1の原始n乗根における
シューア多項式の値

鹿児島大学大学院 理工学研究科
数理情報科学専攻
日高　昌樹

2019年1月31日

序文

この修士論文では, 1 の原始 n 乗根におけるシューア多項式の値について考察し, 次の結果を与えた.

定理 I. 自然数 n が 2 以外の素因数を高々 2 個しかもたない $(*)$ とき, 任意の分割 λ に対して, $s_\lambda(\omega_1, \ldots, \omega_{\phi(n)}) \in \{1, 0, -1\}$ である. ここで, s_λ はシューア多項式, $\phi(n)$ はオイラー関数, $\omega_1, \ldots, \omega_{\phi(n)}$ は 1 の原始 n 乗根すべてである.

n の条件 $(*)$ は比較的ゆるく, たとえば 105 未満の自然数 n はこれを満たす. また, 分割 λ には条件がない. 非常に多くの自然数 n と分割 λ に対してこの値が 3 つにしかならないというのは面白い現象である.

実はこの定理は, 2 系列の特別な分割に対してはすでに知られている結果である.

1 つは $\lambda = (1, 1, \ldots, 1)$ という分割の場合である. この場合は対応するシューア多項式は基本対称式である. 1 の原始 n 乗根たちの基本対称式は要するに n 次の円分多項式 $\Phi_n(x)$ の係数である. つまり, この場合は, 定理 I は「n が $(*)$ の条件を満たすとき, $\Phi_n(x)$ の係数には $1, 0, -1$ しか現れない」と言い換えられる. これは有名な事実であり, 100 年以上前に, A. Migotti が [Mi] で証明を与えている.

もう 1 つは $\lambda = (k)$ という分割の場合である. この場合は対応するシューア多項式は完全斉次対称式である. 1 の原始 n 乗根たちの完全斉次対称式は要するに n 次の円分多項式の逆数 $\Phi_n(x)^{-1}$ の係数である. つまり, この場合は, 定理 I は「n が $(*)$ の条件を満たすとき, $\Phi_n(x)^{-1}$ の係数には $1, 0, -1$ しか現れない」と言い換えられる. これは比較的最近の 2009 年に P. Moree [Mo] が与えた結果にあたる.

定理 I は, これらの既知の結果を一般の分割に拡張したものといえる. つまり, 基本対称式と完全斉次対称式の場合の結果を一般のシューア多項式に拡張したことになる.

証明について述べる. 定理 I は線型代数の定理に帰着させて証明する. 鍵となるのはベクトル空間 V の部分集合 X についての次の性質である (この条件を満たすとき, X は V において性質 (C) をもつという).

(C) V の基底となる $S \subset X$ に対して S に対応する行列式の値は (符号を除いて) S によらず一定となる.

定理 I はこの性質 (C) に関する次の 3 つの定理に帰着させて証明する. まず, 定理 I を定理 II に帰着させ, さらに定理 II は定理 III に帰着させる. そして定理 III は定理 IV というより一般的な形で証明するのである.

定理 II. n が $(*)$ の条件を満たすとき, 1 の n 乗根全体の集合 Z_n は $\mathbb{Q}(\zeta_n)$ において性質 (C) をもつ (ただし, ζ_n は 1 の原始 n 乗根とする).

定理 III. (1) 素数 p に対し, Z_p は $\mathbb{Q}(\zeta_p)$ において性質 (C) をもつ.

(2) 異なる奇素数 p, q に対し, $Z_p \otimes Z_q = \{a \otimes b \mid a \in Z_p, b \in Z_q\}$ は $\mathbb{Q}(\zeta_p) \otimes \mathbb{Q}(\zeta_q)$ において性質 (C) をもつ.

定理 IV. (1) ベクトル空間 V の基本零和系 X は V において性質 (C) をもつ.

(2) X, Y をそれぞれベクトル空間 V, W の基本零和系とすると, $X \otimes Y = \{x \otimes y \mid x \in X, y \in Y\}$ は $V \otimes W$ において性質 (C) をもつ.

ここで, m 次元ベクトル空間 V の $m+1$ 点集合で, V を張り, 和が 0 となるものを基本零和系とよんでいる.

まず, 定理 I は以下のようにして定理 II に帰着される. $k = 0, 1, \ldots$ に対し, 次数 $\phi(n)$ の数ベクトル u_k を

$$u_k = \begin{pmatrix} \omega_1^k \\ \vdots \\ \omega_{\phi(n)}^k \end{pmatrix}$$

と定め, $u_{k+n} = u_k$ であることに注意して, $\Omega_n = \{u_0, \ldots, u_{n-1}\}$ とおく. 問題の値 $s_\lambda(\omega_1, \ldots, \omega_{\phi(n)})$ は

$$s_\lambda(\omega_1, \ldots, \omega_{\phi(n)}) = \frac{\det(u_{\lambda_1+\phi(n)-1}, u_{\lambda_2+\phi(n)-2}, \ldots, u_{\lambda_{\phi(n)}+0})}{\det(u_{\phi(n)-1}, u_{\phi(n)-2}, \ldots, u_0)}$$

とかける (ただし, $\lambda = (\lambda_1, \ldots, \lambda_{\phi(n)})$ である). 右辺は Ω_n の元を列とする行列式の比だが, 分母は λ に依存せず, 分子のみが λ によって Ω_n の元の選び方が変わっている. よって, 定理 I は「Ω_n の元を列とする行列式の値が, Ω_n の元の選び方によらず, 符号を除いて一定または 0 である」つまり「Ω_n が性質 (C) をもつ」と言い換えられる. さらに, Ω_n の張るベクトル空間は自然に $\mathbb{Q}(\zeta_n)$ と同一視できるが, この同一視で Ω_n は Z_n と対応する. よって, 定理 I は定理 II のように「Z_n が性質 (C) をもつ」と言い換えられるのである.

次に定理 II は以下のようにして定理 III に帰着される. 鍵となるのは, n が $n = p_1^{l_1} \cdots p_k^{l_k}$ と素因数分解されるとき, $\mathbb{Q}(\zeta_n)$ は $\mathbb{Q}(\zeta_{p_1}) \otimes \cdots \otimes \mathbb{Q}(\zeta_{p_k})$ の直和と自然に同型

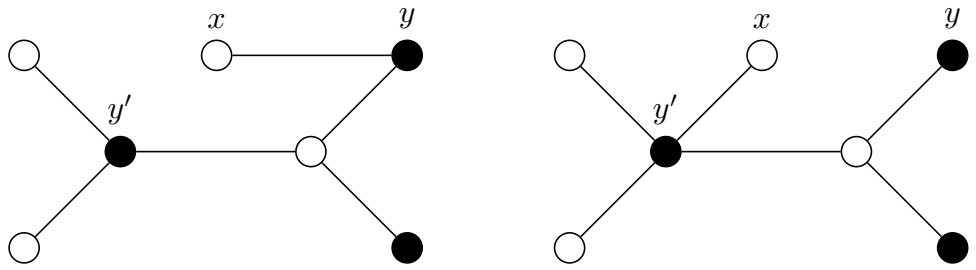
になることである．このとき, Z_n の像は

$$Z_{p_1} \otimes \cdots \otimes Z_{p_k} = \{z_1 \otimes \cdots \otimes z_k \mid z_i \in Z_{p_i}\}$$

の和集合となる．この事実と, 性質 (C) がベクトル空間の直和を取る操作などで保たれることを合わせると, 定理 II は $n = p, pq$ の場合に帰着できる．つまり, 定理 III のように Z_p と $Z_p \otimes Z_q$ が性質 (C) をもつことを示せばよい．

そしてこの定理 III は定理 IV の特別なケースとみなせる．実際 Z_p は $\mathbb{Q}(\zeta_p)$ の基本零和系である．

結局, 定理 IV を示せばよいことになったわけだが, (1) の証明は非常に易しい．(2) の証明は (1) と比べると難しいが, グラフ理論を用いて証明できる．具体的には, $X \otimes Y$ の部分集合を二部グラフと同一視し, 二部グラフにある種の同値関係を定めることで証明する．これは, グラフの葉に対し, 葉を端点とする辺を, 同じ葉を端点とする別の辺に取り換える操作で得られるものを同値とする同値関係である．例えば, 次の二つのグラフは同値になる．



実際, 左のグラフにおいて葉 x に注目して, 辺 xy を xy' に取り換えたものが右のグラフである．この同値関係に関して二部グラフの木はすべて互いに同値になる (定理 3.2.11) のだが, これは定理 IV (2) の言い換えである．このグラフ理論の定理の形で, 定理 IV (2) は証明される．

注意． 3 つの基本零和系のテンソル積は性質 (C) を満たすとは限らない (2 次元, 4 次元, 6 次元ベクトル空間の基本零和系のテンソル積が反例となる)．定理 IV (2) から, 性質 (C) はベクトル空間のテンソル積を取る操作でも保たれそうな気がするが, そうではない．

定理 I の証明に至った経緯を述べる．修士 1 年で, 円分体と円分多項式について学んでいた．そのとき読んだ論文, R. Thangadurai [T] で, 「n が $(*)$ の条件を満たすとき, n 次円分多項式の係数が $1, 0, -1$ のいずれか」であることを知った．また, n を大きくすると, いずれはすべての整数が円分多項式の係数に現れることも知った．円分多項式の係数は,

1 の原始 n 乗根における基本対称式の値だから, 完全斉次対称式でも同様の性質はないかと考え, 研究を始めた. しかし, これはすでに P. Moree [Mo] で与えられた結果があることを知った. そこでシューア多項式ではどうかと考え, いくつか計算して見ると, やはり $1, 0, -1$ しか出てこなかったため, 本格的に証明しようとした.

はじめは, 基本対称式と完全斉次対称式の結果から, ヤコビ・トゥルーディー公式を用いてシューア多項式の結果を導こうとした. しかし, これはうまくはいかなかった ($n = p$ や $n = p^l$ のときはうまくいったが, $n = pq$ のときに計算が難しくなった). そこで, シューア多項式の定義に戻ったところ, うまくいった. 証明にグラフ理論を用いることになったのは面白い.

謝辞

伊藤稔先生には学部 4 年次から 3 年間, 熱心で丁寧な指導をしていただきました. また, 学内セミナーや学会発表においては, スライド作りから発表練習まで, 指導していただきました. 心より感謝申し上げます. また, 学部, 大学院を通して指導してくださった数理情報科学科の先生方, ともに過ごした同期の方々に感謝します.

目 次

1　準備

この章では, 定理 I の主張で出てきた概念を説明し, さらに円分体の基本的性質について述べる. 1.1 節ではシューア多項式を定義し, 基本対称式, 完全斉次対称式との関係を述べる. 1.2 節では 1 の原始 n 乗根とその個数を表すオイラー関数を導入し, その性質をまとめる. 1.3 節では, 円分体の $\mathbb{Q}$ 上のベクトル空間としての次元と, $\mathbb{Q}$ 上の自己同型写像について述べる.

1.1　シューア多項式

この節では I. G. Macdonald [Ma] をもとに, シューア多項式を定義し, 基本対称式, 完全斉次対称式との関係を述べる.

シューア多項式は分割に対して定義される対称多項式だから, まず分割を定義する.

定義 1.1.1. 非負整数の組 $\lambda = (\lambda_1, \ldots, \lambda_l)$ が $\lambda_1 \geq \cdots \geq \lambda_l$ を満たすとき, λ を分割といい, 0 でない λ_i の個数を λ の深さという.

注意 1.1.2. 途中から 0 が並ぶ分割 $(\lambda_1, \ldots, \lambda_l, 0, \ldots, 0)$ は分割 $(\lambda_1, \ldots, \lambda_l)$ と同一視する.

分割 λ に対し, 交代式 $a_\lambda(x_1, \ldots, x_l)$ を定義する.

定義 1.1.3. 深さ l 以下の分割 $\lambda = (\lambda_1, \ldots, \lambda_l)$ に対し, 交代式 $a_\lambda(x_1, \ldots, x_l)$ を

$$a_\lambda(x_1, \ldots, x_l) = \det(x_i^{\lambda_j})_{1 \leq i,j \leq l} = \det \begin{pmatrix} x_1^{\lambda_1} & \cdots & x_1^{\lambda_l} \\ \vdots & \ddots & \vdots \\ x_l^{\lambda_1} & \cdots & x_l^{\lambda_l} \end{pmatrix}$$

と定める.

例えば, $\delta = (l-1, l-2, \ldots, 1, 0)$ に対し, 交代式 $a_\delta(x_1, \ldots, x_l)$ はヴァンデルモンド行列式である. この交代式でシューア多項式を定義する.

