円分体の最大実部分体の整数環について

山縣　幸司　(Koji Yamagata)*

概　　要

ζ_n を 1 の原始 n 乗根とする．円分体 $\mathbb{Q}(\zeta_n)$ の最大実部分体の整数環が $\mathbb{Z}[\zeta_n+\zeta_n^{-1}]$ であることはよく知られている．本稿では実円分多項式の終結式を用いたこの結果の別証明を紹介する．さらに，円分体の最大実部分体の判別式の計算も紹介する．

1. 導入

1.1. 代数体の整数環

まず基本的な言葉の定義を復習する．K を代数体とする．K の元 α がある $a_1,\dots,a_m\in\mathbb{Z}$ により $\alpha^m+a_1\alpha^{m-1}+\cdots+a_{m-1}\alpha+a_m=0$ となるとき，α を**代数的整数**という．K に属する代数的整数全体の集合は可換環をなし，これを K の**整数環**という．

K の元 α の $\mathbb{Q}$ 上の共役元を $\alpha^{(1)},\dots,\alpha^{(n)}(\alpha^{(1)}=\alpha,\ n=[K:\mathbb{Q}])$ と表し，$\{\omega_1,\dots,\omega_n\}$ を K の整数環の $\mathbb{Z}$ 上の基底とする．このとき，K の**判別式** $d(K)$ を $d(K)=\Delta(\omega_1,\dots,\omega_n)^2$ で定義する．ただし，$\Delta(\omega_1,\dots,\omega_n):=\det\big(\big(\omega_j^{(i)}\big)_{i,j}\big)$ である．

1.2. 円分体の整数環

円分体の整数環に関しては基本的な以下の定理が知られている．

定理 1 $\zeta_n\in\bar{\mathbb{Q}}$ を 1 の原始 n 乗根とするとき，円分体 $\mathbb{Q}(\zeta_n)$ の整数環は $\mathbb{Z}[\zeta_n]$ である．

定理 1 は従来，体の判別式の議論を用いて、n が素数ベキの場合に帰着することにより証明されている (例えば [Wa])．一方で，Lüneburg は素数べき分体の議論を介さずに，$\mathbb{Z}[\zeta_n]$ がデデキント環であることを直接示すことにより定理 1 の別証明を与えた [Lü].

1.3. 円分体の最大実部分体の整数環

本稿における主結果は [Lü] における Lüneburg の方法を円分体の最大実部分体 $\mathbb{Q}(\zeta_n+\zeta_n^{-1})$ に適用することである [YY].

定理 2 円分体の最大実部分体 $\mathbb{Q}(\zeta_n+\zeta_n^{-1})$ の整数環は $\mathbb{Z}[\zeta_n+\zeta_n^{-1}]$ である．

定理 2 の従来の証明としては円分体の整数環に帰着する証明 [Wa] や，体の判別式と分岐群の議論を用いる証明 [Li] がある．

2. Lüneburg の方法の円分体の最大実部分体への適用

2.1. 準備

定理 2 の別証明に必要な Chebyshev 多項式や実円分多項式の性質や，それらの判別式及び終結式について述べる．

* 〒 466-8555 愛知県名古屋市昭和区御器所町　名古屋工業大学 大学院工学研究科
e-mail: 26417625@stn.nitech.ac.jp

2.1.1. 実円分多項式と Chebyshev 多項式

定義 3 $\Phi_n(x)$ を n 円分多項式とする．また，$n \leq 3$ に対し，$\zeta_n + \zeta_n^{-1}$ の $\mathbb{Q}$ 上最小多項式を $\Psi_n(x)$ とし，**実円分多項式**と呼ぶ．

定義 4 正規化された第1種，第2種，第3種，第4種 Chebyshev 多項式 $C_n, S_n, V_n, W_n \in \mathbb{Z}[x]$ を次を満たすように定義する：

$$C_n(2\cos\theta) = 2\cos n\theta, \quad S_n(2\cos\theta) = \frac{\sin n\theta}{\sin\theta},$$

奇数 n に対し，

$$V_n(2\cos\theta) = \frac{\cos n\theta/2}{\cos\theta/2}, \quad W_n(2\cos\theta) = \frac{\sin n\theta/2}{\sin\theta/2}.$$

補題 5 (Chebyshev 多項式の微分)

$$C_n'(x) = nS_n(x),$$

$$V_n'(x) = \frac{nW_n(x) - V_n(x)}{2(x+2)}, \quad W_n'(x) = \frac{nV_n(x) - W_n(x)}{2(x-2)}.$$

