\}\}.$$

また $N(H)$ の $\mathbb{F}P_{n-1}$ における補集合を $\bar{N}(H)$ と表す.

定理 2.6.2 は次の等式からわかる（ここで最後の合同は命題 2.6.5 の主張）.

$$|\bar{N}(H)| + |N(H)| = |\mathbb{F}P_{n-1}| \equiv 1 \pmod{p}.$$

2.7 $\det_p A$ と $\bar{N}(H_A)$

この節では定理 2.6.1, つまり次がなりたつことを示そう.

$$\det_p A = \mathbf{0} \Leftrightarrow |\bar{N}(H_A)| \equiv 0 \pmod{p}.$$

これを示すには次の定理 2.7.1 を示せばよい.

定理 2.7.1. 次がなりたつ.

$$|\bar{N}(H_A)|\mathbf{1} = (-1)^{n+1}(\det_p A)^{1+p+\cdots+p^{h-1}}.$$

ここで h は 2.6 節で述べたように $q = p^h$ をみたすものである. この定理の証明は [G1] で述べられているが, 本論文ではこれを次の 3 つの命題に分けて示す.

命題 2.7.2. 次の等式がなりたつ.

$$-|\bar{N}(H_A)|\mathbf{1} = \sum_{z \in \mathbb{F}^n} H_A(z)^{q-1}.$$

命題 2.7.3. 次の等式がなりたつ.

$$\sum_{z \in \mathbb{F}^n} H_A(z)^{q-1} = (-1)^n \langle H_A^{q-1} \rangle_{q-1}.$$

命題 2.7.4. 次の等式がなりたつ.

$$\langle H_A^{q-1} \rangle_{q-1} = (\det_p A)^{1+p+\cdots+p^{h-1}}.$$

最初に命題 2.7.2 を示そう. 証明の土台は $\mathbb{F}^\times = \mathbb{F} \setminus \{\mathbf{0}\}$ が巡回群となるという事実である [KN].

命題 2.7.5. $\mathbb{F}^\times$ は $q-1$ 次巡回群である.

この命題から次の補題はすぐわかる.

補題 2.7.6. $a \in \mathbb{F}$ に対して, 次がなりたつ.

$$a^{q-1} = \begin{cases} \mathbf{0} & (a = \mathbf{0}) \\ \mathbf{1} & (a \neq \mathbf{0}). \end{cases}$$

とくに $i \equiv 0 \pmod{q-1}$ のとき次がなりたつ.

$$a^i = \begin{cases} \mathbf{0} & (a = \mathbf{0}) \\ \mathbf{1} & (a \neq \mathbf{0}). \end{cases}$$

よって $\mathbb{F}^n$ 上の斉次多項式 H に対して $H(z)^{q-1}$ は $\overline{V(H)}$ の特性関数となる. ただし, 2.3 節で定めたように $V(H)$ は H の $\mathbb{F}^n$ における零点集合と定める.

系 2.7.7. 次がなりたつ.

$$H(z)^{q-1} = \begin{cases} \mathbf{0} & (z \in V(H)) \\ \mathbf{1} & (z \notin V(H)). \end{cases}$$

$\mathbb{F}P_{n-1}$ における零点集合 $N(H)$ は $\mathbb{F}^n$ における零点集合 $V(H)$ を用いて次のように表せる.

補題 2.7.8. 次の等式がなりたつ.

$$N(H) = V(H)^{\dagger}.$$

証明. まず $N(H) \subset V(H)^{\dagger}$ を示す. $Z \in N(H)$ として $Z \in V(H)^{\dagger}$ を示す. ここで $Z = \mathrm{cl}(z)$（ただし, $z \in Z$）とする. $Z \in N(H)$ より $H(z) = \mathbf{0}$ である. したがって, $z \in V(H)$ だから $Z = \mathrm{cl}(z) \in V(H)^{\dagger}$ がなりたつ.

$V(H)^{\dagger} \subset N(H)$ も同様に示せる. □

以上の事実から命題 2.7.2 が導かれる.

命題 2.7.2 の証明. この証明は次の計算からわかる.

$$\begin{aligned}
\sum_{z \in \mathbb{F}^n} H_A(z)^{q-1} &= |\overline{V(H_A)}|\mathbf{1} \\
&= ((q-1)|\overline{V(H_A)}^{\dagger}|)\mathbf{1} \\
&= ((q-1)|\overline{V(H_A)^{\dagger}}|)\mathbf{1} \\
&= ((q-1)|\bar{N}(H_A)|)\mathbf{1} \\
&= -|\bar{N}(H_A)|\mathbf{1}.
\end{aligned}$$

ここでまず第 1 の等号は系 2.7.7 からわかる. 次に第 2 の等号は命題 2.6.9 からなりたつ. 第 3 の等号は命題 2.6.7 から成立. また第 4 の等号は命題 2.7.8 からなりたつ. 最後に第 5 の等号は $\mathbb{F}$ の標数が p であることからわかる. □

次に命題 2.7.3 の証明を考えるが, 次の補題を用いる.

補題 2.7.9. $K = (k_1, \ldots, k_n) \in \mathbb{Z}_{\geq 0}$ に対して, 次の等式がなりたつ.

$$\sum_{z \in \mathbb{F}^n} z^K = \begin{cases} (-\mathbf{1})^n & (k_1 \equiv \cdots \equiv k_n \equiv 0 \pmod{q-1}) \\ \mathbf{0} & (\text{それ以外}). \end{cases}$$

ただし, z^K は多重指数の記号で表している. つまり, $z = (z_1, \ldots, z_n)$ に対し

$$z^K = z_1^{k_1} \cdots z_n^{k_n}$$

である.

この補題は次の等式からすぐわかる.

補題 2.7.10. 自然数 i に対して, 次がなりたつ.

$$\sum_{a\in\mathbb{F}} a^i = \begin{cases} -\mathbf{1} & (i \equiv 0 \pmod{q-1}) \\ \mathbf{0} & (\text{その他}). \end{cases}$$

証明. 最初に $i \equiv 0 \pmod{q-1}$ のとき, 次の等式がなりたつ.

$$\sum_{a\in\mathbb{F}} a^i = \mathbf{0} + \sum_{a\in\mathbb{F}\setminus\{\mathbf{0}\}} \mathbf{1} = (q-1)\mathbf{1} = -\mathbf{1}.$$

ここでまず第 1 の等号は補題 2.7.6 からわかる. また第 3 の等号は $\mathbb{F}$ の標数が p であることからわかる.

次に $i \not\equiv 0 \pmod{q-1}$ の場合を考える. c を $q-1$ 次の巡回群 $\mathbb{F}^\times$ の生成元としたとき,

$$\sum_{a\in\mathbb{F}} a^i = \sum_{a\in\mathbb{F}} (ca)^i = c^i \sum_{a\in\mathbb{F}} a^i$$

がなりたつ. ここで第 1 の等号は $a \mapsto ca$ という対応が $\mathbb{F}$ から $\mathbb{F}$ への全単射であることからわかる. $c^i \neq \mathbf{1}$ だからこの等式から $\sum_{a\in\mathbb{F}} a^i = \mathbf{0}$ がわかる. □

以上の準備の下で命題 2.7.3 を示す.

命題 2.7.3 の証明. 以下, $K \in \mathbb{Z}^n_{\geq 0}$ に対して, $H_A(t)^{q-1}$ における t^K の係数を E_K と表す. ここで $t = (t_i)_{1\leq i\leq n}$ は 1.1 節で述べたように $t_1, \ldots, t_n$ という n 個の不定元を成分とする 1 次元行列である. とくに $E_{(q-1,\ldots,q-1)} = \langle H_A^{q-1} \rangle_{q-1}$ がなりたつ. また和が $n(q-1)$ となる $\mathbb{Z}^n_{\geq 0}$ の元全体を ψ とかく. つまり,

$$\psi = \{(k_1, \ldots, k_n) \in \mathbb{Z}^n_{\geq 0} \mid k_1 + k_2 + \cdots + k_n = n(q-1)\}$$

とおく.

$$\begin{aligned} \sum_{z\in\mathbb{F}^n} H_A(z)^{q-1} &= \sum_{z\in\mathbb{F}^n} \sum_{K\in\psi} E_K z^K \\ &= \sum_{K\in\psi} E_K \sum_{z\in\mathbb{F}^n} z^K \\ &= E_{(q-1,\ldots,q-1)} (-\mathbf{1})^n \\ &= \langle H_A^{q-1} \rangle_{q-1} (-\mathbf{1})^n. \end{aligned}$$

ここで第 3 の等号は補題 2.7.9 より $K \in \psi$ に対して

$$\sum_{z\in\mathbb{F}^n} z^K = \begin{cases} (-\mathbf{1})^n & (K = (q-1, \ldots, q-1)) \\ \mathbf{0} & (\text{それ以外}) \end{cases}$$

であることからわかる. □

最後に命題 2.7.4 を示そう. まず多重指数について整理しよう. $\mathbb{Z}^n_{\geq 0}$ における和を次のように定める.

$$(k_1, \ldots, k_n) + (l_1, \ldots, l_n) = (k_1 + l_1, \ldots, k_n + l_n).$$

また $\mathbb{Z}^n_{\geq 0}$ の元の非負整数倍を次のように定める.

$$m(k_1, \ldots, k_n) = (mk_1, \ldots, mk_n).$$

このとき, $K, L \in \mathbb{Z}^n_{\geq 0}$ と $m \in \mathbb{Z}_{\geq 0}$ に対して,

$$t^K t^L = t^{K+L}, \quad (t^K)^m = t^{mK}$$

がなりたつ. 次に和が $n(p-1)$ となる $\mathbb{Z}^n_{\geq 0}$ の元全体を ϕ とかく. つまり,

$$\phi = \{(k_1, \ldots, k_n) \in \mathbb{Z}^n_{\geq 0} \mid k_1 + k_2 + \cdots + k_n = n(p-1)\}$$

と定める. 最後に非負整数 m に対して,

$$\underline{m} = (m, m, \ldots, m)$$

とかく.

次の補題が命題 2.7.4 の証明の鍵となる.

補題 2.7.11. $K_0, K_1, \ldots, K_{h-1} \in \phi$ が

$$p^0 K_0 + p^1 K_1 + \cdots + p^{h-1} K_{h-1} = \underline{q-1}$$

をみたすならば

$$K_0 = K_1 = \cdots = K_{h-1} = \underline{p-1}$$

がなりたつ.

ここで 2.6 節で述べたように h は $q = p^h$ をみたすものである.

証明. まず $K_0 = \underline{p-1}$ を示す. この補題の仮定より K_0 の各成分は p を法として -1 と合同だから, これらの成分は $p-1, 2p-1, 3p-1, \ldots$ のいずれかである. また, $K_0 \in \phi$ だから K_0 の成分の和は $n(p-1)$ となるので, $K_0 = \underline{p-1}$ である.

次に $K_1 = \underline{p-1}$ を示す. この補題の仮定と $K_0 = \underline{p-1}$ より

$$p^1 K_1 + p^2 K_2 + \cdots + p^{h-1} K_{h-1} = \underline{q-p}$$

だから

$$p^0K_1 + p^1K_2 + \cdots + p^{h-2}K_{h-1} = \underline{p^{h-1} - 1}$$

がわかる. したがって, K_1 の各成分は p を法として -1 と合同である. 以下, 同じ手順で $K_1 = \underline{p-1}$ がわかる.

あとは同様の議論で $K_0 = K_1 = \cdots = K_{h-1} = \underline{p-1}$ が示される. □

この補題を用いて命題 2.7.4 の証明をする.