定義 1.1.4. 深さ l 以下の分割 $\lambda = (\lambda_1, \ldots, \lambda_l)$ に対して,

$$s_\lambda(x_1, \ldots, x_l) = \frac{a_{\lambda+\delta}(x_1, \ldots, x_l)}{a_\delta(x_1, \ldots, x_l)}$$

を λ に対応するシューア多項式という. ここで, $\lambda+\delta=(\lambda_1+l-1,\lambda_2+l-2,\ldots,\lambda_l+0)$ とする.

右辺の分母はヴァンデルモンド行列式で, 分子は交代式だからこの分数は割り切れる. したがって $s_\lambda(x_1,\ldots,x_l)$ は対称多項式である.

基本対称式, 完全斉次対称式はシューア多項式の一例である. これを述べるためにまず, 基本対称式, 完全斉次対称式の定義を思い出しておく.

定義 1.1.5. (1) 整数 k $(0\leq k\leq l)$ に対し

$$e_k(x_1,\ldots,x_l)=\sum_{1\leq i_1<\cdots<i_k\leq l}x_{i_1}\cdots x_{i_k}$$

を k 次基本対称式という.

(2) 整数 $k\geq 0$ に対し

$$h_k(x_1,\ldots,x_l)=\sum_{1\leq i_1\leq\cdots\leq i_k\leq l}x_{i_1}\cdots x_{i_k}$$

を k 次完全斉次対称式という.

k 次基本対称式, k 次完全斉次対称式はそれぞれ分割 $(\underbrace{1,\ldots,1}_{k\text{ 個}}),(k)$ に対応するシューア多項式と一致する.

例 1.1.6. (1) 非負整数 k に対して $\lambda=(\underbrace{1,\ldots,1}_{k\text{ 個}})$ のとき,

$$s_\lambda(x_1,\ldots,x_l)=e_k(x_1,\ldots,x_l).$$

(2) 非負整数 k に対して $\lambda=(k)$ のとき,

$$s_\lambda(x_1,\ldots,x_l)=h_k(x_1,\ldots,x_l).$$

1.2 1 の原始 n 乗根とオイラー関数

この節では雪江明彦 [Y] をもとに, 1 の原始 n 乗根についてまとめる. 1 の原始 n 乗根の個数は n と互いに素な n 未満の自然数の個数に一致する. この個数をオイラー関数 $\phi(n)$ という. このオイラー関数の性質についてもあわせてまとめる. 以下, n を自然数とする.

定義 1.2.1. n 乗して初めて 1 になる複素数を 1 の原始 n 乗根という.

例 1.2.2. 小さい n について 1 の原始 n 乗根の例を見せる.
$n=1$ のとき, 1 の n 乗根は 1 のみであり, これは 1 の原始 1 乗根である. $n=2$ のとき, 1 の 2 乗根は $1,-1$ の 2 つだが, 原始 2 乗根は -1 のみである. $n=3$ のとき, 1 の 3 乗根は 3 つあるが, そのうち原始 3 乗根は $\frac{-1+\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2}$ である. $n=4$ のとき, 1 の 4 乗根は 4 つあるが, そのうち原始 4 乗根は $\sqrt{-1}, -\sqrt{-1}$ のみである.

一般に 1 の n 乗根は $e^{\frac{2\pi i}{n}k}$ とかける. これが 1 の原始 n 乗根であるかどうかは k と n が互いに素であるかどうかで判定できる.

命題 1.2.3. 次は同値.
(1) $e^{\frac{2\pi i}{n}k}$ は 1 の原始 n 乗根.
(2) k, n は互いに素.

この命題より, 1 の原始 n 乗根の個数は n と互いに素な n 未満の自然数の個数に一致する. この個数を $\phi(n)$ と定め, オイラー関数という. つまり, オイラー関数は次で定められる.

定義 1.2.4. 自然数 n に対し, $\phi(n)$ を

$$\phi(n) = \begin{cases} 1, & n=1, \\ |(\mathbb{Z}/n\mathbb{Z})^\times|, & n>1 \end{cases}$$

と定め, オイラー関数という.

次の命題は中国剰余定理からすぐにわかる.

命題 1.2.5. m, n が互いに素ならば $\phi(mn) = \phi(m)\phi(n)$.

最後に $\phi(n)$ の例を見せる.

例 1.2.6. $\phi(1)=1, \phi(2)=1, \phi(4)=2$.
一般に p が素数なら, $k>0$ に対し, $\phi(p^k) = p^{k-1}(p-1)$ である.

1.3 円分体 $\mathbb{Q}(\zeta_n)$

1 の原始 n 乗根 ζ_n を $\mathbb{Q}$ に添加した体 $\mathbb{Q}(\zeta_n)$ は円分体とよばれる. この節では, [Y] をもとに $\mathbb{Q}(\zeta_n)$ が $\mathbb{Q}$ 上の $\phi(n)$ 次元ベクトル空間になることを述べる. また, $\mathbb{Q}(\zeta_n)$ の $\mathbb{Q}$ 上

の同型写像について述べる. これらは 4.3 節と 4.4 節で必要となる.

次元について述べるうえで, 円分多項式が鍵となる. よって, まずは円分多項式を定義する.

定義 1.3.1. 自然数 n に対し, 多項式

$$\Phi_n(x) = (x - \omega_1) \cdots (x - \omega_{\phi(n)})$$

を n 次の円分多項式という. ここで, $\omega_1, \ldots, \omega_{\phi(n)}$ は 1 の原始 n 乗根すべてである.

いくつか例を見せる.

例 1.3.2.

$$\begin{aligned}
\Phi_1(x) &= x - 1, \\
\Phi_2(x) &= x + 1, \\
\Phi_3(x) &= x^2 + x + 1, \\
\Phi_4(x) &= x^2 + 1, \\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1, \\
\Phi_{15}(x) &= x^8 - x^7 + x^5 - x^4 + x^3 - x + 1, \\
\Phi_{100}(x) &= x^{40} - x^{30} + x^{20} - x^{10} + 1.
\end{aligned}$$

一般に, 素数 p に対し $\Phi_p(x) = x^{p-1} + \cdots + x + 1$ である. これは,

$$x^p - 1 = (x - 1)(x^{p-1} + \cdots + x + 1)$$

と 1 の p 乗根は 1 を除いてすべて原始 p 乗根であることからわかる.

$\mathbb{Q}$ 上のベクトル空間 $\mathbb{Q}(\zeta_n)$ の次元について述べる. 鍵となるのは次の 2 つの定理である.

定理 1.3.3. L/K を代数拡大, $f(x)$ を $\alpha \in L$ の最小多項式で, $\deg f(x) = m$ とする. このとき, $K(\alpha)$ は K 上 m 次元ベクトル空間である.

定理 1.3.4 ([Y] 命題 4.7.11)**.** 円分多項式 $\Phi_n(x)$ は ζ_n の $\mathbb{Q}$ 上の最小多項式である.

これらの定理を合わせると, 円分体 $\mathbb{Q}(\zeta_n)$ は $\mathbb{Q}$ 上 $\phi(n)$ 次元ベクトル空間であることがわかる.

定理 1.3.3 は [Y] 命題 3.1.23 をこの節の内容に合わせて書き換えたもので, 証明は必要な命題は多いが難しくはない. 定理 1.3.4 の証明は定理 1.3.3 よりは難しく, $\Phi_n(x)$ が整数

係数であることが鍵である. $\Phi_n(x)$ が整数係数であることはガロアの基本定理を用いて証明される.

次に $\mathbb{Q}(\zeta_n)$ の $\mathbb{Q}$ 上の体としての自己同型写像を考える.

定理 1.3.5. $i = 1, 2, \ldots, \phi(n)$ に対し, $\mathbb{Q}$ 上の体の同型写像 $f_i : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$ で

$$f_i(\zeta_n) = \omega_i$$

となるものが存在する.

これは定理 1.3.4 と次の命題からわかる.

命題 1.3.6 ([Y] 命題 3.1.32 (2))**.** L/K を代数拡大, $\alpha \in L$ の K 上の最小多項式を $f(x)$ とする. $\beta \in L$ が $f(\beta) = 0$ を満たすとき, K 上の体の同型写像 $K(\alpha) \to K(\beta)$ で α が β に対応するものが存在する.

この命題の証明は易しい.

2　先行研究

序文で述べた通り, 定理 I はシューア多項式が基本対称式, 完全斉次対称式の場合についてはすでに知られていることである. この章ではこの先行研究をまとめる. これらの先行研究は, 円分多項式の性質に言い換えられるため, まず 2.1 節で円分多項式の性質をまとめる. 2.2 節, 2.3 節でそれぞれ基本対称式, 完全斉次対称式の場合についてまとめる.

2.1　円分多項式

シューア多項式が基本対称式, 完全斉次対称式の場合は, 円分多項式の性質を用いる. この節では, R. Thangadurai [T] をもとに, その性質をまとめる.

シューア多項式が基本対称式の場合は, 定理 I は円分多項式の係数の話に言い換えられる. まず, その説明をする. 以下, 円分多項式の k 次の係数を $a_n(k)$ とする. つまり, $\Phi_n(x) = \sum_{k=0}^{\phi(n)} a_n(k)x^k$ とする. $\omega_1, \ldots, \omega_{\phi(n)}$ を k 次の基本対称式に代入すると,

$$e_k(\omega_1, \ldots, \omega_{\phi(n)}) = \sum_{1 \le i_1 < \cdots < i_k \le \phi(n)} \omega_{i_1} \cdots \omega_{i_k}$$

となる. これは円分多項式 $\Phi_n(x)$ の $\phi(n) - k$ 次の係数に一致している. つまり,

$$e_k(\omega_1, \ldots, \omega_{\phi(n)}) = a_n(\phi(n) - k)$$

である. したがって, シューア多項式が基本対称式の場合は定理 I は円分多項式の係数の話に言い換えられる.

次の定理より, 3 次以上のすべての円分多項式は n が相異なる奇素数の積のものでかくことができる.

定理 2.1.1. (1) $n = p_1^{l_1} \cdots p_k^{l_k}$ ($p_1, \ldots, p_k$ は相異なる素数) を n の素因数分解, $N = p_1 \cdots p_k$ とする. このとき, $\Phi_n(x) = \Phi_N(x^{\frac{n}{N}})$.

(2) $n \ge 3$ を奇数とする. このとき, $\Phi_{2n}(x) = \Phi_n(-x)$.

この定理から円分多項式の係数について次がわかる.

系 2.1.2. (1) $a_n(k) = \begin{cases} a_N(\frac{k}{N}), & N \mid k, \\ 0, & \text{その他.} \end{cases}$

(2) $n \ge 3$ が奇数なら $a_{2n}(k) = (-1)^k a_n(k)$.

(1) より, $\Phi_n(x)$ の係数は n が平方因子をもたないときに帰着される. また (2) より, $n \geq 3$ が奇数なら, $\Phi_{2n}(x)$ の係数は, $\Phi_n(x)$ の係数に帰着される. これを合わせると, 円分多項式の係数は n が相異なる奇素数の積の場合の $\Phi_n(x)$ の係数に帰着される.

以下, 定理 2.1.1 を示すために必要な命題や関数を用意する. まず, $x^n - 1$ は円分多項式の積でかける. つまり, 次が成り立つ.

命題 2.1.3. $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

証明. 自然数 a に対し 1 の原始 a 乗根全体の集合を A_a とする. 以下, ζ_a を 1 の原始 a 乗根とする.

まず, $x^n - 1$ が $\prod_{d|n} \Phi_d(x)$ を割ることを示す. つまり, $k = 0, \ldots, n-1$ に対し, $\zeta_n^k \in A_d$ となる n の約数 d が存在することを示す. $\gcd(k, n) = a$ とする. すると $n = ad, k = ad'$ (d, d' は互いに素) とかける. $\zeta_n^k \in A_d$ を示す. いま,

$$\zeta_n^k = \zeta_{ad}^{ad'} = \zeta_d^{d'}$$

である. ここで, d, d' は互いに素なので, 命題 1.2.3 より, $\zeta_d^{d'} \in A_d$ である. よって, $\zeta_n^k \in A_d$ である.

