11. 円分多項式

正 17 角形の作図可能性が初めて発見されたのは 1796 年, 当時 19 才であった Gauss によりますが, この時彼が発見したのは単なる作図法ではなく, 「円周等分の原理」そのものでした. この時代は正 17 角形の作図というだけでも大発見だったので, その印象が強かったわけですが, 実際には Gauss はもっと奥深い理論を構築しつつあったわけです. (前回書いた正 257 角形や正 65537 角形にしても, 「作図可能であること」自体は Gauss によって既に明らかにされていました.) 森田先生の講義で最後に皆さんが学んだのは, まさにその「円周等分の原理」だったわけですが, 今回のプリントではそれを振り返っていきたいと思います. (今回は演習問題はありません.)

---

n を正整数, $\xi = e^{\frac{2\pi\sqrt{-1}}{n}} = \cos(2\pi/n) + \sqrt{-1}\sin(2\pi/n)$ とすると, ξ は 1 の原始 n 乗根となります. このとき,

正 n 角形が定木とコンパスで作図可能 $\Leftrightarrow$ 拡大次数 $[\mathbb{Q}(\xi) : \mathbb{Q}]$ が 2 のベキ

となることは前回の授業でも軽くお話しました. (円と直線しか描けないので, 作図可能なのは $\mathbb{Q}$ から四則演算と平方根によって構成される数のみ. 逆に, 2 次方程式は定木とコンパスで必ず解くことができる.) すると, 拡大次数 $[\mathbb{Q}(\xi) : \mathbb{Q}]$ は ξ の $\mathbb{Q}$ 上最小多項式の次数と一致するので, その最小多項式に興味が移ります.

さて, 1 の n 乗根はすべて ξ^m $(m \in \mathbb{Z})$ という形をしていますが, そのうち原始 n 乗根になるのは $\mathrm{GCD}(m, n) = 1$ となるもののみです. それら 1 の原始 n 乗根たちを根にもつ多項式

$$F_n(X) = \prod_{\substack{1 \le m \le n \\ \mathrm{GCD}(m,n)=1}} (X - \xi^m)$$

を**円分多項式** (**円周等分多項式**) といいます. 実は, この $F_n(X)$ は整数係数多項式 $(F_n(X) \in \mathbb{Z}[X])$ で, しかも $\mathbb{Q}$ 上既約であることが証明できます ($\mathbb{Q}$ 上既約であることの証明は森田先生のプリントに書いてあるのでこちらでは省略します). 従って, $F_n(X)$ が ξ の $\mathbb{Q}$ 上最小多項式になります.

定義より $F_n(X)$ の次数は 1 から n までの自然数のうち n と互いに素なものの個数と一致するわけですが, その数は **Euler 関数**と呼ばれ, $\varphi(n)$ と書きます:

$$\varphi(n) = \#\{m \in \mathbb{Z} \mid 1 \le m \le n,\ \mathrm{GCD}(m, n) = 1\} = \#(\mathbb{Z}/n\mathbb{Z})^\times.$$

p を素数, k を正整数とする時, $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$ となることは簡単に分かります (1 から p^k までの間に p の倍数が p^{k-1} 個あることが k に関する帰納法により分かる). 一般に, $n = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}$ ($p_1, \ldots, p_l$ は相異なる素数) と素因数分解され

るとき, 中国剰余定理により $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{k_1})^\times \times \cdots \times (\mathbb{Z}/p_l^{k_l}\mathbb{Z})^\times$ なので, $\varphi(n)$ は

$$\varphi(n) = \varphi(p_1^{k_1}) \cdots \varphi(p_l^{k_l}) = \prod_{i=1}^{l} p_i^{k_i-1}(p_i - 1)$$