命題 2.7.4 の証明. $H'_A(t) = H_A(t)^{p-1}$ として, $K \in \mathbb{Z}^n_{\geq 0}$ に対して $H'_A(t)$ における t^K の係数を D_K と表す. つまり, D_K は

$$H'_A(t) = H_A(t)^{p-1} = \sum_{K \in \phi} D_K t^K$$

をみたす. とくに $D_{\underline{p-1}} = \langle H'_A(x) \rangle_{p-1} = \det_p A$ がなりたつ. まず $H_A(t)^{q-1}$ について次がなりたつ.

$$\begin{aligned} H_A(t)^{q-1} &= H_A(t)^{(p-1)(1+p+\cdots p^{h-1})} \\ &= (H_A(t)^{p-1})^1 (H_A(t)^{p-1})^{p^1} \cdots (H_A(t)^{p-1})^{p^{h-1}} \\ &= H'_A(t)^1 H'_A(t)^{p^1} \cdots H'_A(t)^{p^{h-1}}. \end{aligned}$$

p^i 乗はフロベニウス写像の合成だから和や積を保つ. よって

$$\begin{aligned} H'_A(t)^{p^i} &= (H_A(t)^{p-1})^{p^i} \\ &= (\sum_{K \in \phi} D_K t^K)^{p^i} \\ &= \sum_{K \in \phi} (D_K t^K)^{p^i} \\ &= \sum_{K \in \phi} D_K^{p^i} t^{p^i K} \end{aligned}$$

がなりたつ. ゆえに, $H_A(t)^{q-1}$ における $\prod_{1 \leq i \leq n} t_i^{q-1}$ の係数, つまり $\langle H_A(t)^{q-1} \rangle_{q-1}$ は

$$\langle H_A(t)^{q-1} \rangle_{q-1} = \sum_{(K_0, K_1, \ldots, K_{h-1}) \in \Phi} D_{K_0}^{p^0} D_{K_1}^{p^1} \cdots D_{K_{h-1}}^{p^{h-1}}$$

と表せる. ただし, Φ を

$$\Phi = \{(K_0, K_1, \ldots, K_{h-1}) \in \phi^h \mid p^0K_0 + p^1K_1 + \cdots + p^{h-1}K_{h-1} = \underline{q-1}\}$$

と定める．この Φ は補題 2.7.11 から $\Phi = \{(\underline{p-1}, \ldots, \underline{p-1})\}$ だから次の等式が導かれる．

$$\begin{aligned}\langle H_A(t)^{q-1}\rangle_{q-1} &= D_{\underline{p-1}}^{p^0} D_{\underline{p-1}}^{p^1} \cdots D_{\underline{p-1}}^{p^{h-1}} \\ &= D_{\underline{p-1}}^{p^0+p^1+\cdots+p^{h-1}} \\ &= \langle H_A(t)^{p-1}\rangle_{p-1}^{p^0+p^1+\cdots+p^{h-1}} \\ &= (\det_p A)^{p^0+p^1+\cdots+p^{h-1}}.\end{aligned}$$

□

以上で命題 2.7.2 と命題 2.7.3 と命題 2.7.4 が示されたので定理 2.7.1 がなりたつ．したがって, 定理 2.6.1 が導かれた．

2.8 $\det A$ と $N(H_A)$

この節では定理 2.6.3, つまり次がなりたつことを示そう．

$$\det A = \mathbf{0} \Leftrightarrow |N(H_A)| \equiv 1 \pmod{p}.$$

$\det A = \mathbf{0} \Leftrightarrow \delta_A = 0$ だから, 定理 2.6.3 を導くには次を示せばよい．

定理 2.8.1. H_A の射影空間における零点の個数について次がなりたつ．

$$|N(H_A)| \equiv 1 + (-1)^n \delta_A \pmod{p}.$$

ただし, δ_A を次で定める．

$$\delta_A = \begin{cases} 0 & (A : \text{非正則}) \\ 1 & (A : \text{正則}). \end{cases}$$

ここからはこの定理を証明する．この証明は [FM] における本論文の定理 2.2.1 の証明を参考にした．[FM] では次の包除原理（Inclusion–Exclusion Principle [SV]）が鍵を握っている．

補題 2.8.2 (包除原理)**.** 集合 $Y_1, \ldots, Y_n$ に対して, 次の等式がなりたつ．

$$|Y_1 \cup \cdots \cup Y_n| = \sum_{1 \le k \le n} (-1)^{k-1} \mathcal{Y}_k.$$

ただし,

$$\mathcal{Y}_k = \sum_{i_1 < \cdots < i_k} |Y_{i_1} \cap \cdots \cap Y_{i_k}|$$

と定める．

定義 2.8.3. $1 \leq i \leq n$ に対して, ベクトル空間 $\mathbb{F}^n$ の部分空間 $W_1, \ldots, W_n$ を次で定める.

$$W_i = \{(z_1, \ldots, z_n) \in \mathbb{F}^n \mid a_{i1}z_1 + \cdots + a_{in}z_n = \mathbf{0}\}.$$

これらに関して次の 2 つの補題がなりたつ.

補題 2.8.4. 次の 2 つの等式がなりたつ.

$$\operatorname{Ker} A = W_1 \cap \cdots \cap W_n, \quad V(H_A) = W_1 \cup \cdots \cup W_n.$$

補題 2.8.5. $k < n$ ならば $1 \leq i_1, \ldots, i_k \leq n$ に対して,

$$\dim(W_{i_1} \cap \cdots \cap W_{i_k}) > 0$$

がなりたつ.

この補題 2.8.4 はすぐわかる. また補題 2.8.5 は W_i の余次元が 0 か 1 のいずれかであることと次の事実からわかる.

注意 2.8.6. V を n 次元ベクトル空間, W, W' を V の部分空間とする. このとき, W' の余次元が 0 か 1 のいずれかのとき,

$$\dim(W \cap W') = \dim W \text{ または } \dim W - 1$$

がなりたつ.

これらの補題を用いて定理 2.8.1 を示す.

定理 2.8.1 の証明. $|N(H_A)|$ は

$$\mathcal{W}_k = \sum_{i_1 < \cdots < i_k} |W_{i_1}^\dagger \cap \cdots \cap W_{i_k}^\dagger|$$

を用いて次のように表せる.

$$\begin{aligned}
|N(H_A)| &= |V(H_A)^\dagger| \\
&= |(W_1 \cup \cdots \cup W_n)^\dagger| \\
&= |W_1^\dagger \cup \cdots \cup W_n^\dagger| \\
&= \sum_{1 \leq k \leq n} (-1)^{k-1} \mathcal{W}_k \\
&= \sum_{1 \leq k \leq n-1} (-1)^{k-1} \mathcal{W}_k + (-1)^{n-1} \mathcal{W}_n.
\end{aligned}$$

ここで第 1 の等号は補題 2.7.8 からわかる．次に第 2 の等号は命題 2.8.4 からわかる．また第 3 の等号は命題 2.6.7 からわかる．そして第 4 の等号は包除原理（補題 2.8.2）である．

第 1 の項と第 2 の項に分けて計算を進めよう．まず第 1 の項は次のように計算できる．

$$\begin{aligned}
\sum_{1\leq k\leq n-1}(-1)^{k-1}\mathcal{W}_k &= \sum_{1\leq k\leq n-1}(-1)^{k-1}\sum_{i_1<\cdots<i_k}|W_{i_1}^\dagger\cap\cdots\cap W_{i_k}^\dagger| \\
&= \sum_{1\leq k\leq n-1}(-1)^{k-1}\sum_{i_1<\cdots<i_k}|(W_{i_1}\cap\cdots\cap W_{i_k})^\dagger| \\
&\equiv \sum_{1\leq k\leq n-1}(-1)^{k-1}\sum_{i_1<\cdots<i_k}1 \\
&= \sum_{1\leq k\leq n-1}(-1)^{k-1}\binom{n}{k} \\
&= 1\binom{n}{0}-\sum_{0\leq k\leq n}(-1)^k\binom{n}{k}+(-1)^n\binom{n}{n} \\
&= 1+(-1)^n.
\end{aligned}$$

ここで第 2 の等号は命題 2.8.4 からわかる．その次の合同は p を法として考えているが, これは命題 2.6.8 と補題 2.8.5 からわかる．最後の等号は

$$\sum_{0\leq k\leq n}(-1)^k\binom{n}{k}=(1-1)^n=0$$

であることからわかる．

また第 2 の項は次のように計算できる．

$$\mathcal{W}_n=|W_1^\dagger\cap\cdots\cap W_n^\dagger|=|(W_1\cap\cdots\cap W_n)^\dagger|=|(\operatorname{Ker}A)^\dagger|\equiv 1-\delta_A.$$

ここで第 2 の等号は命題 2.8.4 からわかる．また第 3 の等号は命題 2.8.4 からわかる．最後の合同は p を法として考えているが, これは命題 2.6.8 と命題 2.8.4 からわかる．

以上で $|N(H_A)|$ は p を法として次のように表せることがわかる．

$$|N(H_A)|\equiv 1+(-1)^{n-1}+(-1)^n(1-\delta_A)=1-(-1)^n\delta_A. \qquad \square$$

以上で定理 2.8.1 が示されたので, 定理 2.6.3 が証明できたことになる．これで定理 2.6.1, 定理 2.6.2, 定理 2.6.3 がすべて示せたので 2.6 節の冒頭で述べたことから定理 2.2.5, つまり $A\in\mathrm{Mat}(n^2,\mathbb{F}_q)$ に対して

$$\det A=\mathbf{0}\Leftrightarrow\det{}_pA=\mathbf{0}$$

が示せたことになる. さらに 2.2 節の内容と合わせると定理 2.2.1, つまり $A \in \mathrm{Mat}(n^2, \mathbb{A})$ に対して

$$\det_p A = (\det A)^{p-1}$$

が導かれたことになる.

3　超行列式の展開

r 次元行列（つまり, n^r 行列）の超行列式は次のように展開される．以下, $\mathbb{A}$ はこれまでと同様に正標数 p の体 $\mathbb{F}$ 上の可換代数である．

定理 3.0.1. r を自然数とする．$\mathbb{A}$ 上の r 次元行列 A に対して, 次の等式がなりたつ．

$$\det_p A = (-1)^n \sum_{L \in \Psi_r(p-1)} a^{(L)}.$$

ただし, $[n]$ は 1 から n の自然数全体の集合, つまり $[n] = \{1, \ldots, n\}$ とし, A は a_λ という n^r 個の不定元を成分とする r 次元行列 $A = (a_\lambda)_{\lambda \in [n]^r}$ とする．また非負整数成分の r 次元行列 $L = (l_\lambda)_{\lambda \in [n]^r}$ に対して $L! = \prod_{\lambda \in [n]^r} l_\lambda!$, そして

$$a^{(L)} = \frac{1}{L!} \prod_{\lambda \in [n]^r} a_\lambda^{l_\lambda}$$

と定める（一種の多重指数の記法）．また $\Psi_r(c)$ についてはあとで詳しく説明するが, $r = 2$ のときは各行, 各列の和が $p-1$ となる非負整数成分の 2 次元行列全体, つまり

$$\Psi_2(c) = \left\{ (l_{ij})_{1 \le i,j \le n} \in \mathrm{Mat}(n^2, \mathbb{Z}_{\ge 0}) \;\middle|\; \begin{array}{l} {}^\forall i \in [n], \sum_{j \in [n]} l_{ij} = c, \\ {}^\forall j \in [n], \sum_{i \in [n]} l_{ij} = c \end{array} \right\}$$

である．$r = 3$ のときは

$$\Psi_3(c) = \left\{ (l_{ijk})_{1 \le i,j,k \le n} \in \mathrm{Mat}(n^3, \mathbb{Z}_{\ge 0}) \;\middle|\; \begin{array}{l} {}^\forall i \in [n], \sum_{j,k \in [n]} l_{ijk} = c, \\ {}^\forall j \in [n], \sum_{i,k \in [n]} l_{ijk} = c, \\ {}^\forall k \in [n], \sum_{j,k \in [n]} l_{ijk} = c \end{array} \right\}$$

である．$r \ge 4$ のときは書き下さないが想像がつくだろう．

この定理 3.0.1（$r = 2$ の場合）と前章の主結果（定理 2.2.1）から行列式の $p-1$ 乗の展開係数に 0 が含まれないことがわかる（詳しくは第 5 章）．

定理 3.0.1 の証明は, [G1] では r に関する帰納法で証明されている（約 2 ページ）．しかし, 式変形で理解できないところがあり, 自分で理解できる形に説明を改めたのが本論文の証明である．3.2 節では, 約 4 ページかけて証明の準備をする．具体的には $\mathrm{Mat}(n^r, \mathbb{Z}_{\ge 0})$ の部分集合をいくつか導入して, それらの関係を表す命題や補題を与える．この準備の下, 3.3 節では $r = 2$ の場合の証明を与える．また 3.4 節では $r-1$ 次元行列のとき成立するとして r 次元行列の場合の証明を与える．3.2 節から 3.4 節で約 8 ページの証明となる．$r = 1$ の場合は自明なため証明を省略する．

注意 3.0.7. 前章で $\mathbb{F}_p$ の単位元, 零元をそれぞれ $\mathbf{1}, \mathbf{0}$ とかいていたが, 以降それぞれ $1, 0$ とかく. この記号の変更によって, たとえば前章までの記号のままであれば $\mathbf{1}/(L!\mathbf{1})$ とかいていたものを以下単に $1/L!$ とかくことになる.