次に $\prod_{d|n} \Phi_d(x)$ が $x^n - 1$ を割ることを示す. 1 の原始 d 乗根は, 1 の n 乗根なので, 各 $d \mid n$ に対し $\Phi_d(x)$ は $x^n - 1$ を割る. よって, n の異なる約数 a, b に対し, $\Phi_a(x)$ と $\Phi_b(x)$ が共通根を持たないことを示せばよい. つまり, a, b が異なるとき, $A_a \cap A_b = \emptyset$ を示せばよい. $a < b$ とし, $A_a \cap A_b \neq \emptyset$ とする. $\zeta \in A_a \cap A_b$ をとる. ζ は原始 b 乗根より, $k < b$ なら $\zeta^k \neq 1$ である. ところが ζ は 1 の原始 a 乗根より $\zeta^a = 1$ である. $a < b$ よりこれは矛盾である. □

次にメビウス関数を導入する.

定義 2.1.4. 次で定義される関数 $\mu : \mathbb{N} \to \mathbb{Z}$ をメビウス関数という.

$$\mu(n) = \begin{cases} 1, & n = 1, \\ (-1)^k, & n = p_1 \cdots p_k \ (p_1, \ldots, p_k \text{は相異なる素数}), \\ 0, & \text{その他}. \end{cases}$$

メビウス関数には次の性質がある.

命題 2.1.5. (1) m, n が互いに素なら $\mu(mn) = \mu(m)\mu(n)$.

(2) $\displaystyle\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1, \\ 0, & n \neq 1. \end{cases}$

証明. (1) 定義より明らか.

(2) $n = 1$ のとき,

$$\sum_{d|1} \mu(d) = \mu(1) = 1.$$

$n \neq 1$ のとき, 特に $n = p_1 \cdots p_k$ ($p_1, \ldots, p_k$は相異なる素数) のときを考えたらよい. このとき,

$$\begin{aligned}
\sum_{d|n} \mu(d) &= \sum_{i=0}^{k} \sum_{1 \leq l_1 < \ldots < l_i \leq k} \mu(p_{l_1} \cdots p_{l_i}) \\
&= \sum_{i=0}^{k} \binom{k}{i} (-1)^i \\
&= (1-1)^k \\
&= 0
\end{aligned}$$

である. □

円分多項式はメビウス関数を用いて $x^d - 1$ (d は n の約数) の積でかくことができる.

命題 2.1.6. $\Phi_n(x)$ はメビウス関数を用いて

$$\Phi_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)} = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}$$

とかける.

証明には次の補題を用いる.

補題 2.1.7. 自然数 n に対し, $\mathbb{N}$ 上の関数 f, g が

$$f(n) = \prod_{d|n} g(d)$$

を満たすとき,

$$g(n) = \prod_{d|n} f(\frac{n}{d})^{\mu(d)}$$

が成り立つ.

証明. $\prod_{d|n} f(\frac{n}{d})^{\mu(d)}$ を変形すると,

$$\begin{aligned}\prod_{d|n} f(\frac{n}{d})^{\mu(d)} &= \prod_{d|n}\left(\prod_{m|\frac{n}{d}} g(m)\right)^{\mu(d)} \\ &= \prod_{m|n}\left(\prod_{d|\frac{n}{m}} g(m)^{\mu(d)}\right) \\ &= \prod_{m|n} g(m)^{\sum_{d|\frac{n}{m}}\mu(d)} \\ &= g(n)\end{aligned}$$

である. 第 4 の等号では, 命題 2.1.5 (2) を用いた. □

命題 2.1.6 の証明. 補題 2.1.7 において, $g(n) = \Phi_n(x)$ かつ $f(n) = x^n - 1$ とすればよい. □

命題 2.1.6 を用いて定理 2.1.1 を示す.

定理 2.1.1 の証明. (1) $\Phi_n(x)$ を変形すると,

$$\begin{aligned}\Phi_n(x) &= \prod_{d|n}(x^{\frac{n}{d}} - 1)^{\mu(d)} \\ &= \prod_{d|N}(x^{\frac{n}{d}} - 1)^{\mu(d)} \\ &= \prod_{d|N}((x^{\frac{n}{N}})^{\frac{N}{d}} - 1)^{\mu(d)} \\ &= \Phi_N(x^{\frac{n}{N}})\end{aligned}$$

である. 第 2 の等号は μ の定義よりわかる (d が平方因子をもつとき, $\mu(d) = 0$ である).

(2) $\Phi_{2n}(x)$ を変形すると,

$$\begin{aligned}\Phi_{2n}(x) &= \prod_{d|(2n)}(x^d - 1)^{\mu(\frac{2n}{d})} \\ &= \prod_{d|n}(x^d - 1)^{\mu(\frac{2n}{d})}(x^{2d} - 1)^{\mu(\frac{2n}{2d})} \\ &= \prod_{d|n}(x^d - 1)^{\mu(\frac{2n}{d})}\left((x^d - 1)(x^d + 1)\right)^{\mu(\frac{n}{d})} \\ &= \prod_{d|n}(x^d - 1)^{\mu(\frac{2n}{d})+\mu(\frac{n}{d})}(x^d + 1)^{\mu(\frac{n}{d})}\end{aligned}$$

$$
\begin{aligned}
&= \prod_{d|n} (x^d + 1)^{\mu(\frac{n}{d})} \\
&= \prod_{d|n} (-x^d - 1)^{\mu(\frac{n}{d})} \\
&= \prod_{d|n} ((-x)^d - 1)^{\mu(\frac{n}{d})} \\
&= \Phi_n(-x)
\end{aligned}
$$

である. 第 5 の等号は 2 と $\frac{n}{d}$ が互いに素であるから $\mu(\frac{2n}{d}) = -\mu(\frac{n}{d})$ よりわかる. 第 6 の等号は d の取り方が偶数個であることよりわかる. 第 7 の等号は d が奇数であることよりわかる. □

2.2 基本対称式の場合

前節の議論から, 基本対称式に $\omega_1, \ldots, \omega_{\phi(n)}$ を代入した値は, $\Phi_n(x)$ の係数と言い換えられた. よって, シューア多項式が基本対称式の場合は, 定理 I は次の定理に言い換えられる.

定理 2.2.1. *n が 2 以外の素因数を高々 2 つしか持たないとき, $\Phi_n(x)$ の係数は $1, 0, -1$ のいずれかである.*

系 2.1.2 より, $n = p, pq$ の場合に $\Phi_n(x)$ の係数が $1, 0, -1$ であることを示せばよい. $n = p$ のときは, 例 1.3.2 よりすでにわかっている. よって, $n = pq$ の場合, つまり次を示せばよい.

定理 2.2.2. *$\Phi_{pq}(x)$ の係数は $1, 0, -1$ のいずれかである.*

これは A. Migotti [Mi] が初めて証明したが, その後もいくつかの証明が与えられている. この論文では, T. Y. Lam と K. H. Leung [LL] の手法で証明する.

$n = pq$ のとき, $\phi(n) = (p-1)(q-1)$ である. このとき, $\phi(n) = sp + tq$ を満たす整数 s, t が存在する. より強く, 次が成り立つ.

命題 2.2.3. *p, q を異なる素数とする. $sp + tq = (p-1)(q-1)$ を満たす整数 s, t で $0 \leq s \leq q-2$ かつ $0 \leq t \leq p-2$ であるものがただ一組存在する.*

これを示すために次の補題を示す.

補題 2.2.4. 互いに素な自然数 p, q と, 整数 r に対し, 不定方程式

$$px + qy = r$$

は整数解をもつ. その一組を (x_0, y_0) とすると一般解は $(x, y) = (x_0 + qt, y_0 - pt)$ $(t \in \mathbb{Z})$ で与えられる.

証明. ユークリッド互除法より, 解をもつことは明らか. (x, y) を解とすると,

$$px + qy = r, \quad px_0 + qy_0 = r$$

より,

$$p(x - x_0) = q(y_0 - y)$$

である. p, q は互いに素だから $x - x_0 = qt$ $(t \in \mathbb{Z})$ とかける. これをに代入すると,

$$pqt = q(y_0 - y)$$

すなわち $y = y_0 - pt$ である. □

これを用いて, 命題 2.2.3 を示す.

命題 2.2.3 の証明. 補題 2.2.4 より不定方程式 $px + qy = (p-1)(q-1)$ の一般解は一組の解 (x_0, y_0) と整数 t を用いて $(x_0 + qt, y_0 - pt)$ とかける. ここで $0 \leq x_0 + qt' \leq q - 1$ となる t' がただ 1 つとれる. すると $(x_0 - qt', y_0 + pt')$ が求めるものである. 以下これを示す. いま,

$$p(x_0 + qt') + q(y_0 - pq) = (p-1)(q-1)$$

より,

$$\begin{aligned} y + pt' &= \frac{1}{q}\left((p-1)(q-1) - p(x_0 - qt')\right) \\ &\geq \frac{1}{q}\left((p-1)(q-1) - p(q-1)\right) \quad (\because x_0 + qt' \leq q - 1) \\ &= \frac{1}{q}(1 - q) \\ &= \frac{1}{q} - 1 \\ &> -1 \end{aligned}$$

である. $y_0 + pt' \in \mathbb{Z}$ より, $y_0 + pt' \geq 0$. よって $0 \leq x_0 + qt' \leq q - 1$ かつ $0 \leq y_0 + pt'$ である.

あとは, $y_0 + pt' \leq p-2$ と $x_0 - qt' \leq q-2$ を示せばよい. 特に $y_0 + pt' \leq p-2$ を示す ($x_0 - qt' \leq q-2$ も同様にして証明できる). まず, $y_0 + pt' \leq p-1$ を示す. $y_0 + pt' > p-1$ とすると,

$$\begin{aligned} x - qt' &= \frac{1}{q}\left((p-1)(q-1) - (y_0 + pt')q\right) \\ &\geq \frac{1}{q}\left((p-1)(q-1) - pq\right) \\ &< 0 \end{aligned}$$

となり矛盾する. よって, $y_0 + pt' \leq p-1$. ここで, $y_0 + pt' = p-1$ とすると,

$$0 = p(x_0 - qt') + q(p-1) = p(x_0 + q - qt') - q$$

すなわち $q = p(x_0 + q - qt')$ である. q は素数であるからこれは矛盾である. よって, $y_0 + pt' \leq p-2$. □

定理 2.2.2 を証明するために, 補題を 1 つ用意する.

補題 2.2.5. $\phi(pq) = rp + sq$ $(0 \leq r \leq q-2,\ 0 \leq s \leq p-2)$ となる s, t をとると,

$$\Phi_n(x) = \left(\sum_{i=0}^{r} x^{ip}\right)\left(\sum_{j=0}^{s} x^{jq}\right) - \left(\sum_{i=r+1}^{q-1} x^{ip}\right)\left(\sum_{j=s+1}^{p-1} x^{jq}\right) x^{-pq}$$

とかける.

証明. ζ を 1 の原始 pq 乗根とする. このとき, ζ^q は 1 の原始 p 乗根, ζ^p は 1 の原始 q 乗根なので, $\Phi_p(\zeta^q) = \Phi_q(\zeta^p) = 0$ である. $\Phi_p(\zeta^q) = 0, \Phi_q(\zeta^p) = 0$ を式変形すると,

$$\sum_{i=0}^{r}(\zeta^p)^i = -\sum_{i=r+1}^{q-1}(\zeta^p)^i, \quad \sum_{j=0}^{s}(\zeta^q)^j = -\sum_{j=s+1}^{p-1}(\zeta^q)^j$$

である. これらを辺々掛け合わせて左辺にまとめると,

$$\left(\sum_{i=0}^{r}(\zeta^p)^i\right)\left(\sum_{j=0}^{s}(\zeta^q)^j\right) - \left(\sum_{i=r+1}^{q-1}(\zeta^p)^i\right)\left(\sum_{j=s+1}^{p-1}(\zeta^q)^j\right) = 0 \tag{2.2.1}$$

である. ここで,

$$f(x) = \left(\sum_{i=0}^{r}(x^p)^i\right)\left(\sum_{j=0}^{s}(x^q)^j\right), \quad g(x) = \left(\sum_{i=r+1}^{q-1}(x^p)^i\right)\left(\sum_{j=s+1}^{p-1}(x^q)^j\right) x^{-pq}$$

とおく. このとき, $g(x)$ の最低次数は

$$p(r+1)+q(s+1)-pq = rp+sq+p+q-pq = (p-1)(q-1)+p+q-pq = 1$$

である. $f(x)-g(x) = \Phi_{pq}(x)$ を示せばよい. $f(x)-g(x)$ が $\Phi_n(x)$ で割り切れることと, $\deg(f(x)-g(x)) = \deg \Phi_n(x)$ を示せばよい.