補題 6 多項式 $x^n - 1$ の $\mathbb{Q}$ 上既約因子分解は次のようになる．

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

Lüneburg の方法が円分体の最大実部分体に適用できるのは，実円分多項式についても補題6と同様な以下の補題が成り立つためである．

補題 7 [Y13] Chebyshev 多項式の $\mathbb{Q}$ 上既約因子分解は次のようになる．

$$C_n(x) = \prod_{d|n,\ n/d:odd} \Psi_{4d}(x), \quad S_n(x) = \prod_{2<d|2n} \Psi_d(x),$$

$$V_n(x) = \prod_{1<d|n} \Psi_{2d}(x), \quad W_n(x) = \prod_{1<d|n} \Psi_d(x).$$

2.1.2. 終結式と判別式

定義 8 多項式 $f(x) = a_0(x-\alpha_1)\cdots(x-\alpha_n)$, $g(x) = b_0(x-\beta_1)\cdots(x-\beta_m)$ に対し，f, g の**終結式** $\mathrm{Res}(f,g)$ を $\mathrm{Res}(f,g) = a_0^m b_0^n \prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j)$ で定義する．

定義 9 モニックな多項式 $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$ の**判別式** $\mathrm{Disc}(f)$ を $\mathrm{Disc}(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2$ で定義する．

Chebyshev 多項式の終結式と補題7を用いると，実円分多項式の終結式 $\mathrm{Res}(\Psi_n, \Psi_m)$ の計算ができる [Y15]．ϕ をオイラー関数とする．

命題 10 (実円分多項式の終結式) $n, m \geq 3$ に対し，

$$|\mathrm{Res}(\Psi_n, \Psi_m)| = \begin{cases} p^{\frac{\phi(m)}{2}} & (m \mid n \text{かつ} \frac{n}{m} \text{が素数} p \text{のべきになっているとき}); \\ 1 & (\text{その他}). \end{cases}$$

円分多項式の終結式の計算も [Tm, Fe, GD, Le, Lo, Lü] においてなされている．

命題 11

$$\mathrm{Res}(\Phi_n, \Phi_m) = \begin{cases} p^{\frac{\phi(m)}{2}} & (m \mid n \text{かつ} n/m \text{が} p \text{べきになっているとき（} p \text{は素数)}); \\ 1 & (\text{その他}). \end{cases}$$

また，$\mathrm{Disc}(f) = (-1)^{n(n-1)/2}\mathrm{Res}(f, f')$ であるから，補題 5 と補題 7 を使えば，実円分多項式の判別式が計算できる．

命題 12 (実円分多項式の判別式)

$$\mathrm{Disc}(\Psi_n(x)) = \begin{cases} 2^{(m-1)2^{m-2}-1} & (n = 2^m,\ m > 2 \text{のとき}); \\ p^{\frac{mp^m-(m+1)p^{m-1}-1}{2}} & (n = p^m \text{か} n = 2p^m \ (p \text{は奇素数}) \text{のとき}); \\ \dfrac{n^{\frac{\phi(n)}{2}}}{\prod_{i=1}^{t} p_i^{\frac{\phi(n)}{2(p_i-1)}}} & (\text{その他}). \end{cases}$$

実円分多項式の判別式は Lehmer によって組合せ論的な方法でも計算されている [Le]．なお，円分多項式の判別式は次のようになる (例えば [Wa])．

$$\mathrm{Disc}(\Phi_n) = (-1)^{\phi(n)/2}\frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}.$$

2.2. 定理 2 の別証明の概略

まず，$\theta = \zeta_n + \zeta_n^{-1},\ K = \mathbb{Q}(\theta),\ R = \mathbb{Z}[\theta]$ とする．R が整閉であることを示すために，R がデデキント環であることを示す．R がデデキント環であることは任意の極大イデアル $P \subset R$ に対し，その局所化 $R_P := (R \setminus P)^{-1}R$ が離散付値環であることと同値である．$p\mathbb{Z} = P \cap \mathbb{Z}$ により素数 p を定める．

(i) $\underline{p \nmid n \text{のとき}}$　命題 12 より，このとき実円分多項式 Ψ_n の判別式は p で割り切れない．よって，Ψ_n は $\mathbb{F}_p$ 上で分離多項式であるので，以下の補題が適用できる．

補題 13 [Lü] θ を代数的整数とし，$f(x)$ を θ の $\mathbb{Q}$ 上の最小多項式とする．p を素数とし，$P \subset \mathbb{Z}[\theta]$ を極大イデアルで $P \cap \mathbb{Z} = p\mathbb{Z}$ を満たすものとする．$\mu(\theta) \in P$ で次数が最小であるモニックな $\mathbb{Z}$ 係数多項式を $\mu(x)$ とおく．このとき，$f = \mu h + pg$ をみたす多項式 $g(x), h(x) \in \mathbb{Z}[x]$ が存在する．さらに，μ, g, h が $\mathbb{F}_p$ 上で共通因子をもたなければ，$\mathbb{Z}[\theta]$ の極大イデアル P による局所化は離散付値環である．