3.1 Wilson の定理

この節では定理 3.0.1 の証明で必要になる Wilson の定理 [M] について説明する.

定理 3.1.1 (Wilson の定理)**.** 素数 p に対して, $(p-1)! \equiv -1 \pmod{p}$ がなりたつ.

$p = 2$ のとき, この定理は明らか. p が奇素数のときは次の等式を示せば十分である.

$$\prod_{b \in \mathbb{F}_p^\times} b = -1.$$

この等式は $\mathbb{F}_p^\times$ が $p-1$ 次巡回群であること（命題 2.7.5）と次の補題からわかる.

補題 3.1.2. $2m$ 次巡回群 G に対してすべての元の積, つまり $\prod_{g \in G} g$ は位数 2 の元である.

証明. c を G の生成元とすると次の等式がなりたつ.

$$\begin{aligned}\prod_{g \in G} g &= \prod_{0 \le i \le 2m-1} c^i \\ &= c^0 c^1 c^2 \cdots c^{m-1} c^m c^{m+1} \cdots c^{2m-2} c^{2m-1} \\ &= c^0 c^1 c^2 \cdots c^{m-1} c^m c^{-(m-1)} \cdots c^{-2} c^{-1} \\ &= c^m.\end{aligned}$$

□

3.2 準備

この節では定理 3.0.1 の証明の準備をする. 以下, 当面 $L = (l_\lambda)_{\lambda \in [n]^r}$ は非負整数成分の r 次元行列とする.

まず $b \in \mathbb{A}$ と $c = 0, 1, \ldots, p-1$ に対して $b^{(c)}$ は divided power を表す. つまり次のように定める（標数 p だから $c!$ は単元）.

$$b^{(c)} = \frac{1}{c!} b^c.$$

この divided power を用いると $a^{(L)}$ は

$$a^{(L)} = \prod_{\lambda \in [n]^r} a_\lambda^{(l_\lambda)}$$

と表せる. また n 項展開は divided power を用いると次のように表される.

命題 3.2.1. $b_1, \ldots, b_n \in \mathbb{A}$ と $c = 0, 1, \ldots, p-1$ に対して次の等式がなりたつ.

$$\left(\sum_{1 \le i \le n} b_i \right)^{(c)} = \sum_{h_1 + \cdots + h_n = c} \prod_{1 \le i \le n} b_i^{(h_i)}.$$

以下, $i_1, \ldots, i_r$ などを従属変数として和などを考えるとき, その動く範囲を明示しないときは $1, \ldots, n$ の範囲を動くものとする. たとえば, r 次元行列 $(l_{i_1 \cdots i_r})_{1 \le i_1, \ldots, i_r \le n}$ を $(l_{i_1 \cdots i_r})_{i_1, \ldots, i_r}$ とかき, この行列の成分の和を $\sum_{i_1, \ldots, i_r} l_{i_1 \cdots i_r}$ とかく.

定理 3.0.1 に現れた $\Psi_r(c)$ を定めるために記号を 2 つ用意する. まず r 次元行列を 1 次元行列に対応させる写像 T_r^j を次で定める.

定義 3.2.2. $j \in [r]$ と r 次元行列 L に対して, 1 次元行列 $T_r^j(L)$ を次で定める.

$$T_r^j(L) = \left(\sum_{i_1, \ldots, \hat{i_j}, \ldots, i_r} l_{i_1 \cdots i_r} \right)_{i_j}$$

たとえば $r = 2$ のとき, 2 次元行列 L に対して $T_2^1(L), T_2^2(L)$ は次のように表せる.

$$T_2^1(L) = \left(\sum_j l_{ij} \right)_i, \quad T_2^2(L) = \left(\sum_i l_{ij} \right)_j.$$

また $r = 3$ のとき, 3 次元行列 L に対して $T_3^1(L), T_3^2(L), T_3^3(L)$ は次のようになる.

$$T_3^1(L) = \left(\sum_{j,k} l_{ijk} \right)_i, \quad T_3^2(L) = \left(\sum_{i,k} l_{ijk} \right)_j, \quad T_3^3(L) = \left(\sum_{i,j} l_{ijk} \right)_k.$$

次に $T_r^j(L)$ の成分が一定である行列 L 全体を表す記号を定める. 以下, 非負整数 c に対して, 1 次元行列 $\underline{c}$ を

$$\underline{c} = (c)_i$$

と定める.

定義 3.2.3. $j \in [r]$ と非負整数 c に対して r 次元行列の集合 $\Upsilon_r^j(c)$ を次のように定義する.

$$\Upsilon_r^j(c) = (T_r^j)^{-1}(\{\underline{c}\}) = \{L \in \mathrm{Mat}(n^r, \mathbb{Z}_{\geq 0}) \mid T_r^j(L) = \underline{c}\}.$$

定理 3.0.1 にでてきた $\Psi_r(c)$ はこの $\Upsilon_r^1(c), \ldots, \Upsilon_r^r(c)$ の共通部分と定める.

定義 3.2.4. 非負整数 c に対して r 次元行列の集合 $\Psi_r(c)$ を次のように定義する.

$$\Psi_r(c) = \bigcap_{j \in [r]} \Upsilon_r^j(c) = \{L \in \mathrm{Mat}(n^r, \mathbb{Z}_{\geq 0}) \mid {}^{\forall} j \in [r], T_r^j(L) = \underline{c}\}.$$

また $\Psi'_r(c) = \bigcap_{j \in [r-1]} \Upsilon_r^j(c)$ と定める.

次に定理 3.0.1 の証明に用いる記号や命題, 補題を定める.

r 次元行列を $r-1$ 次元行列に対応させる写像 S_r^j を次で定める.

定義 3.2.5. $j \in [r]$ と r 次元行列 L に対して, $r-1$ 次元行列 $S_r^j(L)$ を次で定める.

$$S_r^j(L) = \left(\sum_{i_j} l_{i_1 \cdots i_r} \right)_{i_1, \ldots, \hat{i}_j, \ldots, i_r}.$$

たとえば $r = 2$ のとき, 2 次元行列 L に対し $S_2^1(L) = T_2^2(L), S_2^2(L) = T_2^1(L)$ がなりたつ. また $r = 3$ のとき, 3 次元行列 L に対し 2 次元行列 $S_3^1(L), S_3^2(L), S_3^3(L)$ は次のような 2 次元行列になる.

$$S_3^1(L) = \left(\sum_i l_{ijk} \right)_{j,k}, \quad S_3^2(L) = \left(\sum_j l_{ijk} \right)_{i,k}, \quad S_3^3(L) = \left(\sum_k l_{ijk} \right)_{i,j}.$$

定義 3.2.6. 非負整数成分の $r-1$ 次元行列 M に対して, r 次元行列の集合 $\Omega(M)$ を次のように定義する.

$$\Omega(M) = (S_r^r)^{-1}(\{M\}) = \{L \in \mathrm{Mat}(n^r, \mathbb{Z}_{\geq 0}) \mid S_r^r(L) = M\}.$$

この $\Omega(M)$ と $\Omega(M')$ は $M \neq M'$ であれば共通部分を持たない.

命題 3.2.7. $r-1$ 次元行列 M, M' に対して, 次がなりたつ.

$$M \neq M' \Rightarrow \Omega(M) \cap \Omega(M') = \emptyset.$$

証明. $L \in \Omega(M)$ とする. すると $S_r^r(L) = M$ である. $L \in \Omega(M')$ と仮定すると $S_r^r(L) = M'$ となり矛盾. □

$\Omega(M)$ を用いて $\Psi'_r(c)$ や $\Psi_r(c)$ を表すことができる.

命題 3.2.8. 次がなりたつ.

$$\bigsqcup_{M \in \Psi_{r-1}(c)} \Omega(M) = \Psi'_r(c).$$

したがって, 次もなりたつ.

$$\left(\bigsqcup_{M \in \Psi_{r-1}(c)} \Omega(M) \right) \cap \Upsilon_r^r(c) = \Psi_r(c).$$

これを示すために次の補題を用意する.

補題 3.2.9. $j \in [r-1]$ に対して, 次がなりたつ.

$$T_r^j = T_{r-1}^j \circ S_r^r.$$

証明. 次の等式からわかる.

$$\begin{aligned} T_{r-1}^j(S_r^r(L)) &= T_{r-1}^j \left(\left(\sum_{i_r} l_{i_1 \cdots i_r} \right)_{i_1, \ldots, i_{r-1}} \right) \\ &= \left(\sum_{i_1, \ldots, \hat{i}_j \ldots i_{r-1}} \left(\sum_{i_r} l_{i_1 \cdots i_r} \right) \right)_{i_j} \\ &= \left(\sum_{i_1, \ldots, \hat{i}_j \ldots i_r} l_{i_1 \cdots i_r} \right)_{i_1, \ldots, i_r} \\ &= T_r^j(L). \end{aligned}$$

□

命題 3.2.8 の証明. まず $(\subset)$ を示す. $M \in \Psi_{r-1}(c)$ とし, $L \in \Omega(M)$ とする. このとき $j \in [r-1]$ に対して $L \in \Upsilon_r^j(c)$, つまり $T_r^j(L) = \underline{c}$ を導こう. それは次の等式からわかる.

$$T_r^j(L) = T_{r-1}^j(S_r^r(L)) = T_{r-1}^j(M) = \underline{c}.$$

ここでまず第 1 の等号は補題 3.2.9 からわかる. また第 2 の等号は $L \in \Omega(M)$ より $S_r^r(L) = M$ であることからわかる. 最後に第 3 の等号は $M \in \Psi_{r-1}(c)$ からわかる.

次に ($\supset$) を示す. $L \in \Psi'_r(c)$ とする. $r-1$ 次元行列 $M = S^r_r(L)$ を考える. $L \in \Omega(M)$ がなりたつ. このとき $M \in \Psi_{r-1}(c)$, つまり任意の $j \in [r-1]$ に対して $T^j_r(M) = \underline{c}$ となることは次の等式からわかる.

$$T^j_{r-1}(M) = T^j_{r-1}(S^r_r(L)) = T^j_r(L) = \underline{c}.$$

ここでまず第 2 の等号は補題 3.2.9 からわかる. 次に第 3 の等号は $L \in \Psi'_r(c)$ からわかる. □

成分の和が c となる 1 次元行列全体を $\phi(c)$ と定める.

定義 3.2.10. 非負整数 c に対して, 1 次元行列の集合 $\phi(c)$ を次で定める.

$$\phi(c) = \left\{ (h_i)_i \in \mathrm{Mat}(n^1, \mathbb{Z}_{\geq 0}) \,\middle|\, \sum_i h_i = c \right\}.$$

$r-1$ 次元行列 M に対して, 成分の和がそれぞれ m_μ である n^{r-1} 個の 1 次元行列の組全体, つまり $\prod_{\mu \in [n]^{r-1}} \phi(m_\mu)$ は $\Omega(M)$ と自然に同一視できる.

命題 3.2.11. 非負整数成分の $r-1$ 次元行列 M に対して, $\prod_{\lambda \in [n]^{r-1}} \phi(m_\lambda)$ と $\Omega(M)$ は次のように自然に同一視できる.

$$\prod_{\mu \in [n]^{r-1}} \phi(m_\mu) \to \Omega(M), \quad (L_\mu)_{\mu \in [n]^{r-1}} \mapsto L.$$

ただし,

$$L_\mu = (l_{\mu k})_{k \in [n]}, \quad L = (l_{\mu k})_{\mu \in [n]^{r-1}, k \in [n]} = (l_\lambda)_{\lambda \in [n]^r}$$

とする.