(2.2.1) より ζ が 1 の原始 n 乗根なら $f(\zeta)-g(\zeta)=0$ である. よって $f(x)-g(x)$ は 1 の原始 n 乗根すべてを根にもつ. つまり, $f(x)-g(x)$ は Φ_{pq} で割り切れる.

$\deg(f(x)-g(x)) = \deg \Phi_{pq}(x)$ を示す.

$$\begin{aligned}\deg f(x) &= rp+sq = (p-1)(q-1),\\ \deg g(x) &= p(q-1)+q(p-1)-pq\\ &= pq-p-q\\ &< (p-1)(q-1)\end{aligned}$$

より, $\deg(f(x)-g(x)) = (p-1)(q-1) = \deg \Phi_{pq}(x)$ である. □

これを用いて, 定理 2.2.2 を示す.

定理 2.2.2 の証明. 補題 2.2.5 より,

$$f(x) = \left(\sum_{i=0}^{r}(x^p)i\right)\left(\sum_{j=0}^{s}(x^q)^j\right), \quad g(x) = \left(\sum_{i=r+1}^{q-1}(x^p)i\right)\left(\sum_{j=s+1}^{p-1}(x^q)^j\right)x^{-pq}$$

を用いて $\Phi_n(x) = f(x)-g(x)$ とかける. まず, $f(x)$, $g(x)$ の係数がすべて 1 であることを示す. $f(x)$ について示す. $pi+qj = pi'+qj'$ $(0 \le i, i' \le r$ かつ $0 \le j, j' \le s)$ ならば, $i = i'$ かつ $j = j'$ であることを示せばよい. いま, $pi+qj = pi'+qj'$ より, $p(i-i') = q(j'-j)$ であり, p, q は互いに素なので $q \mid i-i'$ かつ $p \mid j'-j$ である. ここで, $0 \le i, i' \le r < q$ より $i-i' = 0$. つまり $i = i'$. 同様に, $j = j'$ である. $g(x)$ についても同様に示すことができる. よって, $f(x), g(x)$ の係数はすべて 1 である.

次に $f(x)$ と $g(x)$ に共通の次数の項が存在しないことを示す. 共通の次数の項が存在すると仮定する. つまり

$$pi+qj = pi'+qj'-pq$$

を満たす i, i', j, j' が存在すると仮定する. ただし,

$$0 \le i \le r, \quad 0 \le j \le s, \quad r+1 \le i' \le q-1, \quad s+1 \le j' \le p-1$$

である. すると,

$$pi+qj = pi'+qj'-pq$$

すなわち, $p(i-i'+q)=q(j'-j)$ より, $p \mid j'-j$ かつ $q \mid i-i'+q$. いま, $1 \leq j'-j \leq p-1$ より, $p \nmid j'-j$ となり矛盾する. よって, $f(x), g(x)$ には共通の次数の項は存在しない. したがって, $\Phi_{pq}(x)=f(x)-g(x)$ の係数はすべて $1, 0, -1$ のいずれかである. □

注意 2.2.6. $n=105=3\times5\times7$ は n が 2 でない素因数を 3 つもつ最小の自然数である. $\Phi_{105}(x)$ は次のように 41 次と 7 次の係数に -2 が現れることがわかっている.

$$\begin{aligned}\Phi_{105}(x) = {} & x^{48}+x^{47}+x^{46}-x^{43}-x^{42}-2x^{41}-x^{40}-x^{39}+x^{36} \\ & +x^{35}+x^{34}+x^{32}+x^{31}-x^{28}-x^{26}-x^{24}-x^{22}-x^{20}+x^{17} \\ & +x^{16}+x^{15}+x^{14}+x^{13}+x^{12}-x^{9}-x^{8}-2x^{7}-x^{6}-x^{5}+x^{2}+x+1.\end{aligned}$$

2.3 完全斉次対称式の場合

この節では, P. Moree [Mo] における, シューア多項式が完全斉次対称式の場合の先行研究をまとめる. $\omega_1, \ldots, \omega_{\phi(n)}$ を k 次の完全斉次対称式に代入すると,

$$h_k(\omega_1, \ldots, \omega_{\phi(n)}) = \sum_{1\leq i_1 \leq \cdots \leq i_k \leq \phi(n)} \omega_{i_1} \cdots \omega_{i_k}$$

となる. これは円分多項式の逆数 $\Phi_n(x)^{-1}$ の k 次の係数に一致する. つまり完全斉次対称式の場合は, $\Phi_n(x)^{-1}$ の係数を考えることになり, 定理 I は次の定理に言い換えられる.

定理 2.3.1. n が 2 以外の素因数を高々 2 つしかもたないとき, $\Phi_n(x)^{-1}$ の係数は $1, 0, -1$ のいずれかである.

証明は, 基本対称式の場合より易しい. $\Phi_n(x)^{-1}$ の係数を考えるためにまず, 多項式を 1 つ導入する.

定義 2.3.2. 自然数 n に対し, $\Psi_n(x)$ を

$$\Psi_n(x) = \frac{x^n-1}{\Phi_n(x)}$$

と定める.

円分多項式 $\Phi_n(x)$ は x^n-1 を割る (命題 2.1.3) ので, この $\Psi_n(x)$ は多項式である. $\Phi_n(x)^{-1}$ の係数は $\Psi_n(x)$ の係数に帰着される. 実際, $\Psi_n(x)$ を用いると, $\Phi_n(x)^{-1}$ は

$$\frac{1}{\Phi_n(x)} = -\frac{x^n-1}{\Phi_n(x)}\frac{1}{1-x^n} = -\Psi_n(x)(1+x^n+x^{2n}+\cdots)$$

とかける. また, $\deg(\Psi_n(x)) = n - \phi(n) < n$ より, $\Phi_n(x)^{-1}$ の係数には $-\Psi_n(x)$ の係数しか現れない.

$\Psi_n(x)$ の係数を考えるために $\Psi_n(x)$ の性質を考える. $\Phi_n(x)$ と同様に $n \geq 3$ なら, $\Psi_n(x)$ は n が相異なる奇素数の積のものでかける.

命題 2.3.3. (1) $n = p_1^{l_1} \cdots p_k^{l_k}$ ($p_1, \ldots, p_k$は相異なる素数) を n の素因数分解, $N = p_1 \cdots p_k$ とする. このとき, $\Psi_n(x) = \Psi_N(x^{\frac{n}{N}})$.

(2) $n \geq 3$ を奇数とする. このとき, $\Psi_{2n}(x) = (1 - x^n)\Psi_n(-x)$.

証明. (1) $\Psi_n(x)$ を変形すると,

$$\Psi_n(x) = \frac{x^n - 1}{\Phi_n(x)} = \frac{(x^{\frac{n}{N}})^N - 1}{\Phi_N(x^{\frac{n}{N}})} = \Psi_N(x^{\frac{n}{N}})$$

である.

(2) $\Psi_{2n}(x)$ を変形すると,

$$\begin{aligned}
\Psi_{2n}(x) &= \frac{x^{2n} - 1}{\Phi_{2n}(x)} \\
&= \frac{(-x)^{2n} - 1}{\Phi_{2n}(x)} \\
&= ((-x)^n + 1)\frac{((-x)^n - 1)}{\Phi_n(-x)} \\
&= ((-x)^n + 1)\Psi_n(-x) \\
&= (1 - x^n)\Psi_n(-x)
\end{aligned}$$

である. □

$\Psi_n(x)$ の k 次の係数を $b_n(k)$ とする. つまり, $\Psi_n(x) = \sum_{k=0}^{n-\phi(n)} b_n(k)x^k$ とする. 上の命題 2.3.3 より, $\Psi_n(x)$ の係数について次がわかる.

系 2.3.4. (1) $b_n(k) = \begin{cases} b_N(\frac{k}{N}), & N \mid k, \\ 0, & \text{その他.} \end{cases}$

(2) $b_{2n}(k) = \begin{cases} (-1)^k b_n(k), & k < n, \\ (-1)^k b_n(k-n) & k \geq n. \end{cases}$

これはつまり, $\Psi_n(x)$ の係数は n が相異なる奇素数の積の場合の係数に帰着されるということである. よって, 定理 2.3.1 を示すには,$\Psi_p(x), \Psi_{pq}(x)$ の係数が $1, 0, -1$ のいずれかであることを示せばよい.

定理 2.3.1 の証明. $n = p, pq$ のときの $\Psi_n(x)$ を考える. $n = p$ のときは

$$\Psi_p(x) = \prod_{d|p, d<p} \Phi_d(x) = \Phi_1(x) = x - 1$$

である. また, $n = pq$ $(p < q)$ のとき,

$$\begin{aligned}
\Psi_{pq}(x) &= \prod_{d|pq, d<pq} \Phi_d(x) \\
&= \Phi_1(x)\Phi_p(x)\Phi_q(x) \\
&= (x-1)(x^{p-1} + x^{p-2} + \cdots + 1)(x^{q-1} + x^{q-2} + \cdots + 1) \\
&= (x^q - 1)(x^{p-1} + p^{p-2} + \cdots + 1) \\
&= x^{p+q-1} + x^{p+q-2} + \cdots + x^q - (x^{p-1} + p^{p-2} + \cdots + 1)
\end{aligned}$$

である. よって, $\Psi_p(x), \Psi_{pq}(x)$ の係数は $1, 0, -1$ のいずれかである. □

注意 2.3.5. 定理 2.3.1 からは, 「$n < 105$ のときに $\Phi_n(x)^{-1}$ の係数は $1, 0, -1$ のいずれか」ということがわかるだけだが, 実際には $n < 561$ ならば $\Phi_n(x)^{-1}$ の係数は $1, 0, -1$ のいずれかになる ([Mo]).

3　グラフ理論

定理 I の証明では, グラフ理論を用いる. この章ではグラフについて必要事項をまとめる. 具体的には, 3.1 節で一般のグラフについて整理する. 3.2 節では二部グラフの概念を定義し, 二部グラフの集合にある同値関係を定める. この同値関係に関してすべての木が互いに同値になるのである.

3.1　グラフ

この節では R. ディーステル [D] と C. ベルジュ [B] をもとに, グラフについてまとめる. まず, グラフを構成する頂点や辺という概念を導入する. 次に, グラフの特徴を表す概念 (木, 連結など) と木における頂点の距離という概念を導入する. 最後に, 定理 I の証明に必要ないくつかの命題を証明する. 以下, X を空でない有限集合とする. また, 集合 A に対し, $C(A,m)$ を A の m 点集合全体の集合とする.

まず, グラフという概念を定義する.

定義 3.1.1. (1) $E \in C(X,2)$ を X 上のグラフという. つまり, X の 2 点集合の集合をグラフという. $\{x,y\} \in E$ を E の辺といい, E を辺集合という.

(2) X の元を頂点, X を頂点集合という.

(3) X 上のグラフ全体を $\mathcal{G}(X)$ とかく.

(4) $\mathcal{G}_k(X) = \{E \in \mathcal{G}(X) \mid |E| = k\}$ とする.

注意 3.1.2. 一般には頂点集合と辺集合の組 (X,E) をグラフという. 本論文では, 頂点集合は固定して議論することが多いため, 単に E をグラフと呼ぶ. ただし, 後述するグラフの連結成分については頂点集合と辺集合の組で考える.

以下, 辺 $\{x,y\} \in E$ を単に xy とかく. また, 辺 xy に対し, x と y を辺 xy の端点と呼ぶ.

グラフの特徴を表す基本的な用語を導入する.

定義 3.1.3. $E \in \mathcal{G}(X)$ とする.

(1) 相異なる頂点 $x_0, \ldots, x_n \in X$ に対し, $x_0x_1, x_1x_2, \ldots, x_{n-1}x_n \in E$ のとき, $\{x_0x_1, x_1x_2, \ldots, x_{n-1}x_n\}$ を x_0 から x_n への道という.

(2) x から x' への道が複数ある頂点 $x, x' \in X$ が存在するとき, E は閉路をもつという.

(3) 任意の異なる 2 頂点 $x, y \in X$ に対し, x から y への道が存在するとき, E は連結であるという. そうでないとき E は非連結という.

(4) 閉路を持たない連結なグラフを木という.

注意 3.1.4. グラフ E が木であることと, 任意の $x, x' \in X$ に対し x から x' への道が 1 つだけ存在することは同値である.

次に連結成分を定義する. そのためにまず, グラフに対して X 上の同値関係を定める.

定義 3.1.5. $E \in \mathcal{G}(X)$ とする. $x, y \in X$ に対し, $xy \in E$ のとき, $x \sim y$ とかく. この $\sim$ という関係から生成される X 上の同値関係を $\sim_E$ と定める.