と計算されます. これが 2 のベキであるためには各 $p_i^{k_i-1}(p_i-1)$ が 2 のベキでなければなりませんが, それは $p_i = 2$ であるか, または, $k_i = 1$ かつ p_i がフェルマー素数のときに限られます. (z を自然数とするとき, 2^z+1 が素数ならば z は 2 のベキでなければならない. なぜなら, z がある奇素数 q を約数にもち $z = qz'$ であったとすると, $2^z+1 = (2^{z'})^q + 1 = (2^{z'}+1)((2^{z'})^{q-1} - (2^{z'})^{q-2} + \cdots + 1)$ となって必ず合成数になってしまうから.) 以上から,

$$\begin{aligned} & \text{正 } n \text{ 角形が定木とコンパスで作図可能} \\ \Leftrightarrow\ & [\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n) \text{ が 2 のベキ} \\ \Leftrightarrow\ & n = 2^k p_1 \cdots p_l \quad (p_1, \ldots, p_l \text{ は相異なるフェルマー素数}) \end{aligned}$$

となって, 作図可能な正 n 角形が特定できるわけです.

正 n 角形が作図可能であることが分かっても, 実際の作図方法を調べるには円分多項式 $F_n(X)$ の根を (段階的にいくつかの 2 次方程式を解きつつ) 求める必要があります. それには $F_n(X)$ の整数係数多項式としての具体的な形を知っておく方が良いのですが, その具体的な形というのは Möbius 関数を使って表されます.

Möbius 関数 $\mu : \mathbb{N} \to \mathbb{C},\ m \mapsto \mu(m)$ とは次のように定義されます:

1. $\mu(1) = 1$,
2. ある素数 p があって $p^2 | m$ となるなら $\mu(m) = 0$,
3. 上記以外のとき, $m = p_1 \cdots p_l$ ($p_1, \ldots, p_l$ は相異なる素数) と素因数分解されるとすると $\mu(m) = (-1)^l$.

この μ に関して, 次のことがいえます. ($\sum_{d|m}$ は m の (正の) 約数全体をわたる和.)

命題 11.1. $\displaystyle\sum_{d|m} \mu(d) = \begin{cases} 1 & (m = 1) \\ 0 & (m > 1). \end{cases}$

[証明] $m = 1$ のときは明らか. $m > 1$ のとき, m を素因数分解して $m = p_1^{k_1} \cdots p_l^{k_l}$ と

すると

$$\begin{aligned}\sum_{d|m}\mu(d) &= \sum_{0\le x_i\le k_i\ (i=1,\dots,l)}\mu(p_1^{x_1}\cdots p_l^{x_l})\\ &= \mu(1)+\{\mu(p_1)+\cdots+\mu(p_l)\}+\{\mu(p_1p_2)+\mu(p_1p_3)+\cdots+\mu(p_{l-1}p_l)\}\\ &\quad +\cdots+\mu(p_1\cdots p_l)\\ &= \sum_{i=0}^{l}\left(\begin{array}{c} l \\ i \end{array}\right)(-1)^i=(1-1)^l=0. \qquad \square\end{aligned}$$

これにより, $F_n(X)$ の形が次のように分かります:

命題 11.2. (1) $F_n(X)=\prod_{d|n}(X^d-1)^{\mu\left(\frac{n}{d}\right)}$.

(2) $F_n(X)\in\mathbb{Z}[X]$.

[証明] (1) 一般に, m を自然数とするとき, 1 の原始 m 乗根全体に, m の各約数 d に対する 1 の原始 d 乗根全体を次々加えていけば, 最終的に 1 のすべての m 乗根を得る. 別の言い方をすれば,

$$\{1,\dots,m\}=\bigcup_{d|m}\{z\in\mathbb{N}\mid 1\le z\le m,\ \mathrm{GCD}(z,m)=\frac{m}{d}\}.$$

よって,

$$X^m-1=\prod_{i=1}^{m}(X-\xi^i)=\prod_{d|m}F_d(X)$$

を得る (この式は森田先生のプリントにある $F_n(X)$ の既約性の証明の最後のところで重要ですね). これを使って, 証明したい式の右辺を変形していけば,

$$\prod_{d|n}(X^d-1)^{\mu\left(\frac{n}{d}\right)}=\prod_{d|n}\prod_{d'|d}F_{d'}(X)^{\mu\left(\frac{n}{d}\right)}=\prod_{d'|n}\prod_{d''|\frac{n}{d'}}F_{d'}(X)^{\mu(d'')}=\prod_{d'|n}F_{d'}(X)^{\sum_{d''|\frac{n}{d'}}\mu(d'')}=F_n(X).$$