次の等式の証明はすぐわかる.

補題 3.2.12. $B_1, \ldots, B_n$ を有限集合とし, f_i を B_i から可換環 R への写像とする. このとき次の等式がなりたつ.

$$\prod_i \sum_{b \in B_i} f_i(b) = \sum_{(b_1, \ldots, b_n) \in B_1 \times \cdots \times B_n} \prod_i f_i(b_i).$$

3.3 2 次元の場合の証明

この節では定理 3.0.1 が $r = 2$ の場合でなりたつことを示す.

命題 3.3.1 (定理 3.0.1 の $r=2$ の場合)**.** $\mathbb{A}$ 上の 2 次元行列 A に対して, 次がなりたつ.

$$\begin{aligned}\det_p A &= (-1)^n \sum_{L\in\Psi_2(p-1)} \prod_{\lambda\in[n]^2} a_\lambda^{(l_\lambda)} \\ &= (-1)^n \sum_{L\in\Psi_2(p-1)} \prod_{i,j} a_{ij}^{(l_{ij})}.\end{aligned}$$

この命題の証明の前に $\Upsilon_2^1(c), \Upsilon_2^2(c), \Psi_2(c)$ という記号を整理する.

系 3.3.2. 非負整数 c に対して, $\Upsilon_2^1(c), \Upsilon_2^2(c)$ は次のように表せる.

$$\begin{aligned}\Upsilon_2^1(c) &= \{L\in \mathrm{Mat}(n^2,\mathbb{Z}_{\geq 0}) \mid T_r^1(L) = \underline{c}\} \\ &= \{(l_{ij})_{i,j}\in \mathrm{Mat}(n^2,\mathbb{Z}_{\geq 0}) \mid {}^\forall i\in[n], \textstyle\sum_j l_{ij} = c\}, \\ \Upsilon_2^2(c) &= \{L\in \mathrm{Mat}(n^2,\mathbb{Z}_{\geq 0}) \mid T_r^2(L) = \underline{c}\} \\ &= \{(l_{ij})_{i,j}\in \mathrm{Mat}(n^2,\mathbb{Z}_{\geq 0}) \mid {}^\forall j\in[n], \textstyle\sum_i l_{ij} = c\}.\end{aligned}$$

系 3.3.3. 非負整数 c に対して, $\Psi_2(c)$ は次のように表せる.

$$\begin{aligned}\Psi_2(c) &= \Upsilon_2^1(c)\cap\Upsilon_2^2(c) \\ &= \{L\in \mathrm{Mat}(n^2,\mathbb{Z}_{\geq 0}) \mid T_r^1(L) = T_r^2(L) = \underline{c}\} \\ &= \left\{ (l_{ij})_{i,j}\in \mathrm{Mat}(n^2,\mathbb{Z}_{\geq 0}) \;\middle|\; \begin{array}{l} {}^\forall i\in[n], \sum_j l_{ij} = c, \\ {}^\forall j\in[n], \sum_i l_{ij} = c \end{array} \right\}.\end{aligned}$$

また $\phi(c)^n$ と $\Upsilon_2^1(c)$ が自然に同一視できることは命題 3.3.1 を導くための鍵となる.

補題 3.3.4. 非負整数 c に対して, $\phi(c)^n$ と $\Upsilon_2^1(c)$ は次の対応で自然に同一視できる.

$$\phi(c)^n \to \Upsilon_2^1(c), \quad (L_1,\dots,L_n)\mapsto L.$$

ただし, $L_i = (l_{ij})_j$, $L = (l_{ij})_{i,j}$ である.

これは命題 3.2.11 の $M = \underline{c}$ のケースである.

以上の準備の下, 命題 3.3.1 は次のように証明できる.

命題 3.3.1 の証明. 以下,

$$H = (h_j)_j, \quad L_i = (l_{ij})_j, \quad L = (l_{ij})_{ij}$$

とし,

$$\phi = \phi(p-1), \quad \Upsilon_2^1 = \Upsilon_2^1(p-1), \quad \Upsilon_2^2 = \Upsilon_2^2(p-1), \quad \Psi_2 = \Psi_2(p-1)$$

と表す. 1 次元行列 At は

$$At = (\sum_j a_{ij}t_j)_i$$

と表せる. したがって, 次の等式がなりたつ.

$$\begin{aligned}(-1)^{-n}\det_p(At) &= (p-1)!^{-n}\det_p(At)\\ &= \prod_i (\sum_j a_{ij}t_j)^{(p-1)}\\ &= \prod_i \sum_{H\in\phi}\prod_j (a_{ij}t_j)^{(h_j)}\\ &= \sum_{(L_1,\dots,L_n)\in\phi^n}\prod_i\prod_j (a_{ij}t_j)^{(l_{ij})}.\end{aligned}$$

ここでまず第 1 の等号は Wilson の定理からわかる. 次に第 3 の等号は n 項展開（命題 3.2.1）を考えればわかる. また第 4 の等号は補題 3.2.12 からわかる. 補題 3.3.4 より ϕ^n と Υ_2^1 が自然に同一視できることから次の等式がわかる.

$$\begin{aligned}(-1)^{-n}\det_p(At) &= \sum_{L\in\Upsilon_2^1}\prod_i\prod_j (a_{ij}t_j)^{(l_{ij})}\\ &= \sum_{L\in\Upsilon_2^1}\prod_i\prod_j (a_{ij}t_j)^{(l_{ij})}\\ &= \sum_{L\in\Upsilon_2^1}\prod_i\prod_j a_{ij}^{(l_{ij})}t_j^{l_{ij}}\\ &= \sum_{L\in\Upsilon_2^1} a^{(L)}\prod_i\prod_j t_j^{l_{ij}}\\ &= \sum_{L\in\Upsilon_2^1} a^{(L)}\prod_j t_j^{\sum_i l_{ij}}.\end{aligned}$$

$\det_p A$ は $\det_p(Ax)$ における $\prod_j x_j^{p-1}$ の係数である. 系 3.3.2 より Υ_2^2 が各列の和が $p-1$ となる 2 次元行列全体であることから次の等式がなりたつことがわかる.

$$\det_p A = (-1)^n \sum_{L\in\Upsilon_2^1\cap\Upsilon_2^2} a^{(L)} = (-1)^n \sum_{L\in\Psi_2} a^{(L)}. \qquad \square$$

3.4 次元が一般の場合の証明

この節では定理 3.0.1 が r が一般の場合でもなりたつことを示す. つまり $\mathbb{A}$ 上の r 次元行列 A に対して, 次がなりたつ.

$$\det_p A = (-1)^n \sum_{L\in\Psi_r(p-1)} \prod_{\lambda\in[n]^r} a_\lambda^{(l_\lambda)}$$

定理 3.0.1 の証明. 以下,

$$M = (m_\mu)_{\mu\in[n]^{r-1}}, \quad H = (h_k)_k, \quad L_\mu = (l_{\mu k})_k, \quad L = (l_\lambda)_{\lambda\in[n]^r}$$

とし,

$$\Psi_{r-1} = \Psi_{r-1}(p-1), \quad \Psi'_r = \Psi'_r(p-1), \quad \Upsilon^r_r = \Upsilon^r_r(p-1), \quad \Psi_r = \Psi_r(p-1)$$

と表す. r に関する帰納法で証明する. $r = 2$ のときは命題 3.3.1 の主張である. ここで $r-1$ 次元行列に対してこの定理がなりたつと仮定する. r 次元行列 A に対しても成立することを示そう. まず次の等式がわかる.

$$\begin{aligned}
(-1)^{-n}\det_p(At) &= \sum_{M\in\Psi_{r-1}} \prod_{\mu\in[n]^{r-1}} (\sum_k a_{\mu k}t_k)^{(m_\mu)} \\
&= \sum_{M\in\Psi_{r-1}} \prod_{\mu\in[n]^{r-1}} \sum_{H\in\phi(m_\mu)} \prod_k (a_{\mu k}t_k)^{(h_k)} \\
&= \sum_{M\in\Psi_{r-1}} \sum_{(L_\mu)_{\mu\in[n]^{r-1}}\in\prod_{\mu\in[n]^{r-1}}\phi(m_\mu)} \prod_{\mu\in[n]^{r-1}} \prod_k (a_{\mu k}t_k)^{(l_{\mu k})} \\
&= \sum_{M\in\Psi_{r-1}} \sum_{L\in\Omega(M)} \prod_{\mu\in[n]^{r-1}} \prod_k (a_{\mu k}t_k)^{(l_{\mu k})} \\
&= \sum_{L\in\bigsqcup_{M\in\Psi_{r-1}}\Omega(M)} \prod_{\mu\in[n]^{r-1}} \prod_k (a_{\mu k}t_k)^{(l_{\mu k})}.
\end{aligned}$$

ここでまず第 1 の等号は仮定からわかる. 次に第 2 の等号は n 項展開（命題 3.2.1）を考えればわかる. また第 3 の等号は補題 3.2.12 からわかる. 第 4 の等号は命題 3.2.11 より $\prod_{\mu\in[n]^{r-1}}\phi(m_\mu)$ と $\Omega(M)$ が自然に同一視できることからわかる. 最後に第 5 の等号は命題 3.2.7 からわかる. 命題 3.2.8 より $\bigsqcup_{M\in\Psi_{r-1}}\Omega(M) = \Psi'_r$ だから次の等式がなりたつ.

$$
\begin{aligned}
(-1)^{-n}\det_p(At) &= \sum_{L\in\Psi'_r}\prod_{\mu\in[n]^{r-1}}\prod_k (a_{\mu k}t_k)^{(l_{\mu k})} \\
&= \sum_{L\in\Psi'_r}\prod_{\mu\in[n]^{r-1}}\prod_k a_{\mu k}^{(l_{\mu k})}t_k^{l_{\mu k}} \\
&= \sum_{L\in\Psi'_r} a^{(L)}\prod_{\mu\in[n]^{r-1}}\prod_k t_k^{l_{\mu k}} \\
&= \sum_{L\in\Psi'_r} a^{(L)}\prod_k t_k^{\sum_{\mu\in[n]^{r-1}} l_{\mu k}}.
\end{aligned}
$$

$\det_p A$ は $\det_p(At)$ における $\prod_k t_k^{p-1}$ の係数である．$L\in\Upsilon_r^r$ と「任意の $k\in[n]$ に対して $\sum_{\mu\in[n]^{r-1}} l_{\mu k}=p-1$ が同値である」ということから次の等式がなりたつことがわかる．

$$
\det_p A = (-1)^n \sum_{L\in\Psi'_r\cap\Upsilon_r^r} a^{(L)} = (-1)^n \sum_{L\in\Psi_r} a^{(L)}. \qquad \square
$$

4　超行列式の積公式

この章では Glynn の超行列式が積を保つということの証明をする. 1.3 節で Cayley や Schläfli, Gelfand, Kapranov, Zelevinsky らも超行列式を考えたと述べたが, 実は Glynn の超行列式にのみ積を保つという性質がある. 以下, $\mathbb{A}$ はこれまでと同じく標数 p の体 $\mathbb{F}$ 上の可換代数とする.

定理 4.0.1. 自然数 r, s が $r, s \geq 2$ をみたすとき, $\mathbb{A}$ 上の r 次元行列 A と s 次元行列 B に対して次の等式がなりたつ.

$$\det_p(AB) = (\det_p A)(\det_p B).$$

以下の証明は Glynn [G1] の証明を丁寧にまとめたものである.

この章は本論文の主題である行列式の冪の展開係数と論理的な関係はなく, 読み飛ばしても他の章を読む際に支障はないが, Glynn の超行列の積を保つという特徴は興味深いのでここにまとめた.

4.1　準備

この節ではこの定理 4.0.1 を示すための準備をする. まず超行列同士の積が結合法則をみたすことはすぐわかる. 以下, R は可換環である.