この同値関係を用いて連結成分を定義する.

定義 3.1.6. $E \in \mathcal{G}(X)$ とする. 同値関係 $\sim_E$ に関する X の同値類 $T \in X/\sim_E$ に対し, 辺集合 F を

$$F = \{xy \in E \mid x, y \in T\}$$

と定めると, (T, F) は連結なグラフとなる. これを E の連結成分という.

例 3.1.7. グラフ E が連結ならば, (X, E) が E の連結成分となる.

注意 3.1.8. $(T_1, E_1), \ldots, (T_k, E_k)$ を E の連結成分すべてとすると, E は $E_1, \ldots, E_k$ の交わりのない和集合でかける. つまり,

$$E = E_1 \sqcup \cdots \sqcup E_k$$

である.

次に頂点の特徴を表す記号, 用語を定義する.

定義 3.1.9. $E \in \mathcal{G}(X)$ とする.

(1) $x \in X$ に対し, x を端点とする E の辺の個数を $\det_E(x)$ と定める. つまり, $\deg_E(x) = |\{y \in X \mid xy \in E\}|$ と定める.

(2) E において, $x \in X$ を端点とする辺が 1 つであるとき, つまり, $\deg_E(x) = 1$ のとき, x を E の葉という.

(3) E において, $x \in X$ を端点とする辺が存在しないとき, つまり, $\deg_E(x) = 0$ のとき, x を E の孤立点という.

木に対して, 頂点間の距離を導入する.

定義 3.1.10. $E \in \mathcal{G}(X)$ を木とする. 異なる頂点 $a, b \in X$ に対し, E における a から b への道を $P(a,b)$ とする. このとき, $|P(a,b)|$ を a, b の距離と定め, $d(a,b)$ とかく.

注意 3.1.11. 実際には距離は木に限らず, 一般の有限グラフに対して定義することができる. 一般の有限グラフでは道が複数存在することがある. その場合は $|P(a,b)|$ の最小値を a, b の距離と定める. また, 道が 0 個の場合は距離は ∞ と定める.

この距離について次が成り立つ.

命題 3.1.12. $|X| > 1$ とする. $E \in \mathcal{G}(X)$ が木のとき, 頂点 $x \in X$ に対し, x からの距離が最大となる頂点は葉である.

証明. y を x からの距離が最大となる頂点とする. y が葉でないとする. x から y への道を $P(x,y)$ とすると, $x'y \in E \setminus P(x,y)$ となる $x' \in X$ が存在する. すると $P(x,y) \sqcup \{x'y\}$ は x から x' への道である. E は木であるから, x から x' への道はこの 1 つに限る. このとき $d(x,x') = d(x,y) + 1$ である. これは y の取り方に反する. □

以下, $|X| > 1, m = |X| - 1$ とする. 次の命題は木を特徴づける性質である ([B] p.84 定理 1).

命題 3.1.13. $E \in \mathcal{G}(X)$ に対し次の (1) から (5) は同値である.
(1) E は木である.
(2) E は連結で $|E| = m$.
(3) E は閉路をもたず $|E| = m$.
(4) E は閉路をもたず, 辺を一つ加えると必ず閉路をもつ.
(5) E は連結で, どの一つの辺を取り去っても連結でなくなる.

最後に定理 I の証明に使う命題をいくつか用意する.

命題 3.1.14. $E \in \mathcal{G}_m(X)$ が閉路をもつならば E は非連結.

証明. 命題 3.1.13 (2), (3) より明らか. □

命題 3.1.15. 連結なグラフ $E \in \mathcal{G}(X)$ が閉路をもつならば, $|E| \geq |X|$.

証明. 命題 3.1.13 より明らか. □

命題 3.1.16. $E \in \mathcal{G}_m(X)$ が非連結ならば閉路を持たない連結成分が存在する.

証明. $(T_1, E_1), \ldots, (T_k, E_k)$ を E の連結成分すべてとする. このとき, $E = E_1 \sqcup E_2 \sqcup \cdots \sqcup E_k$ である. すべての i に対し, E_i が閉路をもつとすると, 命題 3.1.15 より, $|E_i| \geq |T_i|$ である. よって,

$$|E| = |E_1| + \cdots + |E_k| \geq |T_1| + \cdots + |T_k| = |X| > m$$

となり矛盾する. □

3.2 二部グラフ

この節では, 定理 I の証明に使う定理を証明する. 二部グラフのある同値関係に関して, 二部グラフの木はすべて互いに同値になるという定理である (定理 3.2.11). この定理の証明では, 標準グラフという概念が鍵になる.

まず, 二部グラフという概念を定義する.

定義 3.2.1. X, Y を互いに交わりのない, つまり $X \cap Y = \emptyset$ となる空でない有限集合とする.

(1) $E \subset X \times Y$ を (X, Y) 上の二部グラフという. また, $(x, y) \in E$ を E の辺といい, E を辺集合という.

(2) X, Y の元を頂点, X, Y を頂点集合という.

(3) $\mathcal{G}(X, Y)$ を (X, Y) 上の二部グラフ全体の集合とする.

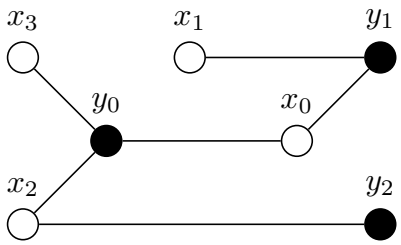
(4) $\mathcal{G}_k(X, Y) = \{E \in \mathcal{G}(X, Y) \mid |E| = k\}$ と定める.

注意 3.2.2. (X, Y) 上の二部グラフは, X の元同士, Y の元同士が辺で結ばれていない $X \sqcup Y$ 上のグラフと同一視できる. 二部グラフ E の辺 (x, y) を $\{x, y\}$ と同一視するわけだが, 以下これを前節のように単に xy や yx とかく.

例 3.2.3. $X = \{x_0, x_1, x_2, x_3\}, Y = \{y_0, y_1, y_2\}$ とする.

$$E = \{x_0y_0, x_0y_1, x_1y_1, x_2y_0, x_2y_2, x_3y_0\}$$

は二部グラフで, 図を描くと次のようになる.



以下, $m = |X| + |Y| - 1$ とし, $\mathcal{G}_m(X, Y)$ 上の同値関係を定める. そのためにまず, $X \times Y$ のある部分集合を定義する.

定義 3.2.4. (1) $y \in Y$ に対し, $X(y) = X \times \{y\}$ と定める.
(2) $x \in X$ に対し, $Y(x) = \{x\} \times Y$ と定める.

$\mathcal{G}_m(X, Y)$ 上の同値関係 $\sim$ を定義するためにまず, $\mathcal{G}_m(X, Y)$ 上の関係 $\backsim$ を定義する.

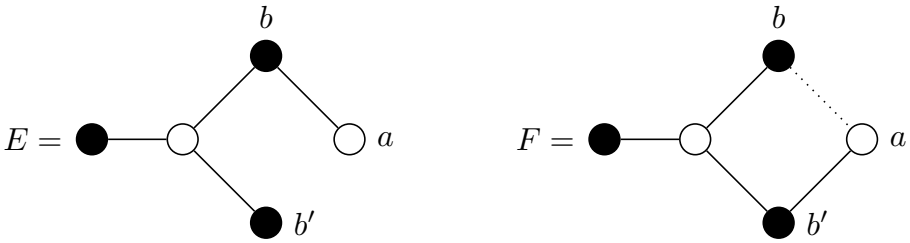
定義 3.2.5. $E, F \in \mathcal{G}_m(X, Y)$ が次のどちらかを満たすとき, $E \backsim F$ とする.
(1) $|E \cap X(y)| = |F \cap X(y)| = 1$ かつ $E \setminus X(y) = F \setminus X(y)$ を満たす $y \in Y$ が存在.
(2) $|E \cap Y(x)| = |F \cap Y(x)| = 1$ かつ $E \setminus Y(x) = F \setminus Y(x)$ を満たす $x \in X$ が存在.

定義 3.2.6. 関係 $\backsim$ で生成される $\mathcal{G}_m(X, Y)$ 上の同値関係を $\sim$ とかく.

注意 3.2.7. $E \backsim F$ とは, E のある葉 a に対し, a を端点とする辺 ab を辺 ab' に取り換えると, F に等しくなるということである.

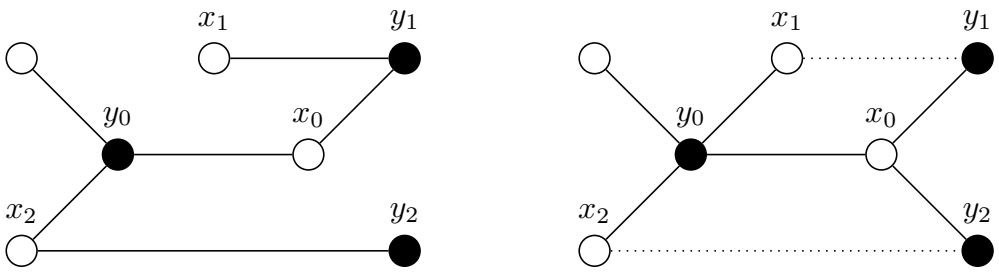
関係 $\backsim$ の例と同値関係 $\sim$ の例を見せる.

例 3.2.8. 次のグラフ E, F に対し, $E \backsim F$ である.



実際, E において (a が E の葉であることに注意して) 辺 ab を ab' に取り換えると F になる.

例 3.2.9. 次の 2 つのグラフは同値である.



実際, 左のグラフにおいて辺 x_1y_1 を x_1y_0 に取り換え, 次に x_2y_2 を x_0y_2 に取り換えると右のグラフとなる.

この $\mathcal{G}_m(X,Y)$ 上の同値関係について次が成り立つ.

命題 3.2.10. $E \in \mathcal{G}_m(X,Y)$ が閉路をもつなら孤立点をもつグラフに同値.

証明. 命題 3.1.14 より E は非連結である. すると, 命題 3.1.16 より閉路を持たない連結成分 (T,F) が存在する. $|T| = 1$ のときは明らか. $|T| > 1$ とする. このとき, F は $\mathcal{G}(X \cap T, Y \cap T)$ の木である. 命題 3.1.12 より, F には葉が存在する. その 1 つを a とする. a は E においても葉である. 辺 $ab \in E$ を aa_1 $(a_1 \notin T)$ に取り換えたグラフを E_1 とすると $E \sim E_1$ である. このとき,

$$T_1 = T \setminus \{a\}, \quad F_1 = F \setminus \{ab\}$$

とすると, (T_1, F_1) は E_1 の閉路を持たない連結成分である. $|T_1| = 1$ なら T_1 の元が E_1 の孤立点である. つまり, E は孤立点をもつグラフに同値である. $|T_1| > 1$ とする. (T_1, F_1) は $\mathcal{G}(X \cap T_1, Y \cap T_1)$ の木であり, 葉が存在する. 以下同様に繰り返すと, $E_k \sim E$ で,

$$|T_k| = 1, \quad |F_k| = 0$$

となる連結成分 (T_k, F_k) が存在するような E_k がとれる. 1 点集合 T_k の元は E_k の孤立点だから, E は孤立点をもつグラフに同値である. □

次は, 定理 I の証明に必要な最も重要な定理である.

定理 3.2.11. $\mathcal{G}(X,Y)$ の木はすべて互いに同値.

これを証明するためにまず, 標準グラフという概念を導入する.

定義 3.2.12. (X,Y) 上の二部グラフ E が $x \in X, y \in Y$ に対し

$$E = X(y) \cup Y(x)$$

であるとき E を標準グラフといい, H_{xy} とかく.

簡単に言えば標準グラフ H_{xy} とは, すべての頂点が x または y と結ばれている木である. 例えば上の例 3.2.9 の右のグラフは標準グラフ $H_{x_0y_0}$ である.

定理 3.2.13. 標準グラフはすべて互いに同値である.

証明. $x, x' \in X$ と $y \in Y$ に対し, $H_{xy} \sim H_{x'y}$ を示せばよい.

$$H_{xy} = X(y) \cup Y(x)$$

である. H_{xy} において y 以外の Y の頂点は葉である. すべての $b \in Y \setminus \{y\}$ に対し, 辺 xb を辺 $x'b$ に取り換えたグラフを E_1 とする. すると, $E_1 \sim H_{xy}$ である. いま, $x'y \in E$ であったから, $x'y \in E_1$ である. よって, $Y(x') \subset E_1$ である. また, $X(y) \subset E_1$ であるから, $E_1 \supset X(y) \cup Y(x') = H_{xy'}$ である. $|E_1| = |H_{xy'}|$ なので, $E_1 = H_{xy'}$ である. したがって $H_{xy} \sim H_{x'y}$. □

定理 3.2.11 の証明に使う補題を用意する.