上式の二番目の等式は, n の約数 d' に対して $\{\frac{n}{d}\mid d|n,\ d'|d\}=\{d''\mid d''|\frac{n}{d'}\}$ が成り立つことによる. 最後の等式は命題 11.1 による.

(2) (1) 右辺の分子を $P(X)$, 分母を $Q(X)$ とすると,

$$\frac{P(X)}{Q(X)}=F_n(X)\in\mathbb{C}[X]$$

より, $\mathbb{C}[X]$ の元として $Q(X)|P(X)$ でなければならないが, $Q(X)$ の最高次の係数が 1 で $P(X)\in\mathbb{Z}[X]$ だから, 割り算のときに, 係数に整数以外のものがでてくるはずがない. よって $F_n(X)\in\mathbb{Z}[X]$. $\square$

例. $n = p$: 素数のときは,

$$F_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

合成数の場合, 例えば,

$$\begin{aligned}
F_4(X) &= \frac{X^4 - 1}{X^2 - 1} = X^2 + 1 \\
F_6(X) &= \frac{(X^6 - 1)(X - 1)}{(X^3 - 1)(X^2 - 1)} = X^2 - X + 1 \\
F_8(X) &= \frac{X^8 - 1}{X^4 - 1} = X^4 + 1 \\
F_9(X) &= \frac{X^9 - 1}{X^3 - 1} = X^6 + X^3 + 1 \\
F_{10}(X) &= \frac{(X^{10} - 1)(X - 1)}{(X^5 - 1)(X^2 - 1)} = X^4 - X^3 + X^2 - X + 1 \\
F_{12}(X) &= \frac{(X^{12} - 1)(X^2 - 1)}{(X^6 - 1)(X^4 - 1)} = X^4 - X^2 + 1 \\
F_{14}(X) &= \frac{(X^{14} - 1)(X - 1)}{(X^7 - 1)(X^2 - 1)} = X^6 - X^5 + X^4 - X^3 + X^2 - X + 1 \\
F_{15}(X) &= \frac{(X^{15} - 1)(X - 1)}{(X^5 - 1)(X^3 - 1)} = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1 \\
F_{16}(X) &= \frac{(X^{16} - 1)}{(X^8 - 1)} = X^8 + 1
\end{aligned}$$

正 15 角形の作図法 (ヒントだけ).

$\varphi = 2\pi/15$, $\xi = \cos\varphi + \sqrt{-1}\sin\varphi$ とする. $F_{15}(\xi) = 0$ より,

$$-\xi^8 + \xi^7 + \xi^4 + \xi = \xi^5 + \xi^3 + 1.$$

$\cos 8\varphi = \cos(15 - 8)\varphi = \cos 7\varphi$ に注意して両辺の実部のみをみると,

$$\cos 4\varphi + \cos\varphi = \cos\frac{2\pi}{3} + \cos\frac{2\pi}{5} + 1$$

を得る. $\cos(2\pi/3)$ と $\cos(2\pi/5)$ はそれぞれ正 3 角形, 正 5 角形の作図の際に既に作図できている. $c = \cos(2\pi/3) + \cos(2\pi/5)$ とおく. $2\cos\alpha\cos\beta = \cos(\alpha+\beta) + \cos(\alpha-\beta)$ に注意すれば,

$$2\cos 4\varphi\cos\varphi = c$$

を得るので, $\cos 4\varphi$ と $\cos\varphi$ は 2 次方程式

$$x^2 - (c+1)x + \frac{1}{2}c = 0$$

の解である. だからこれを定木とコンパスで解けば $\cos\varphi$ の作図が可能である.