(ii) $\underline{p \mid n \text{のとき}}$　$n = mp^e\ (p \nmid m, e > 0)$ とする．R_P の極大イデアル PR_P が単項イデアルであることを示せばよい．補題 7 と命題 10 の実分多項式の終結式の値を用いることで，$\Psi_n(x) = \Psi_m(x)^{\phi(p^e)} + pg(x)$ を満たす $\mathbb{Z}$ 係数の多項式 $g(x)$ が存在し，$g(\theta)$ が R の単元であることが示される．$\varepsilon = -g(\theta)^{-1} \in R$ とおくと，

$$p = \Psi_m(\theta)^{\phi(p^e)}\varepsilon \in R \tag{1}$$

である．$\nu(x)$ を $\theta + P$ の $(\mathbb{Z}+P)/P \cong \mathbb{F}_p$ 上の最小多項式とすると，$\nu(x)$ は $\Psi_n(x)$ を $\mathbb{F}_p$ 上の多項式として割り切る．よって，$\nu(x)$ は $\Psi_m(x)$ を割り切るので，

$$\Psi_m(x) = \nu(x)H(x) + pG(x) \tag{2}$$

を満たす $\mathbb{Z}$ 係数多項式 $H(x), G(x)$ が存在する．(1) に (2) を代入し展開することで，$p = \nu(\theta)\alpha_1 + p^{\phi(p^e)}\beta_1$ を満たす R の元 α_1, β_1 がとれる．(2) の右辺の p に同式左辺の p を代入することを繰り返せば，任意の正整数 i に対して

$$p = \nu(\theta)\alpha_i + p^{\phi(p^e)^i}\beta_i$$

を満たす α_i, β_i の存在がわかる．ベキ零根基はすべての素イデアルの共通部分に等しいので，剰余環 $R_P/\nu(\theta)R_P$ のただ一つの素イデアル $PR_P/\nu(\theta)R_P$ は $R_P/\nu(\theta)R_P$ のベき零根基である．よって，$p^N \in \nu(\theta)L$ をみたす正の整数 N が存在する．$\phi(p^e) \geq 2$ であったので $\phi(p^e)^i \geq N$ となる i がある．よって，$p = \nu(\theta)\alpha_i + p^{\phi(p^e)i}\beta_i \in \nu(\theta)L$ であるから，

$$PR_P = pR_P + \nu(\theta)R_P = \nu(\theta)R_P$$

である．

注 14 (円分体の最大実部分体の判別式) 定理 2 より，$\{1, \ldots, \zeta_n^{\phi(n)/2-1}\}$ は $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ の整数環の $\mathbb{Z}$ 上の基底であるから，$d(\mathbb{Q}(\zeta_n + \zeta_n^{-1})) = \mathrm{Disc}(\Psi_n)$ である．

参考文献

[Tm] Apostol, Tom M. Resultants of cyclotomic polynomials. Proc. Amer. Math. Soc. 24 1970 457–462.

[Fe] Diederichsen, Fritz-Erdmann. Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz. (German) Abh. Math. Sem. Hansischen Univ. 13, (1940). 357–412.

[GD] Dresden, Gregory. Resultants of cyclotomic polynomials. Rocky Mountain J. Math. 42 (2012), no. 5, 1461–1469.

[Sa] Jeong, Sangtae. Resultants of cyclotomic polynomials over $\mathbb{F}_q[T]$ and applications. Commun. Korean Math. Soc. 28 (2013), no. 1, 25–38.

[Le] Lehmer, D. H. An extended theory of Lucas' functions. Ann. of Math. (2) 31 (1930), no. 3, 419–448.

[Li] Liang, Joseph J. On the integral basis of the maximal real subfield of a cyclotomic field. J. Reine Angew. Math. 286/287 (1976), 223–226.

[Lo] Louboutin, Stéphane. Resultants of cyclotomic polynomials. Publ. Math. Debrecen 50 (1997), no. 1-2, 75–77.

[Lü] Lüneburg, Heinz. Resultanten von Kreisteilungspolynomen. (German) Arch. Math. (Basel) 42 (1984), no. 2, 139–144.

[Wa] Washington, Lawrence C. Introduction to cyclotomic fields. Second edition. Graduate Texts in Mathematics, 83. Springer-Verlag, New York, 1997.

[YY] Yamagata, Koji and Yamagishi, Masakazu. On the ring of integers of real cyclotomic fields. (投稿中).

[Y13] Yamagishi, Masakazu. A note on Chebyshev polynomials, cyclotomic polynomials and twin primes, Journal of Number Theory 133 (2013) 2455–2463.

[Y15] Yamagishi, Masakazu. Resultants of Chebyshev Polynomials: The First, Second, Third, and Fourth Kinds. Canad. Math. Bull. 58 (2015), no. 2, 423–431.