補題 3.2.14. $|X|, |Y| > 1$, $E \in \mathcal{G}_m(X, Y)$ を木とする. また, 頂点 $x \in X, y \in Y$ に対し $xy \in E$ とする. このとき, $E \neq H_{xy}$ ならば, x と y のどちらとも辺で結ばれていない葉が存在する.

証明. x からの距離の最大値を考える. $\max_{a \in X \sqcup Y} d_E(x, a) > 2$ のときは明らかである. $\max_{a \in X \sqcup Y} d_E(x, a) = 2$ とする (E は二部グラフなので, $a \in X$ である). すると, すべての $b \in Y$ に対し, $d_E(x, b) = 1$, つまり $xb \in E$ である. 命題 3.1.12 より $d_E(x, a) = 2$ となる頂点 a は葉である. $d_E(x, a) = 2$ となるすべての a に対し, $ay \in E$ とすると, E が標準グラフとなり矛盾する. よって, $ay \notin E$ となる a が存在する. □

この補題を用いて定理 3.2.11 を証明する.

定理 3.2.11 の証明. $E \in \mathcal{G}_m(X, Y)$ が木なら, E がある標準グラフに同値であることを示せばよい.

$|X| = 1$ または $|Y| = 1$ のとき, E は明らかに標準グラフである.

$|X|, |Y| > 1$ とする. $xy \in E$ を満たす $x \in X$ と $y \in Y$ をとる. $E \sim H_{xy}$ を示せばよい. x または y と辺で結ばれている頂点の個数を $\deg_E(x, y)$ とする. つまり $\deg_E(x, y) = \deg_E(x) + \deg_E(y)$ とする. $\deg_E(x, y) = |X| + |Y|$ のとき, E は標準グラフである. $\deg_E(x, y) < |X| + |Y|$ とする. このとき, E は標準グラフでない. よって, 補題 3.2.14 より, x, y と辺で結ばれていない葉 $a \in X \sqcup Y$ が存在する. ここで, $a \in X$ と仮定する ($a \in Y$ としても同様に証明できる). a は葉である. $ab \in E$ とする. このとき, $T_0 = E \setminus \{ab\}$ とすると

$$E = T_0 \sqcup \{ab\}$$

とかける. いま, $E_1 = T_0 \sqcup \{ay\}$ とすると, $E \sim E_1$ である. 実際,

$$|E \cap Y(a)| = |\{ab\}| = 1, \quad |E_1 \cap Y(a)| = |\{ay\}| = 1$$

であり,

$$E \setminus Y(a) = T_0, \quad E_1 \setminus Y(a) = T_0$$

である. すると, $\deg_{E_1}(x,y) = \deg_E(x,y) + 1$ である. $\deg_{E_1}(x,y) = |X| + |Y|$ なら, E_1 は標準グラフである. つまり, E は標準グラフに同値である. $\deg_{E_1}(x,y) < |X| + |Y|$ とすると, 同様にして, $E_2 \backsim E_1$ かつ $\deg_{E_2}(x,y) = \deg_{E_1}(x,y) + 1$ となる E_2 がとれる. 以下, これを繰り返す. 頂点は有限個なので, これは有限回で終わる. つまり, $E \sim E_k$ かつ $\deg_{E_k}(x,y) = |X| + |Y|$ を満たす E_k がとれる. E_k は標準グラフなので, E は標準グラフに同値である. □

4　定理 I の証明

この章では, 本論文の主結果である定理 I を証明する. 4.1 節で, ベクトル空間のテンソル積, 直和について記号を導入する. 4.2 節で, ベクトル空間の部分集合に対する性質 (C) を導入する. 4.3 節で定理 I を線型代数の定理に帰着させる. これは, n が 2 以外の素因数を高々 2 つしかもたないとき, 1 の n 乗根全体の集合 Z_n が性質 (C) をもつという定理である. これを証明することになる. 4.4 節ではこの線型代数の定理は $n = p, pq$ の場合が本質的であり, その他の場合は $n = p, pq$ のどちらかの場合に帰着できることを説明する. $n = p, pq$ の場合をそれぞれ 4.5 節, 4.6 節で証明する. $n = p$ のときの証明は易しい. $n = pq$ の場合は, 3 章のグラフ理論を用いて証明する.

4.1　記号の準備

定理 I の証明において, ベクトル空間のテンソル積や直和を考える. この節では, テンソル積のある部分集合を表す記号や, 直和成分を表す記号を導入する.

まずは, テンソル積のある部分集合を表す記号を導入する.

定義 4.1.1. V, W をベクトル空間とする.

(1) $X \subset V$ と $Y \subset W$ に対し,

$$X \otimes Y = \{x \otimes y \mid x \in X, y \in Y\}$$

と定める.

(2) $x \in V$ と $Y \subset W$ に対し,

$$x \otimes Y = \{x \otimes y \mid y \in Y\}$$

と定める. 同様に, $y \in W$ と $X \subset V$ に対し,

$$X \otimes y = \{x \otimes y \mid x \in X\}$$

と定める.

次に, 直和成分を表す記号を導入する.

定義 4.1.2. (1) V の直和 $\bigoplus_{i \in \Lambda} V$ に対し, $i \in \Lambda$ に対応する直和成分を $V^{(i)}$ とかく.

(2) $v \in V$ に対応する $V^{(i)}$ の元を $v^{(i)}$ とかく.

(3) $X \subset V$ に対応する $V^{(i)}$ の部分集合を $X^{(i)}$ とかく.

4.2 ベクトル空間の部分集合の性質 (C)

定理 I の主張は, ベクトル空間のある部分集合がある性質 (C) をもつことに帰着される. この節ではこの性質を導入し, この性質が直和をとる操作で保たれることなどを証明する.

まず, ベクトル空間の部分集合の性質 (C) を次で定める.

定義 4.2.1. V を有限次元ベクトル空間, X をその部分集合とする. X が次をみたすとき, X は V において性質 (C) をもつという.

(C) V の基底となる $S \subset X$ に対して S に対応する行列式の値は (符号を除いて) S によらず一定となる.

要するに, V の基底となる X の部分集合に対し, それの張る平行体の体積が一定になるということである.

性質 (C) を詳しく論じるために, ベクトル空間の部分集合に (符号の違いを無視した) 行列式を対応させる写像 D を導入する. 自然な準同型 $\mathbb{C} \to \mathbb{C}/\{\pm 1\}$ で $z \in \mathbb{C}$ に対応するものを $[z]$ とする. m 次元ベクトル空間 V に対し, $D : H(V, m) \to \mathbb{C}/\{\pm 1\}$ を

$$\{v_1, \ldots, v_m\} \mapsto [\det(v_1, \ldots, v_m)]$$

で定める. ここで, $H(V, m)$ は V の元からなる m 点多重集合全体の集合とする.

注意 4.2.2. 行列式 $\det(v_1, \ldots, v_m)$ は V の基底を 1 つ固定してこの基底における $v_1, \ldots, v_m$ の数ベクトル表示を並べた行列の行列式とする. つまり, V の基底 $w_1, \ldots, w_m$ に対し, $(v_1, \ldots, v_m) = (w_1, \ldots, w_m)A$ とするとき, $\det(v_1, \ldots, v_m) = \det A$ と定める. ここで, V の基底の取り方によって行列式の値は定数倍の違いがでるが, 基底の取り方は今後の議論に影響しない.

注意 4.2.3. $H(V, m)$ の元は多重集合であるから, 本来は $\{\!\{v_1, \ldots, v_m\}\!\}$ のようにかくが, 本論文ではほとんどの場合重複がないときを考えるので, 単に $\{v_1, \ldots, v_m\}$ とかくことにする.

この D を用いると, 性質 (C) は,

V の基底となる $S \subset X$ に対して $D(S)$ は S によらず一定となる.

と言い換えられる.

実は, 性質 (C) はベクトル空間の直和を取る操作などで保たれる. これを示すために, D の性質を考える (この命題では多重集合も考えることになるので, 注意が必要である).

命題 4.2.4. *V を m 次元ベクトル空間とするとき, 次が成り立つ.*
(1) *$X \cup \{v\} \in H(V, m)$ とする. このとき, $w \in X$ に対し, $D(X \cup \{v\}) = D(X \cup \{v + w\})$.*
(2) *$X \cup \{-v\} \in H(V, m)$ とする. このとき, $D(X \cup \{-v\}) = D(X \cup \{v\})$.*

これは D の定義と, 行列の基本変形からすぐにわかる. この D の性質を用いて, 性質 (C) がベクトル空間の直和を取る操作で保たれること, つまり次を示す (これは定理 I を $n = p, pq$ の場合に帰着させる際の鍵となる).

定理 4.2.5. *V, W をそれぞれ a, b 次元ベクトル空間とする. 部分集合 $X \subset V$ と $Y \subset W$ がそれぞれ V, W において性質 (C) をもつとき, $X \cup Y$ は $V \oplus W$ において性質 (C) をもつ.*

証明. $S \in C(X \cup Y, a + b)$ をとる. $|S \cap X| > a$ のとき, $S \cap X$ は一次従属なので, S も一次従属. $|S \cap Y| > b$ のときも同様に, S は一次従属. よって, $|S \cap X| = a$ かつ $|S \cap Y| = b$ のときを考える. 特に一次独立な S を考える. このとき, $X_0 = S \cap X$ と $Y_0 = S \cap Y$ はどちらも一次独立. すると,

$$D(S) = D(X_0 \cup Y_0) = \left[\det \begin{pmatrix} X_0 & O \\ O & Y_0 \end{pmatrix}\right] = [\det X_0 \det Y_0]$$

である. ここで, X, Y がそれぞれ V, W において性質 (C) をもつので, $[\det X_0], [\det Y_0]$ の値は一定である. よって, $D(S) = [\det X_0 \det Y_0]$ の値も一定である. つまり, $X \cup Y$ は $V \oplus W$ において性質 (C) をもつ. □

注意 4.2.6. ベクトル空間 V, W の部分集合 X, Y に対し, X, Y をそれぞれ $X + \{\vec{0}\}, \{\vec{0}\} + Y$ と同一視することで, $X \cup Y$ を $V \oplus W$ の部分集合とみなしている.

また, 次も定理 I を $n = p, pq$ の場合に帰着させる際の鍵となる.

定理 4.2.7. *V を a 次元ベクトル空間とする. V の部分集合 X が V において性質 (C) をもつとき, $X_\pm$ は V において性質 (C) をもつ. ここで, $X_\pm = X \cup (-X)$ である.*

証明. $S \in C(X_\pm, a)$ をとる. $X_0 = S \cap X$, $X_1 = S \cap (-X)$ とする. このとき,

$$D(S) = D(X_0 \sqcup X_1) = D(X_0 \cup (-X_1)) \tag{4.2.1}$$

である. いま, $-X_1 \subset X$ より, $X_0 \cup (-X_1) \subset X$ である. X は V において性質 (C) をもつので, $D(S)$ は S によらず一定または 0 である. よって $X_\pm$ も V において性質 (C) をもつ. □

注意 4.2.8. 上の証明の (4.2.1) において, X_0 と X_1 は交わりを持たないが X_0 と $-X_1$ はそうとは限らない. よって $X_0 \cup (-X_1)$ は多重集合になる場合がある.

この 2 つの定理とこれから述べる 4.3 節, 4.4 節の議論を合わせると, 定理 I の証明は $n = p, pq$ の場合に帰着されることになる.

4.3 線型代数の定理に帰着

定理 I は 1 の n 乗根全体の集合 Z_n が性質 (C) をもつこと, つまり, 次の定理に帰着される.

定理 4.3.1. n が 2 以外の素因数を高々 2 つしかもたないとき, Z_n は $\mathbb{Q}(\zeta_n)$ において性質 (C) をもつ.

以下, これに帰着できる理由を説明する. 定理 I で問題としている値 $s_\lambda(\omega_1, \ldots, \omega_{\phi(n)})$ は, 次で定める数ベクトルを並べた行列の行列式の比である.

定義 4.3.2. $k = 0, 1, \ldots$ に対し, $\phi(n)$ 次の数ベクトル u_k を

$$u_k = \begin{pmatrix} \omega_1^k \\ \vdots \\ \omega_{\phi(n)}^k \end{pmatrix}$$

と定める.