命題 4.1.1. 次の等式がなりたつ.

$$(A_1A_2)A_3 = A_1(A_2A_3).$$

ただし, A_1, A_2, A_3 をそれぞれ R 上の r_1 次元行列, r_2 次元行列, r_3 次元行列とし, $r_1 \geq 1, r_2 \geq 2, r_3 \geq 1$ をみたすとする.

また次の等式もすぐわかる. ただし, $R[t] = R[t_1, \ldots, t_n]$ は $t_1, \ldots, t_n$ という n 個の不定元の R 係数多項式環である.

命題 4.1.2. 自然数 k と $c \in R$ と $f(t) \in R[t]$ に対して, 次の等式がなりたつ.

$$\langle cf(t)\rangle_k = c\langle f(t)\rangle_k.$$

次の命題が超行列式の積公式を導く上で最大の鍵となる.

命題 4.1.3. 自然数 r が $r \geq 2$ をみたすとき, $\mathbb{A}$ 上の r 次元行列 A に対して次の等式がなりたつ.

$$\det_p A = \langle \det_p(tA) \rangle_{p-1}.$$

Glynn の超行列式の定義（定義 1.1.6）では At の超行列式のある項の係数を A の超行列式と定めたが, この命題は At を tA と置き換えても構わないということを主張している. この事実は定理 3.0.1 の結果が $A = (a_{i_1 \cdots i_r})_{1 \leq i_1, \ldots, i_r \leq n}$ の r 個の添字 $i_1, \ldots, i_r$ に関して対称であることからわかる. 定義 1.1.6 にしたがって計算すると, 最後の添字 i_r に注目して計算することになる. しかし, 実際は定理 3.0.1 の対称性から他の添字に注目して計算しても同じ結果を得る. とくに添字 i_1 に注目して計算しても同じ結果になることをこの命題 4.1.3 は主張している.

4.2 積公式の証明

この節では定理 4.0.1 の証明をする. まず $s = 2$ のケースについて r に関する帰納法で証明した後に, 一般のケースを s に関する帰納法で証明する.

まず次を示そう.

命題 4.2.1. 自然数 r が $r \geq 2$ をみたすとき, $\mathbb{A}$ 上の r 次元行列 A と 2 次元行列 B に対して次の等式がなりたつ.

$$\det_p(AB) = (\det_p A)(\det_p B).$$

証明. A が 2 次元行列のとき次の等式がなりたつ.

$$\det_p(AB) = (\det(AB))^{p-1} = (\det A)^{p-1}(\det B)^{p-1} = \det_p A \det_p B.$$

ここでまず第 1, 第 3 の等号は AB, A, B が 2 次元行列だから定理 2.2.1 からわかる. 次に第 2 の等号は通常の行列式の積公式である.

A が k 次元行列のとき $\det_p(AB) = (\det_p A)(\det_p B)$ がなりたつと仮定する. A が $k+1$ 次元行列のときもこの等式がなりたつことを示す. これは次の計算からわかる.

$$\begin{aligned}
\det_p(AB) &= \langle \det_p(t(AB)) \rangle_{p-1} \\
&= \langle \det_p((tA)B) \rangle_{p-1} \\
&= \langle \det_p(tA) \det_p B \rangle_{p-1} \\
&= \langle \det_p(tA) \rangle_{p-1} \det_p B \\
&= \det_p A \det_p B.
\end{aligned}$$

ここでまず第 1, 第 5 の等号は命題 4.1.3 からなりたつ. 次に第 2 の等号は超行列の積は結合法則をみたすこと（命題 4.1.1）からわかる. 第 3 の等号は tA が k 次元行列であることに注意すると仮定から導かれる. 最後に第 4 の等号は命題 4.1.2 からわかる. □

この命題から定理 4.0.1 を証明しよう.

定理 4.0.1 の証明. B が 2 次元行列のときは命題 4.2.1 の主張である.

B が k 次元行列のとき $\det_p(AB) = (\det_p A)(\det_p B)$ がなりたつと仮定する. B が $k+1$ 次元行列のときもこの等式がなりたつことを示す. これは次の等式からわかる.

$$\begin{aligned}
\det_p(AB) &= \langle \det_p((AB)t) \rangle_{p-1} \\
&= \langle \det_p(A(Bt)) \rangle_{p-1} \\
&= \langle \det_p A \det_p(Bt) \rangle_{p-1} \\
&= \det_p A \langle \det_p(Bt) \rangle_{p-1} \\
&= \det_p A \det_p B.
\end{aligned}$$

ここで第 1, 第 5 の等号は超行列式の定義（定義 1.1.6）である. 第 2 の等号は超行列の積の結合法則（命題 4.1.1）からわかる. 次に第 3 の等号は Bt が k 次元行列であることに注意すると仮定から導かれる. 最後に第 4 の等号は命題 4.1.2 からわかる. □

5 $(\det X)^m$ の展開係数に 0 を含む m の条件

この章では自然数 m に対して $(\det X)^m$ の展開係数で 0 となるものがあるかどうか考えよう. まず展開係数を次で定める.

定義 5.0.1. $L \in \Psi_2(m)$ に対して C_L は次の等式をみたす整数とする.

$$(\det X)^m = \sum_{L \in \Psi_2(m)} C_L x^L.$$

ここで $\Psi_2(m)$ は第 3 章で述べたように各行, 各列の和が m となる非負整数を成分とする n^2 行列全体である. また X は x_{ij}（ただし, $1 \leq i, j \leq n$）という n^2 個の不定元を成分とする n^2 行列 $X = (x_{ij})_{1 \leq i,j \leq n}$ とする. 第 2 章では x_{ij} は $\mathbb{F}_p$ 係数の多項式とみなしたが, 今後は x_{ij} は基本的に $\mathbb{Z}$ 係数の多項式とみなす. この n^2 個の不定元の $\mathbb{Z}$ 係数多項式環を $\mathbb{Z}[X]$ とかく. C_L を定めた上の等式は $\mathbb{Z}[X]$ における等式ということになる.

この章ではまず次の定理を示す.

定理 5.0.2. p が素数のとき, 任意の $L \in \Psi_2(p-1)$ に対して $C_L \neq 0$. つまり, $(\det X)^{p-1}$ の展開係数は 0 を含まない.

この定理は Glynn [G2] が明らかにしたことであり, 第 2 章と第 3 章の結果から導かれる（詳しくは 5.1 節）.

実はこの定理の裏もなりたつ（ただし, $n \geq 3$ のときのみ）.

定理 5.0.3. $n \geq 3$ とする. $m = p-1$ をみたす素数 p が存在しないとき, ある $L \in \Psi_2(m)$ が存在して $C_L = 0$.

この定理は本論文で初めて明らかにされる事実である（詳しくは 5.2 節）.

この定理 5.0.2 と定理 5.0.3 は正則二部グラフの完全マッチングへの分割の個数の話に言い換えられる（詳しくは第 6 章）.

5.1 $(\det X)^{p-1}$ の展開係数は 0 を含まない

この節では定理 5.0.2, つまり $(\det X)^{p-1}$ の展開係数は 0 を含まないことを示す. この証明では第 2 章「通常の行列に対する超行列式」と第 3 章「超行列式の展開」が鍵となる.

定理 5.0.2 の証明. この証明では不定元 x_{ij} は $\mathbb{F}_p$ 係数の多項式として扱う. 定義 5.0.1

の等式の x_{ij}（これは $\mathbb{Z}$ 係数の多項式）にこの $\mathbb{F}_p$ 係数の多項式 x_{ij} を代入することで, $\mathbb{F}_p[X]$ における次の等式を得る.

$$(\det X)^m = \sum_{L \in \Psi_2(m)} C_L x^L.$$

また $\mathbb{F}_p[X]$ において次の等式もなりたつ.

$$(\det X)^{p-1} = \det_p X = \sum_{L \in \Psi_2(p-1)} \frac{(-1)^n}{L!} x^L.$$

ここで第 1 の等号は定理 2.2.1 の主張である. また第 2 の等号は定理 3.0.1（$\mathbb{A} = \mathbb{F}_p[X]$ のケース）の主張である. この 2 つの等式を係数比較することで, $L \in \Psi_2(p-1)$ に対して次の等式を得る（両辺は $\mathbb{F}_p$ の元とみなす）.

$$C_L = \frac{(-1)^n}{L!}.$$

したがって次がなりたつ.

$$L! C_L \equiv (-1)^n \pmod{p}.$$

よって $C_L \neq 0$ である. □

5.2 $m \neq p-1$ なら $(\det X)^m$ の展開係数は 0 を含む

前節で定理 5.0.2 を証明したが, 実はこの裏である定理 5.0.3 も成立する（ただし, $n \geq 3$ のときのみ）. この節ではこのこと, つまり $m = p-1$ をみたす素数 p が存在しないとき $(\det X)^m$ の展開係数は必ず 0 を含むことを示す. この事実は本論文で初めて明らかにすることである.

以下, m は $m = p-1$ をみたす素数 p が存在しない自然数とする. この定理は $n = 3$ のときが本質的であり, これから $n \geq 4$ の場合も導かれる.

まず $n = 3$ のときに定理 5.0.3 がなりたつこと, つまり X が 3 次正方行列のとき $(\det X)^m$ の展開係数に 0 を含むことを示そう. 具体的にいうと, 次の $L = L^{ab}(3)$ に対する展開係数が 0 となる.

$$L^{ab}(3) = \begin{pmatrix} ab+b-1 & a & 1 \\ a & ab & b \\ 1 & b & ab+a-1 \end{pmatrix} \in \Psi_2(m).$$

ただし, a と b は $m+1 = (a+1)(b+1)$ をみたす自然数とする（$m+1$ は合成数なのでこのような a と b は必ず存在する）.

命題 5.2.1. $C_{L^{ab}(3)} = 0$.

証明. $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3 \in \mathbb{Z}[X]$ を次で定める.

$$\begin{array}{lll} \alpha_1 = x_{11}x_{22}x_{33}, & \alpha_2 = x_{12}x_{23}x_{31}, & \alpha_3 = x_{13}x_{21}x_{32}, \\ \beta_1 = x_{12}x_{21}x_{33}, & \beta_2 = x_{11}x_{23}x_{32}, & \beta_3 = x_{13}x_{22}x_{31}. \end{array}$$

すると, 次の等式がなりたつ.

$$\det X = \alpha_1 + \alpha_2 + \alpha_3 - \beta_1 - \beta_2 - \beta_3.$$

よって $(\det X)^m$ は次のように展開される.

$$(\det X)^m = \sum_{k_1+k_2+k_3+l_1+l_2+l_3=m} (-1)^{l_1+l_2+l_3} \binom{m}{k_1, k_2, k_3, l_1, l_2, l_3} \alpha_1^{k_1}\alpha_2^{k_2}\alpha_3^{k_3}\beta_1^{l_1}\beta_2^{l_2}\beta_3^{l_3}.$$

ただし, 次のような多項係数の記号を用いる.

$$\binom{m}{k_1, k_2, k_3, l_1, l_2, l_3} = \frac{m!}{k_1!k_2!k_3!l_1!l_2!l_3!}.$$

ここで

$$x^{L^{ab}(3)} = \alpha_1^{k_1}\alpha_2^{k_2}\alpha_3^{k_3}\beta_1^{l_1}\beta_2^{l_2}\beta_3^{l_3}.$$

をみたす非負整数の組 $(k_1, k_2, k_3, l_1, l_2, l_3)$ は

$$(ab-1, 0, 0, a, b, 1), \quad (ab, 1, 1, a-1, b-1, 0)$$

の 2 つのみであることに注意する. 実際 $(k_1, k_2, k_3, l_1, l_2, l_3)$ は次の 9 つの等式をみたす必要があるが, この解が上の 2 つのみであることはすぐわかる.

$$\begin{array}{lll} k_1 + l_2 = ab + b - 1, & k_2 + l_1 = a, & k_3 + l_3 = 1, \\ k_3 + l_1 = a, & k_1 + l_3 = ab, & k_2 + l_2 = b, \\ k_2 + l_3 = 1, & k_3 + l_2 = b, & k_1 + l_1 = ab + a - 1. \end{array}$$

この 2 つの組に対応する多項係数は等しい, つまり次の等式がなりたつ.

$$\binom{m}{ab-1, 0, 0, a, b, 1} = \binom{m}{ab, 1, 1, a-1, b-1, 0}.$$

この等式と

$$(\det X)^m = \sum_{L \in \Psi_2(m)} C_L x^L$$

という展開を比較すると次がわかる.

$$\begin{aligned} C_{L^{ab}(3)} &= (-1)^{a+b+1}\binom{m}{ab-1,0,0,a,b,1} \\ &\quad + (-1)^{(a-1)+(b-1)+0}\binom{m}{ab,1,1,a-1,b-1,0} \\ &= 0. \end{aligned}$$

□

次に $n \geq 4$ のときに定理 5.0.3 がなりたつこと, つまり X が n 次正方行列のとき $(\det X)^m$ の展開係数は 0 を含むことを示そう. 具体的に次の $L = L^{ab}(n)$ に対する展開係数が 0 となる.

$$L^{ab}(n) = \begin{pmatrix} L^{ab}(3) & & & \\ & m & & \\ & & \ddots & \\ & & & m \end{pmatrix} \in \Psi_2(m).$$

つまり $L^{ab}(n)$ は 3×3 行列 $L^{ab}(3)$ と $n-3$ 個の 1×1 行列 (m) が対角線上に並んだ対角ブロック行列である. ただし, a と b は先ほどと同じように $m+1 = (a+1)(b+1)$ をみたす自然数とする.