$\omega_1, \ldots, \omega_{\phi(n)}$ はそれぞれ 1 の n 乗根だから $u_{k+n} = u_k$ であることに注意して, $\Omega_n = \{u_1, \ldots, u_{n-1}\}$ とおく. シューア多項式はその分子のみが分割 λ に依存する. つまり, $s_\lambda(\omega_1, \ldots, \omega_{\phi(n)})$ は分子における Ω_n の元の選び方だけに依存する. よって定理 I の主張は, 「Ω_n の元を列とする行列式の値が Ω_n の元の選び方によらず符号を除いて一定, または 0 である」と言い換えられる. したがって, 定理 I は次の定理に帰着される.

定理 4.3.3. 任意の $v_1, \ldots, v_{\phi(n)} \in \Omega_n$ に対し, $\det(v_1 \ldots v_{\phi(n)})$ は符号を除いて一定, または 0.

これはつまり, Ω_n で張られるベクトル空間 $\langle \Omega_n \rangle$ の部分集合 Ω_n が性質 (C) をもつとい

うことである. 次の命題で定理 4.3.3 を言い換えたものが定理 4.3.1 である.

命題 4.3.4. ζ_n を 1 の原始 n 乗根とすると, 線型同型写像 $\langle\Omega_n\rangle \to \mathbb{Q}(\zeta_n)$ で, Ω_n の像が Z_n となるものが存在する.

証明. $\mathbb{Q}(\zeta_n)$ から $\langle\Omega\rangle$ への線型同型写像で, Z_n が Ω に対応するものを与える. 定理 1.3.5 より, $i = 1, 2, \ldots, \phi(n)$ に対し, $\mathbb{Q}$ 上の自己同型写像 $f_i : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$ で

$$f_i(\zeta_n) = \omega_i$$

となるものが存在する. 線型写像 $f : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)^{\phi(n)}$ を

$$x \mapsto \begin{pmatrix} f_1(x) \\ \vdots \\ f_{\phi(n)}(x) \end{pmatrix}$$

で定める. すると, これは単射である. このとき,

$$\zeta_n^k \mapsto \begin{pmatrix} f_1(\zeta_n^k) \\ \vdots \\ f_{\phi(n)}(\zeta_n^k) \end{pmatrix} = \begin{pmatrix} \omega_1^k \\ \vdots \\ \omega_{\phi(n)}^k \end{pmatrix} = u_k$$

だから, f による Z_n の像は Ω である. $\mathbb{Q}(\zeta_n)$ は Z_n で張られるので, f による $\mathbb{Q}(\zeta_n)$ の像は Ω で張られる. つまり, $\operatorname{Im} f = \langle\Omega\rangle$ である. これで, $\mathbb{Q}(\zeta_n)$ から $\langle\Omega\rangle$ への線型同型写像で, Z_n が Ω に対応するものが得られた. □

以上で定理 I は定理 4.3.1 に帰着された.

4.4 $\mathbb{Q}(\zeta_n)$ の構造

この節では, 定理 4.3.1 を $n = p, pq$ の場合に帰着させる. そのために $\mathbb{Q}(\zeta_n)$ の $\mathbb{Q}$ 上のベクトル空間としての構造を考える. n が $n = p_1^{l_1} \cdots p_k^{l_k}$ と素因数分解されるとき, $\mathbb{Q}(\zeta_n)$ は $\mathbb{Q}(\zeta_{p_1}) \otimes \cdots \otimes \mathbb{Q}(\zeta_{p_k})$ の直和と自然に同型になり, Z_n に対応する部分集合は $Z_{p_1} \otimes \cdots \otimes Z_{p_k}$ の和集合となる. これが鍵となり, 定理 4.3.1 を $n = p, pq$ の場合に帰着させることができる. この節ではさらに, これを基本零和系という概念を用いてより一般的な形の定理に帰着させる.

まずは, $\mathbb{Q}(\zeta_n)$ が $\mathbb{Q}(\zeta_{p_1}) \otimes \cdots \otimes \mathbb{Q}(\zeta_{p_k})$ の直和と自然に同型になることを示す. つまり, 次を示す.

定理 4.4.1. (1) a, b が互いに素なとき, 線型同型写像 $\mathbb{Q}(\zeta_{ab}) \to \mathbb{Q}(\zeta_a) \otimes \mathbb{Q}(\zeta_b)$ で, Z_{ab} の像が $Z_a \otimes Z_b$ であるものが存在する.

(2) 素数 p に対し, 線型同型写像 $\mathbb{Q}(\zeta_{p^l}) \to \bigoplus_{j\in\Lambda} \mathbb{Q}(\zeta_p)^{(j)}$ で, Z_{p^l} の像が $\bigsqcup_{j\in\Lambda} Z_p^{(j)}$ であるものが存在する. ここで, $|\Lambda| = p^{l-1}$ である.

(3) a が奇数のとき, 線型同型写像 $\mathbb{Q}(\zeta_{2a}) \to \mathbb{Q}(\zeta_a)$ で, Z_{2a} の像が $(Z_a)_\pm$ であるものが存在する.

(4) a が奇数のとき, 線型同型写像 $\mathbb{Q}(\zeta_{2^k a}) \to \bigoplus_{i\in\Lambda} \mathbb{Q}(\zeta_a)^{(i)}$ で, $Z_{2^k a}$ の像が $\bigsqcup_{i\in\Lambda} (Z_a)_\pm^{(i)}$ であるものが存在する. ここで, $|\Lambda| = 2^{k-1}$ である.

証明. 1.3 節の議論から, $\mathbb{Q}(\zeta_n)$ は $\mathbb{Q}$ 上 $\phi(n)$ 次元ベクトル空間であった. これを用いて証明する.

(1) $\mathbb{Q}(\zeta_a) \otimes \mathbb{Q}(\zeta_b)$ から $\mathbb{Q}(\zeta_{ab})$ への線型同型写像で, Z_{ab} が $Z_a \otimes Z_b$ に対応するものを与える. $\mathbb{Q}(\zeta_a)$ と $\mathbb{Q}(\zeta_b)$ が $\mathbb{Q}(\zeta_{ab})$ の部分体であることに注意して, 双線型写像 $\mathbb{Q}(\zeta_a) \times \mathbb{Q}(\zeta_b) \to \mathbb{Q}(\zeta_{ab})$ を

$$(x, y) \mapsto xy$$

で定める. これから, 線型写像 $f : \mathbb{Q}(\zeta_a) \otimes \mathbb{Q}(\zeta_b) \to \mathbb{Q}(\zeta_{ab})$ が

$$x \otimes y \mapsto xy$$

で定まる. このとき,

$$f(\zeta_a^i \otimes \zeta_b^j) = \zeta_{ab}^{aj+bi}$$

である. この f が線型同型写像であることを示そう. 次元は等しいので, 全射であることを示せばよい. すべての m に対し, $f(\zeta_a^i \otimes \zeta_b^j) = \zeta_{ab}^{aj+bi} = \zeta_{ab}^m$ となる, つまり $aj + bi = m$ となる i, j が存在することを示せばよい. a, b は互いに素なのでこれは明らかである. したがって, f は全射である. $Z_a \otimes Z_b$ の f による像が Z_{ab} であることはすぐわかる.

(2) $\bigoplus_{j\in\Lambda} \mathbb{Q}(\zeta_p)^{(j)}$ から $\mathbb{Q}(\zeta_{p^l})$ への線型同型写像で, $\bigsqcup_{j\in\Lambda} Z_p^{(j)}$ が Z_{p^l} に対応するものを与える. $\mathbb{Q}(\zeta_p)$ が $\mathbb{Q}(\zeta_{p^l})$ の部分体であることに注意して, $\Lambda = \{0, 1, \ldots, p^{l-1} - 1\}$ に対し, $\bigoplus_{j\in\Lambda} \mathbb{Q}(\zeta_p)^{(j)}$ を考える. 線型写像 $g : \bigoplus_{j\in\Lambda} \mathbb{Q}(\zeta_p)^{(j)} \to \mathbb{Q}(\zeta_{p^l})$ を

$$x^{(j)} \mapsto \zeta_{p^l}^j x$$

で定める. このとき,

$$g(\zeta_p^{i\,(j)}) = \zeta_{p^l}^{p^{l-1}i+j}$$

である. この g が線型同型写像であることを示そう. 次元は等しいので, この g が全射であることを示せばよい. すべての m に対し, $g(\zeta_p^{i\,(j)}) = \zeta_{p^l}^{p^{l-1}i+j} = \zeta_{p^l}^m$ となる, つまり

$p^{l-1}i+j=m$ となる i,j $(0\leq j<p^{l-1})$ が存在することを示せばよいがこれは明らかである. $\bigsqcup_{j\in\Lambda}Z_p^{(j)}$ の g による像が Z_{p^l} であることはすぐわかる.

(3) (1) の線型同型写像と, 次で定める線型同型写像を合成すればよい.

線型写像 $\mathbb{Q}(\zeta_2)\otimes\mathbb{Q}(\zeta_a)\to\mathbb{Q}(\zeta_a)$ を

$$1\otimes x\mapsto x$$

で定める. これは明らかに線型同型写像で, この写像による $Z_2\otimes Z_a$ の像は $(Z_a)_\pm$ である.

(4) (2), (3) の線型同型写像を合成すればよい. □

この線型同型写像による $\mathbb{Q}(\zeta_n)$ の像 $\mathbb{Q}(\zeta_n)'$ は n に応じてそれぞれ次のようになる.

$$\mathbb{Q}(\zeta_n)'=\begin{cases}\mathbb{Q}(\zeta_p), & n=p,2p,\\ \mathbb{Q}(\zeta_p)\otimes\mathbb{Q}(\zeta_q), & n=pq,2pq,\\ \bigoplus_{i\in\Lambda}\mathbb{Q}(\zeta_p)^{(i)}\ (\text{ただし } |\Lambda|=p^{l-1}), & n=p^l,\\ \bigoplus_{i\in\Lambda}\mathbb{Q}(\zeta_p)^{(i)}\ (\text{ただし } |\Lambda|=2^{k-1}p^{l-1}), & n=2^kp^l,\\ \bigoplus_{i\in\Lambda}(\mathbb{Q}(\zeta_p)\otimes\mathbb{Q}(\zeta_q))^{(i)}\ (\text{ただし } |\Lambda|=p^{l-1}q^{m-1}), & n=p^lq^m,\\ \bigoplus_{i\in\Lambda}(\mathbb{Q}(\zeta_p)\otimes\mathbb{Q}(\zeta_q))^{(i)}\ (\text{ただし } |\Lambda|=2^{k-1}p^{l-1}q^{m-1}), & n=2^kp^lq^m.\end{cases}$$

また, Z_n の像 Z_n' は, それぞれ次のようになる.

$$Z_n'=\begin{cases}Z_p, & n=p,\\ (Z_p)_\pm, & n=2p,\\ Z_p\otimes Z_q, & n=pq,\\ (Z_p\otimes Z_q)_\pm, & n=2pq,\\ \bigsqcup_{i\in\Lambda}Z_p^{(i)}, & n=p^l,\\ \bigsqcup_{i\in\Lambda}(Z_p)_\pm^{(i)}, & n=2^kp^l,\\ \bigsqcup_{i\in\Lambda}(Z_p\otimes Z_q)^{(i)}, & n=p^lq^m,\\ \bigsqcup_{i\in\Lambda}(Z_p\otimes Z_q)_\pm^{(i)}, & n=2^kp^lq^m.\end{cases}$$

いま, Z_n' が $\mathbb{Q}(\zeta_n)'$ において性質 (C) をもつことを示せばよいのだが, 定理 4.2.5 と定理 4.2.7 を用いると, $n=2p,p^l,2^kp^l$ の場合は $n=p$ の場合に, $n=2pq,p^lq^m,2^kp^lq^m$ の場合は $n=pq$ の場合に帰着される. よって, 定理 4.3.1 は $n=p,pq$ の場合, つまり次の定理に帰着される.

定理 4.4.2. (1) 素数 p に対し, Z_p は $\mathbb{Q}(\zeta_p)$ において, 性質 (C) をもつ.

(2) 異なる奇素数 p, q に対し, $Z_p \otimes Z_q$ は $\mathbb{Q}(\zeta_p) \otimes \mathbb{Q}(\zeta_q)$ において, 性質 (C) をもつ.

これらをより一般的な基本零和系の定理の形で証明する. ここで $a-1$ 次元ベクトル空間 V の a 点集合で, V を張り, 和が 0 となるものを基本零和系とよぶことにする. つまり, ベクトル空間の基本零和系とは次で定義されるものである.

定義 4.4.3. a を自然数とする. $a-1$ 次元ベクトル空間 V に対し,

$$|X| = a, \quad \sum X = 0, \quad \langle X \rangle = V$$

を満たす V の部分集合 X を V の基本零和系という. ここで, $\sum X = \sum_{x \in X} x$ である.

例えば, 素数 p に対し, Z_p は $\mathbb{Q}(\zeta_p)$ の基本零和系である. 実際, $\mathbb{Q}(\zeta_p)$ は $\phi(p) = p-1$ 次元ベクトル空間で, Z_p は

$$|Z_p| = p, \quad \sum Z_p = 0, \quad \langle Z_p \rangle = \mathbb{Q}(\zeta_p)$$

を満たす.

注意 4.4.4. $a-1$ 次元ベクトル空間 V の基底 $v_1, \ldots, v_{a-1}$ に対し, $v_a = -(v_1 + \cdots + v_{a-1})$ とすると, $\{v_1, \ldots, v_a\}$ は V の基本零和系である. 基本零和系は実質的にこの形のもので尽きている.

Z_p は基本零和系だから, 定理 4.4.2 は次の定理の特別なケースとみなせる.

定理 4.4.5. (1) a を自然数とする. $a-1$ 次元ベクトル空間 V の基本零和系は V において性質 (C) をもつ.

(2) a, b を自然数とする. V, W をそれぞれ $a-1, b-1$ 次元ベクトル空間とする. 部分集合 $X \subset V$ と $Y \subset W$ をそれぞれ, V, W の基本零和系とする. すると, $X \otimes Y$ は $V \otimes W$ において性質 (C) をもつ.

結局, これを示せばよいことになる. (1) と (2) は 4.5 節, 4.6 節でそれぞれ証明する. (1) の証明は易しい. (2) の証明はグラフ理論を用いる.

注意 4.4.6. 3 つの基本零和系のテンソル積は性質 (C) を満たすとは限らない (2 次元, 4 次元, 6 次元ベクトル空間の基本零和系のテンソル積が反例となる). 定理 4.4.5 (2) から, 性質 (C) はベクトル空間のテンソル積を取る操作でも保たれそうな気がするが, そうではない.

4.5 $n = p$ の場合の証明

この節では, 定理 4.4.5 の (1) を示す.

定理 4.4.5 (1) の証明. X を V の基本零和系とする. 任意に $S, T \in C(X, a-1)$ をとる. この S, T に対して, $D(S) = D(T)$ を示せばよい.

いま, $S = X \setminus \{v\}, T = X \setminus \{v'\}$ となる $v, v' \in V$ が存在する. $Q = X \setminus \{v, v'\}$ と定めると, $S = Q \sqcup \{v'\}, T = Q \sqcup \{v\}$ である. このとき,

$$\begin{aligned} D(S) &= D(Q \sqcup \{v'\}) \\ &= D(Q \sqcup \{v' + \sum Q\}) \\ &= D(Q \sqcup \{\sum_{u \in X \setminus \{v\}} u\}) \\ &= D(Q \sqcup \{-v\}) \\ &= D(Q \sqcup \{v\}) \\ &= D(T) \end{aligned}$$

である. 第 2 の等号では命題 4.2.4 (1) を用いた. 第 4 の等号では $\sum X = 0$ を用いた. 第 5 の等号では命題 4.2.4 (2) を用いた. □

4.6 $n = pq$ の場合の証明

この節では, 定理 4.4.5 の (2) を示す.

証明の概要を述べる. 以下, $d = \dim(V \otimes W) = (a-1)(b-1)$ とし, さらに $m = ab - d$ とする. まず, $C(X \otimes Y, d)$ にある同値関係 $\sim$ を定める. これは $S \sim T$ なら, $D(S) = D(T)$ となるような同値関係である. $X \otimes Y$ における補集合を考えると, $C(X \otimes Y, m)$ 上の同値関係が考えられる. この $C(X \otimes Y, m)$ は, 3.2 節で定めた二部グラフの集合 $\mathcal{G}_m(X, Y)$ と同一視でき, $C(X \otimes Y, m)$ 上の同値関係は $\mathcal{G}_m(X, Y)$ 上の同値関係と一致する. そして $C(X \otimes Y, d)$ の一次独立な元の補集合は $\mathcal{G}_m(X, Y)$ の木と対応する. よって, すべての木が互いに同値になるという定理 3.2.11 より, $C(X \otimes Y, d)$ の一次独立な元はすべて互いに同値になり, D の値が等しくなるのである. このように補集合を考えることで, 定理 4.4.5 (2) は 3.2 節で述べたグラフの定理に帰着され証明できるのである.

証明の準備をする. $C(X \otimes Y, d)$ 上の同値関係の導入のためにまず $C(X \otimes Y, d)$ 上の関係 $\sim$ を定める.

定義 4.6.1. $S,T \in C(X \otimes Y, d)$ が次のどちらかを満たすとき, $S \dot{\sim} T$ とする.

(1) $|S \cap X(w)| = |T \cap X(w)| = a-1$ かつ, $S \smallsetminus X(w) = T \smallsetminus X(w)$ を満たす $w \in Y$ が存在.

(2) $|S \cap Y(v)| = |T \cap Y(v)| = b-1$ かつ $S \smallsetminus Y(v) = T \smallsetminus Y(v)$ を満たす $v \in X$ が存在.

ここで, $w \in Y$ に対し, $X(w) = X \otimes w$ と定める. 同様に $v \in X$ に対し, $Y(v) = v \otimes Y$ と定める.

定義 4.6.2. 関係 $\dot{\sim}$ で生成される同値関係を $\sim$ とかく.

この同値関係で, 次が成り立つ.

命題 4.6.3. $S \sim T$ ならば $D(S) = D(T)$.

証明. $S \dot{\sim} T$ のとき, $D(S) = D(T)$ を示せばよい. S,T が定義 4.6.1 の (1) を満たすとする ((2) を満たすときも同様に証明できる). つまり, $|S \cap X(w)| = |T \cap X(w)| = a-1$ かつ $S \smallsetminus X(w) = T \smallsetminus X(w)$ を満たす $w \in Y$ が存在すると仮定する. 第 1 の条件から,

$$S \cap X(w) = X(w) \smallsetminus \{v \otimes w\}, \quad T \cap X(w) = X(w) \smallsetminus \{v' \otimes w\}$$

となる $v, v' \in X$ が存在する. $P = S \smallsetminus X(w) = T \smallsetminus X(w)$, $Q = X(w) \smallsetminus \{v \otimes w, v' \otimes w\}$ とおくと,

$$S = P \sqcup Q \sqcup \{v' \otimes w\}, \quad T = P \sqcup Q \sqcup \{v \otimes w\}$$

である. すると,

$$\begin{aligned} D(S) &= D(P \sqcup Q \sqcup \{v' \otimes w\}) \\ &= D(P \sqcup Q \sqcup \{v' \otimes w + \sum Q\}) \\ &= D(P \sqcup Q \sqcup \{\sum_{u \in X \smallsetminus \{v\}} u \otimes w\}) \\ &= D(P \sqcup Q \sqcup \{-v \otimes w\}) \\ &= D(P \sqcup Q \sqcup \{v \otimes w\}) \\ &= D(T) \end{aligned}$$

である. 第 2 の等号では命題 4.2.4 (1) を用いた. 第 4 の等号では $\sum X(w) = 0$ を用いた. 第 5 の等号では命題 4.2.4 (2) を用いた. □

以下, $m = ab - d = |X| + |Y| - 1$ とする. $X \otimes Y$ において補集合を取る写像 $C(X \otimes Y, d) \to C(X \otimes Y, m)$, $S \mapsto S^c = X \otimes Y \setminus S$ を考える.

$C(X \otimes Y, d)$ 上の同値関係をもとに, $C(X \otimes Y, m)$ 上の同値関係を次で定める.

定義 4.6.4. $C(X \otimes Y, m)$ 上の同値関係 $\sim$ を $S, T \in C(X \otimes Y, d)$ に対し, $S^c \sim T^c \Leftrightarrow S \sim T$ となるように定める.

この同値関係について次が成り立つ.

定理 4.6.5. $C(X \otimes Y, m)$ 上の同値関係 $\sim$ は次で定義する $C(X \otimes Y, m)$ 上の関係 $\sim$ で生成される同値関係である.

定義 4.6.6. $S, T \in C(X \otimes Y, m)$ が次のどちらかを満たすとき, $S \sim T$ とする.

(1) $|S \cap X(w)| = |T \cap X(w)| = 1$ かつ, $S \setminus X(w) = T \setminus X(w)$ を満たす $w \in W$ が存在.

(2) $|S \cap Y(v)| = |T \cap Y(v)| = 1$ かつ $S \setminus Y(v) = T \setminus Y(v)$ を満たす $v \in V$ が存在.

$C(X \otimes Y, m)$ は, $v \otimes w \in X \otimes Y$ を $v \in X$ と $w \in Y$ を結ぶ辺とみなすことで, 自然に $\mathcal{G}_m(X, Y)$ と同一視できる. この同一視のもと, $C(X \otimes Y, m)$ 上の同値関係 $\sim$ は, 定義 3.2.5 で定めた $\mathcal{G}_m(X, Y)$ 上の同値関係と同じものとみなせる.

$X \otimes Y$ の部分集合 S の一次従属性について考える. 次は明らか.

命題 4.6.7. (1) $X(w) \subset S$ となる $w \in W$ が存在するとき, S は一次従属.

(2) $Y(v) \subset S$ となる $v \in V$ が存在するとき, S は一次従属.

次も命題 4.6.3 より明らか.

命題 4.6.8. $S \sim T$ となる $S, T \in C(X \otimes Y, d)$ に対し, S が一次従属なら, T も一次従属.

この 2 つの命題から次が成り立つ.

命題 4.6.9. $S \in C(X \otimes Y, d)$ とする. 次は同値.

(1) S は一次独立.

(2) S^c は木.

証明. (1)⇒(2) を示す. S^c が木でないとすると, 命題 3.1.13 より S^c は閉路をもつ. このとき, 命題 3.2.10 より, S^c は孤立点 $v \in X$ (または $w \in Y$) をもつグラフ T^c に同値である. このとき, $Y(v) \subset T$ (または $X(w) \subset T$) である. よって, 命題 4.6.7 より, T は一次

従属. いま $S \sim T$ だったから, 命題 4.6.8 より, S も一次従属となり矛盾する.

(2)⇒(1) を示す. S が一次従属とすると, $Y(v) \subset T$ (または $X(w) \subset T$) となる $v \in X$ (または $w \in Y$) が存在する. このとき, $S^c \cap Y(v) = \emptyset$ (または $S^c \cap X(w) = \emptyset$), つまり v (または w) は S^c において孤立点である. これは S^c が木であることに矛盾する. □

当初の目的であった定理 4.4.5 (2) を証明する.

定理 4.4.5 (2) の証明. $S, T \in C(X \otimes Y, d)$ がどちらも一次独立とする. 命題 4.6.9 より, S^c, T^c はどちらも木である. よって, 定理 3.2.11 より, $S^c \sim T^c$ である. よって $S \sim T$ であり, $D(S) = D(T)$. □

参考文献

[B] C. ベルジュ, 組合せ論の基礎 (野崎昭弘 訳), サイエンス社 (1973).

[D] R. ディーステル, グラフ理論 (根上生也 · 太田克弘 訳), シュプリンガー · ジャパン (2000).

[LL] T. Y. Lam and K. H. Leung, *On the cyclotomic polynomial* $\Phi_{pq}(X)$, Amer. Math. Monthly, (1918), 562–564.

[Ma] I. G. Macdonald, "Symmetric Functions and Hall Polynomials Second Edition", Oxford University Press Inc., New York (1995).

[Mi] A. Migotti, *Zur Theorie der Kreisteilungsgleichung*, S.-B. der Math.-Naturwiss. Classe der Kaiser. Akad. der Wiss., Wien **87** (1883), 7–14.

[Mo] P. Moree, *Inverse cyclotomic polynomials*, J. Number Theory, **129** (2009), 667–680.

[T] R. Thangadurai, *On the Coefficients of Cyclotomic Polinomials*, Cyclotomic fields and related topics (Pune 1999), 311–322, Bhaskaracharya Pratishthana Pune 2000.

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