命題 5.2.2. $C_{L^{ab}(n)} = 0$.

証明. $x^{L^{ab}(n)}$ は次のように表せる.

$$\begin{aligned} x^{L^{ab}(n)} &= x_{11}^{ab+b-1}x_{12}^{a}x_{13}^{1} \\ &\quad \cdot x_{21}^{a}x_{22}^{ab}x_{23}^{b} \\ &\quad \cdot x_{31}^{1}x_{32}^{b}x_{33}^{ab+a-1} \\ &\quad \cdot \prod_{4 \leq i \leq n} x_{ii}^{m}. \end{aligned}$$

したがって,

$$x^{L^{ab}(n)} = \prod_{1 \leq i \leq m} x_{1\sigma_i(1)}x_{2\sigma_i(2)}\cdots x_{n\sigma_i(n)}$$

をみたす $\sigma_1, \ldots, \sigma_m \in S_n$ は $\varepsilon, (123), (132), (12), (23), (13)$ のいずれかである. あとは $n = 3$ のときと同様の議論で $C_{L^{ab}(n)} = 0$ が示される. □

6　正則二部グラフの完全マッチングへの偶分割と奇分割の個数の比較

前章で論じた $(\det X)^m$ の展開係数 C_L が 0 か否かという問題は, 正則二部グラフの完全マッチングへの分割の個数に関する問題に言い換えられる. つまり, 前章の定理はこのグラフの問題についての定理とみなせる. またこのグラフの問題は Alon–Tarsi 予想というラテン方陣に関する未解決問題の一般化とみなせる. さらに前章の定理 5.0.2 からこの予想の特別な場合が解決される.

6.4 節では Glynn [G2] による Alon–Tarsi 予想の特別なケースの解決をまとめている. [G2] で扱っているのはラテン方陣だが, 議論を素直に読むとむしろグラフの話と解釈するのが自然である. このグラフの話を整理したのが 6.1 節から 6.3 節である.

6.1　各行, 各列の和が一定の正方行列の置換行列への分割

この節では $L \in \Psi_2(m)$ に対して, L の置換行列への分割を説明する. ここで $\Psi_2(m)$ は第 3 章で述べたように各行, 各列の和が m となる非負整数成分の n 次正方行列全体である. この L の置換行列への分割は, 正則二部グラフの完全マッチングへの分割と同一視するのが自然である（詳しくは 6.3 節）.

$\Psi_2(1)$ は n 次の置換行列全体であることはすぐわかる. これに注意すれば m 個の置換行列の和が $\Psi_2(m)$ に含まれることもすぐわかる. 逆に $L \in \Psi_2(m)$ を m 個の置換行列の和で表したとき, 対応する置換行列たちの組（正確には置換の組）を L の置換行列への分割とよぶ. 以下, 単にこれを L の分割とよぶ.

定義 6.1.1. $L \in \Psi_2(m)$ とする. m 個の置換 $\sigma_1, \ldots, \sigma_m \in S_n$ が次の等式をみたすとき, $\Sigma = (\sigma_1, \ldots, \sigma_m)$ を L の置換行列への分割とよぶ（以下, 単に L の分割とよぶ）.

$$\sum_{1 \le i \le m} P_{\sigma_i} = L.$$

ただし, δ_{ij} を Kronecker のデルタとし, $\sigma \in S_n$ から定まる置換行列 P_σ を $P_\sigma = (\delta_{\sigma(i)j})_{1 \le i,j \le n}$ と表す. また L の分割全体を $\mathrm{P}(L)$ と表す.

この置換 $\sigma_1, \ldots, \sigma_m$ の符号の積を分割 Σ の符号と定める.

定義 6.1.2. $L \in \Psi_2(m)$ の分割 $\Sigma = (\sigma_1, \ldots, \sigma_m)$ に対して, Σ の符号 $\operatorname{sgn}\Sigma$ を次で定

める.

$$\operatorname{sgn}\Sigma = \prod_{1\leq i\leq m} \operatorname{sgn}\sigma_i.$$

とくに $\operatorname{sgn}\Sigma = 1$ なら Σ を L の偶分割とよび, $\operatorname{sgn}\Sigma = -1$ なら Σ を L の奇分割とよぶ. さらに L の偶分割全体を $\mathrm{EP}(L)$, L の奇分割全体を $\mathrm{OP}(L)$ とかく.

6.2 偶分割と奇分割の個数の差 $|\mathrm{EP}(L)| - |\mathrm{OP}(L)|$ と展開係数 C_L

この節では $L \in \Psi_2(m)$ に対して, 偶分割の個数 $|\mathrm{EP}(L)|$ と奇分割の個数 $|\mathrm{OP}(L)|$ が等しいか否かという問題を考えよう. 第 5 章の議論から次のことがわかる.

定理 6.2.1. p が素数のとき任意の $L \in \Psi_2(p-1)$ に対して

$$|\mathrm{EP}(L)| \neq |\mathrm{OP}(L)|.$$

定理 6.2.2. $n \geq 3$ とする. 任意の素数 p に対して $m \neq p-1$ であるとき, ある $L \in \Psi_2(m)$ が存在して

$$|\mathrm{EP}(L)| = |\mathrm{OP}(L)|.$$

これらの定理は, $(\det X)^m$ の展開係数 C_L に関する次の命題に注意すれば, それぞれ定理 5.0.2, 定理 5.0.3 からわかる.

命題 6.2.3. $L \in \Psi_2(m)$ に対して次の等式がなりたつ.

$$C_L = |\mathrm{EP}(L)| - |\mathrm{OP}(L)|.$$

以下, この命題を示そう.

この命題を示すために補題を 3 つ用意する. まず $(\det X)^m$ は次のように展開できる.

補題 6.2.4. 不定元を成分とする行列 X に対して次の等式がなりたつ.

$$(\det X)^m = \sum_{\Sigma\in S_n^m} \operatorname{sgn}(\Sigma)\alpha^{\Sigma}.$$

ただし, $\sigma \in S_n$ に対して $\alpha_\sigma \in \mathbb{Z}[X]$ を

$$\alpha_\sigma = \prod_{1\leq i\leq n} x_{i\sigma(i)}$$

とし, $\Sigma = (\sigma_1, \ldots, \sigma_m)$ のとき $\alpha^\Sigma \in \mathbb{Z}[X]$ を

$$\alpha^\Sigma = \alpha_{\sigma_1}\cdots\alpha_{\sigma_m}$$

と定める.

次の補題はすぐわかる.

補題 6.2.5. $L \in \Psi_2(m)$ のとき, $\Sigma \in \mathrm{P}(L)$ に対して $\alpha^{\Sigma} = x^L$.

最後に補題 6.2.4, 補題 6.2.5 を

$$(\det X)^m = \sum_{L \in \Psi_2(m)} C_L x^L$$

という展開と係数比較すると次がわかる.

補題 6.2.6. 次の等式がなりたつ.

$$C_L = \sum_{\Sigma \in \mathrm{P}(L)} \operatorname{sgn} \Sigma.$$

この補題から命題 6.2.3 を導く.

命題 6.2.3 の証明. 今述べた補題 6.2.6 から次を得る.

$$\begin{aligned} C_L &= \sum_{\Sigma \in \mathrm{P}(L)} \operatorname{sgn} \Sigma \\ &= \sum_{\Sigma \in \mathrm{EP}(L)} \operatorname{sgn} \Sigma + \sum_{\Sigma \in \mathrm{OP}(L)} \operatorname{sgn} \Sigma \\ &= |\,\mathrm{EP}(L)| - |\,\mathrm{OP}(L)|. \end{aligned}$$

□

以上で命題 6.2.3 が導かれたので定理 6.2.1, 定理 6.2.2 が示された.

6.3 正則二部グラフの完全マッチングへの分割

前節までで述べた L の分割は, 正則二部グラフの完全マッチングへの分割の話とみなせる. この節ではこのグラフの分割の説明をする. グラフに関する用語は [K3] を参考にした.

頂点集合 V とその頂点同士を結ぶ辺たちの組をグラフとよぶ. 本論文では単にグラフと言えば多重グラフ（つまり多重辺やループを含むようなグラフ）を意味することとする.

V のどの頂点に対してもその頂点と接続する辺がただ 1 つ存在するグラフを V 上の完全マッチングとよぶ.

頂点集合 V が V_1 と V_2 に分割されているとする（つまり $V = V_1 \sqcup V_2$ をみたす）. V_1 の頂点と V_2 の頂点を結ぶ辺のみから構成されるグラフを (V_1, V_2) 上の二部グラフとよぶ.

どの頂点にも接続する辺の数が一定であるグラフを正則グラフとよび, とくにその接続する辺の数が m 個であるときそのグラフを m-正則グラフとよぶ.

以下, (V_1, V_2) 上の m-正則二部グラフ全体を $\mathrm{RBG}(m)$ とかく. また (V_1, V_2) 上の二部グラフであるような V 上の完全マッチング全体を PM とかく. $\mathrm{PM} = \mathrm{RBG}(1)$ であることはすぐわかる.

正則二部グラフに関して次がなりたつ.

命題 6.3.1. (V_1, V_2) 上の正則二部グラフが存在するとき $|V_1| = |V_2|$ がなりたつ.

本論文ではこの命題の証明は省略する. この命題に注意して, 以下 V_1, V_2 を $[n]$ と同一視する. すると $\mathrm{RBG}(m)$ の元は $[n]^2$ から $\mathbb{Z}_{\geq 0}$ への写像とみなせる. ここで $[n]$ は n 以下の自然数全体である. また次がなりたつことはすぐわかる.

命題 6.3.2. $G \in \mathrm{RBG}(m)$ であるためのグラフ G の必要十分条件は次をみたすことである.

$$
\begin{aligned}
&{}^{\forall} i \in [n], \sum_{j \in [n]} G(i,j) = m, \\
&{}^{\forall} j \in [n], \sum_{i \in [n]} G(i,j) = m.
\end{aligned}
$$

これに注意すれば PM の m 個の元の和が $\mathrm{RBG}(m)$ の元であることはすぐわかる. 逆に $G \in \mathrm{RBG}(m)$ を m 個の PM の元の和で表すことを G の完全マッチングへの分割とよぶ. 以下, 単にこれを G の分割とよぶ.

定義 6.3.3. $G \in \mathrm{RBG}(m)$ とする. $(\tau_1, \ldots, \tau_m) \in \mathrm{PM}^m$ が次の等式をみたすとき, これを G の完全マッチングへの分割とよぶ（以下, 単に G の分割とよぶ）.

$$
\sum_{1 \leq i \leq m} \tau_i = G.
$$

また G の分割全体を $\mathrm{P}(G)$ とする.

この G の分割は 6.1 節, 6.2 節で述べた L の分割と自然に同一視できる. つまり $\mathrm{RBG}(m)$ と $\Psi_2(m)$（各行, 各列の和が m となる n 次正方行列全体）は次の対応で同一視できる.

$$
\mathrm{RBG}(m) \to \Psi_2(m), \quad G \mapsto (G(i,j))_{1 \leq i,j \leq n}.
$$

このことは命題 6.3.2 からわかる．完全マッチング全体 $\mathrm{PM} = \mathrm{RBG}(1)$ と置換行列全体 $\Psi_2(1)$ も同一視できるので, $G \in \mathrm{RBG}(m)$ の分割に偶奇, つまり符号が自然に定まる．以下, G の偶分割全体を $\mathrm{EP}(G)$, 奇分割全体を $\mathrm{OP}(G)$ とかく．偶分割の個数 $|\mathrm{EP}(G)|$ と奇分割の個数 $|\mathrm{OP}(G)|$ が等しいか否かという問題に関する定理が, 6.2 節の議論の言い換えで次のように得られる．

定理 6.3.4. p を素数とする．このとき任意の $G \in \mathrm{RBG}(p-1)$ に対して

$$|\mathrm{EP}(G)| \neq |\mathrm{OP}(G)|.$$

定理 6.3.5. $n \geq 3$ とする．$m = p - 1$ をみたす素数 p が存在しないとき, ある $G \in \mathrm{RBG}(m)$ が存在して

$$|\mathrm{EP}(G)| = |\mathrm{OP}(G)|.$$

6.4 Glynn による Alon–Tarsi 予想の部分的解決

前節で述べたグラフの問題は Alon–Tarsi 予想という未解決問題の自然な一般化とみなせる．また定理 6.3.4 から Alon–Tarsi 予想の特別な場合が解決される．この節ではこのことを説明する．[G2] の内容を前節までのグラフの話の観点からまとめたものである．

まず Alon–Tarsi 予想の説明をする．Alon–Tarsi 予想はラテン方陣の個数についての予想である．n 次ラテン方陣とは各行, 各列に 1 から n の自然数が 1 回ずつ現れる $n \times n$ 行列である．以下, n 次ラテン方陣全体を $\mathrm{LS}(n)$ とかく．

n 次ラテン方陣はすべての成分が 1 である正方行列 $L'(n) = (1)_{1 \leq i,j \leq n} \in \Psi_2(n)$ の分割と自然に同一視できる（グラフの話でいうと, 完全二部グラフ G' の完全マッチングへの分割と同一視できる）．実際, 次の写像は全単射である．

$$\mathrm{P}(L'(n)) \to \mathrm{LS}(n), \quad (\sigma_1, \ldots, \sigma_n) \mapsto \sum_{1 \leq i \leq n} iP_{\sigma_i}.$$

ラテン方陣の符号をそれに対応する $L'(n)$ の分割の符号と定める．言い換えると次のようになる．

命題 6.4.1. 任意の $\Lambda \in \mathrm{LS}(n)$ に対して, n 個の置換 $\sigma_1, \ldots, \sigma_n \in S_n$ が一意的に存在して次の等式がなりたつ．

$$\Lambda = \sum_{1 \leq i \leq n} iP_{\sigma_i}.$$

定義 6.4.2. $\Lambda \in \mathrm{LS}(n)$ に対して Λ の符号 $\operatorname{sgn}\Lambda$ を次で定める.

$$\operatorname{sgn}\Lambda = \prod_{1\leq i\leq n} \operatorname{sgn}\sigma_i.$$

この符号により偶ラテン方陣, 奇ラテン方陣の概念が定まる. n 次の偶ラテン方陣全体を $\mathrm{ELS}(n)$, 奇ラテン方陣全体を $\mathrm{OLS}(n)$ とかく. 偶ラテン方陣と奇ラテン方陣の個数の比較に関する次の予想が Alon–Tarsi 予想である [AT].

予想 6.4.3 (Alon–Tarsi 予想)**.** n が偶数のとき, $|\mathrm{ELS}(n)| \neq |\mathrm{OLS}(n)|$.

偶ラテン方陣と奇ラテン方陣の個数はそれぞれ

$$|\mathrm{ELS}(n)| = |\mathrm{EP}(L'(n))| = |\mathrm{EP}(G')|, \quad |\mathrm{OLS}(n)| = |\mathrm{OP}(L'(n))| = |\mathrm{OP}(G')|$$

と表せる. したがって, 前節のグラフの問題は Alon–Tarsi 予想の一般化とみなせる. つまり, 「偶ラテン方陣と奇ラテン方陣の個数は等しいか」という問題は,「グラフの偶分割と奇分割の個数は等しいか」という問題の特別なケースとみなせる. Glynn の結果である定理 5.0.2 から定理 6.3.4 を経由して Alon–Tarsi 予想の特別なケースが解決される [G2].

定理 6.4.4. $n = p - 1$ のとき, $|\mathrm{ELS}(n)| \neq |\mathrm{OLS}(n)|$.

実際は定理を得た経緯は逆であり, この Glynn の Alon–Tarsi 予想に関する結果がまずあり, これを本論文でまとめ直したのが前節の内容である. つまり [G2] の証明は定理 5.0.2 が鍵であり, これを素直に読むとラテン方陣というよりグラフの話と解釈するのが自然だという認識にいたったのである.

注意 6.4.5. なお, n が 3 以上の奇数のときは $|\mathrm{ELS}(n)| = |\mathrm{OLS}(n)|$ である. これを示すことは比較的易しい. 次の写像が全単射であることを確認すればよい.

$$\mathrm{ELS}(n) \to \mathrm{OLS}(n), \quad \sum_{1\leq i\leq n} iP_{\sigma_i} \mapsto \sum_{1\leq i\leq n} iP_{\sigma_i(12)}.$$

注意 6.4.6. ラテン方陣の符号は通常は別の定義をするが, 偶ラテン方陣と奇ラテン方陣の個数の比較を考える上では問題ない. 詳しくは次章で述べる.

7　ラテン方陣の符号

前章でラテン方陣の符号を定めたが, これは印符号とよばれるものであり, 通常採用するラテン方陣の符号はこれとは異なる（通常は後述する行符号と列符号の積で定める）. しかし, ラテン方陣の符号をどちらで定めても Alon–Tarsi 予想を考える上では問題ない. この章ではこのことを説明する. この章の内容は Janssen の論文 [J] からの引用である.

7.1　行符号, 列符号, 印符号

この節ではラテン方陣における行符号, 列符号, 印符号を定める.
まずラテン方陣から $[n]^3$ の部分集合が自然に定まる.

定義 7.1.1. $\Lambda = (\lambda_{ij})_{1\leq i,j\leq n} \in \mathrm{LS}(n)$ に対して, N_Λ を次のように定める.

$$N_\Lambda = \{(i,j,k) \in [n]^3 \mid \lambda_{ij} = k\}.$$

この i,j,k のうち 2 つを固定すると, $(i,j,k) \in N_\Lambda$ をみたす残りの 1 つが一意に定まる, つまり次の命題が成立することはすぐわかる.

命題 7.1.2. $\Lambda = (\lambda_{ij})_{1\leq i,j\leq n} \in \mathrm{LS}(n)$ に対して, 次の 3 つの写像はどれも全単射である.

$$r\Phi_\Lambda : [n]^2 \longrightarrow N_\Lambda, \quad (j,k) \longmapsto (i,j,k) \quad (\text{ただし}, i \text{ は } \lambda_{ij} = k \text{ をみたす}).$$
$$c\Phi_\Lambda : [n]^2 \longrightarrow N_\Lambda, \quad (i,k) \longmapsto (i,j,k) \quad (\text{ただし}, j \text{ は } \lambda_{ij} = k \text{ をみたす}).$$
$$s\Phi_\Lambda : [n]^2 \longrightarrow N_\Lambda, \quad (i,j) \longmapsto (i,j,k) \quad (\text{ただし}, k \text{ は } \lambda_{ij} = k \text{ をみたす}).$$

次の定理は実質的にこの命題の言い換えである.

定理 7.1.3. $\Lambda = (\lambda_{ij})_{1\leq i,j\leq n} \in \mathrm{LS}(n)$ とする.

(1) ある $\tau_1, \ldots, \tau_n \in S_n$ が一意に存在して, 任意の $i,j,k \in [n]$ に対して

$$\lambda_{ij} = k \iff \tau_i(j) = k.$$

(2) ある $\rho_1, \ldots, \rho_n \in S_n$ が一意に存在して, 任意の $i,j,k \in [n]$ に対して

$$\lambda_{ij} = k \iff \rho_j(i) = k.$$

(3) ある $\sigma_1, \ldots, \sigma_n \in S_n$ が一意に存在して, 任意の $i,j,k \in [n]$ に対して

$$\lambda_{ij} = k \iff \sigma_k(i) = j.$$

注意 7.1.4. この $\tau_1, \ldots, \tau_n$ を Λ から定まる行置換という．また $\rho_1, \ldots, \rho_n$ を Λ から定まる列置換, $\sigma_1, \ldots, \sigma_n$ を Λ から定まる印置換という．6.4 節で述べた $\mathrm{LS}(n)$ と $\mathrm{P}(L'(n))$ の同一視の下では, 印置換 $\sigma_1, \ldots, \sigma_n$ は命題 6.4.1 の $\sigma_1, \ldots, \sigma_n$ と一致する．

これらの置換を用いてラテン方陣の行符号, 列符号, 印符号を定める．

定義 7.1.5. $\Lambda \in \mathrm{LS}(n)$ に対して $\mathrm{rsgn}\,\Lambda, \mathrm{csgn}\,\Lambda, \mathrm{ssgn}\,\Lambda$ をそれぞれ次で定める．

$$\mathrm{rsgn}\,\Lambda = \prod_{i=1}^{n} \mathrm{sgn}\,\tau_i, \qquad \mathrm{csgn}\,\Lambda = \prod_{i=1}^{n} \mathrm{sgn}\,\rho_j, \qquad \mathrm{ssgn}\,\Lambda = \prod_{k=1}^{n} \mathrm{sgn}\,\sigma_k.$$

これらをそれぞれ Λ の行符号, 列符号, 印符号とよぶ．また行符号と列符号の積を $\mathrm{rcsgn}\,\Lambda = \mathrm{rsgn}\,\Lambda\,\mathrm{csgn}\,\Lambda$ とかく．

7.2 行符号と列符号の積と印符号の関係

この節では $\Lambda \in \mathrm{LS}(n)$ に対して $\mathrm{rcsgn}\,\Lambda$ と $\mathrm{ssgn}\,\Lambda$ に次の関係があることを示そう．

定理 7.2.1. $\Lambda \in \mathrm{LS}(n)$ に対して, 次の等式がなりたつ．

$$\mathrm{rcsgn}\,\Lambda = \varepsilon(n)\,\mathrm{ssgn}\,\Lambda.$$

ただし,

$$\varepsilon(n) = \begin{cases} 1 & (n \equiv 0, 1 \pmod 4) \\ -1 & (n \equiv 2, 3 \pmod 4). \end{cases}$$

と定める．

注意 7.2.2. 通常は単にラテン方陣 Λ の符号と言えば $\mathrm{rcsgn}\,\Lambda$ を指す．しかし, 6.4 節では $\mathrm{ssgn}\,\Lambda$ をラテン方陣の符号と呼んで議論していた．だが, この定理 7.2.1 からラテン方陣の符号をどちらで定義しても偶ラテン方陣と奇ラテン方陣が入れ替わる可能性があるが, これらの個数の差を考える上では問題ない．

以下の定理 7.2.1 の証明は [J] をまとめ直したものである．

証明に必要な記号や命題をいくつか用意する．まず置換に対してその転倒数を次で定める．

定義 7.2.3. $\sigma \in S_n$ に対して非負整数 $\mathrm{Inv}\,\sigma$ を次で定める．

$$\mathrm{Inv}\,\sigma = |\{(i, j) \in [n] \times [n] \mid i < j, \sigma(i) > \sigma(j)\}|.$$

この転倒数を用いて置換の符号は次のように表せる.

命題 7.2.4. $\sigma \in S_n$ に対して, 次がなりたつ.

$$\operatorname{sgn}\sigma = (-1)^{\operatorname{Inv}\sigma}.$$

3 つの関係演算子から定まる N_Λ^2 の部分集合を考える.

定義 7.2.5. 関係演算子 $\sim_1, \sim_2, \sim_3$ に対して, N_Λ^2 の部分集合 $N_\Lambda^2(\sim_1, \sim_2, \sim_3)$ を次で定める.

$$N_\Lambda^2(\sim_1, \sim_2, \sim_3) = \{((i,j,k),(i',j',k')) \in N_\Lambda^2 \mid i \sim_1 i', j \sim_2 j', k \sim_3 k'\}.$$

とくに演算子が空白のときは関係を要求しないものとする. たとえば, $N_\Lambda^2(\quad, <, >)$ は次のようになる.

$$N_\Lambda^2(\quad, <, >) = \{((i,j,k),(i',j',k')) \in N_\Lambda^2 \mid j < j', k > k'\}.$$

定理 7.2.1 は次の補題に帰着される.

補題 7.2.6. $L \in \mathrm{LS}(n)$ に対して, 次がなりたつ.

$$\begin{aligned}
\sum_{i=1}^{n} \operatorname{Inv}\tau_i &= \binom{n}{2}^2 - |N_\Lambda^2(<,<,>)| - |N_\Lambda^2(>,<,>)|, \\
\sum_{j=1}^{n} \operatorname{Inv}\rho_j &= \binom{n}{2}^2 - |N_\Lambda^2(<,<,>)| - |N_\Lambda^2(<,>,>)|, \\
\sum_{k=1}^{n} \operatorname{Inv}\sigma_k &= \binom{n}{2}^2 - |N_\Lambda^2(<,>,<)| - |N_\Lambda^2(<,>,>)|.
\end{aligned}$$

ただし, $\binom{n}{2}$ は二項係数を表す. つまり

$$\binom{n}{2} = \frac{n!}{2!(n-2)!}$$

である.

定理 7.2.1 の証明. 補題 7.2.6 を認めて定理 7.2.1 を示そう. 命題 7.2.4 より次がわかる.

$$\begin{aligned}
\operatorname{rcsgn}\Lambda \operatorname{ssgn}\Lambda &= \operatorname{rsgn}\Lambda \operatorname{csgn}\Lambda \operatorname{ssgn}\Lambda \\
&= (-1)^{\sum_{i=1}^n \operatorname{Inv}\tau_i} + (-1)^{\sum_{j=1}^n \operatorname{Inv}\rho_j} + (-1)^{\sum_{k=1}^n \operatorname{Inv}\sigma_k} \\
&= (-1)^{\sum_{i=1}^n \operatorname{Inv}\tau_i + \sum_{j=1}^n \operatorname{Inv}\rho_j + \sum_{k=1}^n \operatorname{Inv}\sigma_k}.
\end{aligned}$$

補題 7.2.6 より次の等式がなりたつ.

$$\sum_{i=1}^{n} \mathrm{Inv}\,\tau_i + \sum_{j=1}^{n} \mathrm{Inv}\,\rho_j + \sum_{k=1}^{n} \mathrm{Inv}\,\sigma_k \\ = 3\binom{n}{2}^2 - 2|N_\Lambda^2(<,<,>)| - 2|N_\Lambda^2(<,>,<)| - 2|N_\Lambda^2(<,>,>)|.$$

ここで $|N_\Lambda^2(<,>,<)| = |N_\Lambda^2(>,<,>)|$ であることを用いた. あとは $\binom{n}{2}$ が $n \equiv 0,1 \pmod 4$ のとき偶数, $n \equiv 2,3 \pmod 4$ のとき奇数であることを確認すれば定理 7.2.1 を得る. □

この補題 7.2.6 は次の 3 つの補題からすぐわかる.

補題 7.2.7. $\Lambda \in \mathrm{LS}(n)$ に対して, 次がなりたつ.

$$N_\Lambda^2(\quad,<,>) = N_\Lambda^2(=,<,>) \sqcup N_\Lambda^2(<,<,>) \sqcup N_\Lambda^2(>,<,>),$$
$$N_\Lambda^2(<,\quad,>) = N_\Lambda^2(<,=,>) \sqcup N_\Lambda^2(<,<,>) \sqcup N_\Lambda^2(<,>,>),$$
$$N_\Lambda^2(<,>,\quad) = N_\Lambda^2(<,>,=) \sqcup N_\Lambda^2(<,>,<) \sqcup N_\Lambda^2(<,>,>),$$

補題 7.2.8. $L \in \mathrm{LS}(n)$ に対して, 次がなりたつ.

$$\sum_{i=1}^{n} \mathrm{Inv}\,\tau_i = |N_\Lambda^2(=,<,>)|,$$
$$\sum_{j=1}^{n} \mathrm{Inv}\,\rho_j = |N_\Lambda^2(<,=,>)|,$$
$$\sum_{k=1}^{n} \mathrm{Inv}\,\sigma_k = |N_\Lambda^2(<,>,=)|.$$

補題 7.2.9. $L \in \mathrm{LS}(n)$ に対して, 次がなりたつ.

$$|N_\Lambda^2(\quad,<,>)| = \binom{n}{2}^2, \quad |N_\Lambda^2(<,\quad,>)| = \binom{n}{2}^2, \quad |N_\Lambda^2(<,>,\quad)| = \binom{n}{2}^2.$$

補題 7.2.7 は明らか. 補題 7.2.8 を示す.

補題 7.2.8 の証明. この補題 7.2.8 の第 1 の等式のみを証明する. 第 2, 第 3 の等式は第 1 の等式と同様に示せる. $s = 1, \ldots, n$ を固定して, 次のような N_Λ の部分集合を考える.

$$N_\Lambda^{(s)} = \{(i,j,k) \in N_\Lambda \mid i = s\}.$$

すると

$$N_\Lambda = \bigsqcup_{s=1}^{n} N_\Lambda^{(s)}$$

がなりたつ. このとき, $[n]$ と $N_\Lambda^{(s)}$ は次の対応で同一視できる.

$$[n] \to N_\Lambda^{(s)}, \quad j \mapsto (s, j, \tau_s(j)).$$

この対応で j, j' はそれぞれ $I^{(s)} = (s, j, k), I'^{(s)} = (s, j', k')$ に対応するとする.

$$j \mapsto I^{(s)} = (s, j, k), \quad j' \mapsto I'^{(s)} = (s, j', k').$$

このとき, j, j' に「$j < j', \tau_s(j) > \tau_s(j')$」がなりたつことと I, I' に「$j < j', k > k'$」がなりたつのは同値である. よって, 次の等式がなりたつ.

$$\begin{aligned} \operatorname{Inv} \tau_s &= |\{(j, j') \in [n] \times [n] \mid j < j', \tau_s(j) > \tau_s(j')\}| \\ &= |\{(I^{(s)}, I'^{(s)}) \in N_\Lambda^{(s)} \times N_\Lambda^{(s)} \mid j < j', k > k'\}|. \end{aligned}$$

言い換えると,

$$I = (i, j, k), \quad I' = (i', j', k') \in N_\Lambda$$

のという組のうち

$$i = i' = s, \quad j < j', \quad k > k'$$

をみたすものの個数が $\operatorname{Inv} \tau_s$ である. s を 1 から n まで動かして和をとれば次の等式を得る.

$$\begin{aligned} \sum_{s=1}^{n} \operatorname{Inv} \tau_s &= |\{(I, I') \in N_\Lambda \times N_\Lambda \mid i = i', j < j', k > k'\}| \\ &= |N_\Lambda^2(=, <, >)|. \end{aligned}$$

□

次に補題 7.2.9 を示す.

補題 7.2.9 の証明. この補題 7.2.9 の第 1 の等式は次の計算でわかる. 次の等式がなり

たつ.

$$\begin{aligned}
|N_\Lambda^2(\quad,<,>)| &= |\{((i,j,k),(i',j',k')) \in N_\Lambda^2 \mid j<j', k>k'\}| \\
&= \sum_{(i,j,k)\in N_\Lambda} |\{(i',j',k') \in N_\Lambda \mid j<j', k>k'\}| \\
&= \sum_{(j,k)\in[n]^2} |\{(i',j',k') \in N_\Lambda \mid j<j', k>k'\}| \\
&= \sum_{(j,k)\in[n]^2} (n-j)(k-1) \\
&= \sum_{j\in[n]} (n-j) \sum_{k\in[n]} (k-1) \\
&= \binom{n}{2}^2.
\end{aligned}$$

ここでまず第 1 の等号は $N_\Lambda^2(\quad,<,>)$ の定義である. 次に第 2 の等号は (i,j,k) を固定したものの和で書き表している. また第 3 の等号は $[n]^2$ と N_Λ は $r\Phi_\Lambda$ で同一視できることからわかる. 最後に第 4 の等号は (j,k) を固定すると $j<j'$ をみたす j' は $n-j$ 個, $k>k'$ をみたす k' は $k-1$ 個であることからわかる.

第 2, 第 3 の等式は第 1 の等式と同様に示せる. □

したがって, ラテン方陣の符号を前章のように ssgn で定めても, 通常どおりに rcsgn で定めても偶方陣と奇方陣の個数の差を考える上では問題ない.

参考文献

[AT] N. Alon, M. Tarsi, *Colorings and orientations of graphs*, Combinatorica, 12 (1992), no. 2, 125–134.

[C] A. Cayley, *The theory of linear transformations*, The Cambrige Mathematical Journal, 4 (1845), 193–209.

[FM] B. Friedman, S. McGuinness, *The Alon–Tarsi conjecture: A perspective on the main results*, Discrete Mathematics, 342 (1845), no. 8, 2234–2253.

[CLO] D. Cox, J. Little, D. O'Shea（著）, 落合啓之, 示野信一, 西山亨, 室政和, 山本敦子（訳）,『グレブナー基底と代数多様体入門（上)』, シュプリンガー・フェアラーク東京株式会社, 2000.

[GKZ] I. M. Gelfand, M. M. Kapranov, A. V. Zelevinsky, Discriminents, resultants, and multidimentsional determinants, Birhkäuser, 1994.

[G1] D. G. Glynn, *The modular counterparts of Cayley's hyperdeterminants*, Bulletin of the Australian Mathematical Society, 57 (1998), no. 3, 479–492.

[G2] D. G. Glynn, *The conjectures of Alon–Tarsi and Rota in dimension prime minus one*, SIAM J. Discrete Math, 24 (2010), no. 2, 193–210.

[GW] R. Goodman, N. R. Wallach, Representations and invariants of the classical groups, Cambridge, 1998.

[J] J. C. M. Janssen, *On Even and odd latin squares*, Journal of Combinatorial Theory, Series A, 69 (1995), no. 1, 173–181.

[K1] 木本一史,「対称群上の帯球関数とリース行列式」, 数理解析研究所講究録, 2031 巻 (2017), 218–234.

[K2] 木本一史,「ラテン方陣に関する Alon–Tarsi 予想と対称群の帯球関数について」, 数理解析研究所講究録, 2039 巻 (2017), 193–210.

[K3] 木本一史,『レクチャー 離散数学 グラフの世界への招待』, サイエンス社, 2019.

[KN] 木村哲三, 新妻弘,『群・環・体 入門』, 共立出版, 1999.

[M] 松坂和夫,『代数系入門』, 岩波書店, 1976.

[N] 野海正敏,「立体行列」, 数理科学, 4 月号 (1995), 16–21.

[S] L. Schläfli, *Über die resultante eines systemes mehrer algebraischer gleichungen*, Denkschr. der Kaiserlicher Akad. der Wiss, math–neturwiss. Klasse, 4 Band, 1852; *Gesammelte abhandlungen*, Band 2, S. 9–112, Birkhäuser Verlag, Basel,

1953.

[SV] A. Shen, N. K. Vereshchagin, Basic set theory, American Mathematical Society, 2002.

[Y] 雪江明彦, 『代数学 2 環と体とガロア理論』, 日本評論社, 2010.