# コンパスと定規(目盛なし)を用いた作図

2023年8月30日

※正十七角形の作図が可能であることの証明を書きましたが, 修正および加筆の可能性はあります.

## 1　導入(定義と基本的な性質)

※記法: Card で, 有限集合の元の個数を表す.
本ファイルでは, コンパスと定規(目盛なし)で作図可能な点に関して扱う. なお, 体論の基礎(拡大次数など)は前提知識とする. また, 具体例の紹介において, アイゼンシュタインの既約判定法および $\mathbb{Z}[X]$ の既約な元などの知識を使う. なお, 基本的に $i$ は虚数単位を表す.

本ファイルは, 文献[1]による議論に基づく. まず, コンパスと定規で作図可能な点を定義する. そのためには, コンパスと定規で可能な操作の範囲を明確にする必要がある.

**定義 1.1.** $S = \{(0,0),(0,1),(1,0)\}$ とおく.
以下の操作が, コンパスと定規で可能である.
操作1: $S$ の2点 $A, B$ を通る直線を定規で引く.
操作2: $S$ の2点 $A, B$ に対して, 点 $A$ を中心として, 半径が線分 $AB$ の長さであるような円をコンパスで描く.
操作3: 操作1,2で描いた図形の交点を $S$ に加える.
操作4: 操作1,2,3で得られる直線, 円および点集合 $S$ をもとに同じ操作を繰り返す.
以上の操作で $S$ に加えることができる点 $(x, y)$ を作図可能な点という.
※ $(0,0)$ と $(1,0)$ を結んだ直線($x$ 軸)および $(0,0)$ と $(0,1)$ を結んだ直線($y$ 軸)は作図可能である.

**定義 1.2.** (1) $x$ を実数とする．$x$ が作図可能とは, 点 $(x, 0)$ が作図可能なことをいう．
(2) $z = x + iy (x, y \in \mathbb{R})$ を複素数とする．$z$ が作図可能とは, 点 $(x, y)$ が作図可能なことをいう．

**補足 1.1.** 以下の操作は, コンパスと定規で作図可能な典型的な操作であり, 断りなしに用いる．

1. 2 点 $A$ と $B$ が与えられたとする．点 $A$ と点 $B$ を通る直線 $\ell$ について, $AB$ の垂直 2 等分線を引く．
2. 点 $A$ と直線 $\ell$ が与えられたとする．このとき, 点 $A$ から直線 $\ell$ に垂線を下ろす．
3. 点 $A$ と直線 $\ell$ が与えられたとする．このとき, 点 $A$ を通り, 直線 $\ell$ に平行な直線を引く．
4. 角の 2 等分線を引く．

**補足 1.2.** 定義 1.1 において, $S$ の初期値を $\{(0, 0), (0, 1), (1, 0)\}$ とおいた．代わりに $\{(0, 0), (0, 1)\}$ を用いても良い．実際, $S$ を用いて, $x$ 軸を引く．その後, コンパスで $(-1, 0)$ を描く．さらに, $(1, 0)$ と $(-1, 0)$ の垂直 2 等分線 ($y$ 軸) を引く．すると, コンパスで $(0, 1)$ を描くことができる．

**補足 1.3.** $x, y$ を実数とする．このとき, 以下の 2 条件は同値である:

条件 1 複素数 $a + ib$ は作図可能.

条件 2 $a, b$ はともに作図可能.

実際, 複素数 $a + ib$ が作図可能ならば, 点 $(a, b)$ は作図可能である．すると, 直線 $x = a$ は作図可能であるため, 点 $(a, 0)$ は作図可能である．よって $a$ は作図可能である．同様に, 直線 $y = b$ および $(0, b)$ が作図可能である．よってコンパスを用いると $(b, 0)$ が作図可能である．したがって, $b$ は作図可能である．

逆に, $a, b$ が作図可能とする．$(a, 0)$ が作図可能のため, 直線 $x = a$ は作図可能である．$(b, 0)$ および $(0, b)$ が作図可能のため, 直線 $y = b$ も作図可能である．以上により, 点 $(a, b)$ は作図可能である．

$$\mathcal{C} = \{x \in \mathbb{R} \mid x \text{ は作図可能 }\},$$

とおく．コンパスを用いることで, $\mathbb{Z} \subset \mathcal{C}$ であることがわかる．次の定理は, $\mathcal{C}$ に関する詳細を述べたものである．

**定理 1.1.** (1) $\mathcal{C}$ は体.
(2) 任意の $a \in \mathcal{C}$ について, $a > 0$ ならば $\sqrt{a} \in \mathcal{C}$.
(3) 任意の $a \in \mathcal{C}$ について, 以下を満たす体の拡大の列

$$K_1 = \mathbb{Q} \subset K_2 \subset \cdots \subset K_n \subset \mathbb{R}$$

が存在する: $a \in K_n$ かつ, 任意の $j = 1, 2, \ldots, n-1$ に対して, 正の実数 $y_j \in K_j$ が存在して, $K_{j+1} = K_j(\sqrt{y_j})$.

**証明.** (1) コンパスを用いることで, $a \in \mathcal{C}$ ならば $-a \in \mathcal{C}$ である．また, $a, b \in \mathcal{C}$ のとき, $a + b \in \mathcal{C}$, $ab \in \mathcal{C}$, $a/b \in \mathcal{C}(b \neq 0)$ を示す．簡単のために, $a, b > 0$ とする．
1-1) $a + b$ について: 点 $(0, b)$ と点 $(-b, 0)$ を結ぶ直線 $\ell_1$(傾き 1) と直線 $\ell_2 : y = b$ は作図可能である．また, 直線 $\ell_1$ と平行な直線 $\ell_3$ で $(a, 0)$ を通るものを考える $(y = x - a)$．すると, $\ell_1$ と $\ell_3$ の交点は $(a + b, b)$ であるため, $a + b$ は作図可能.
1-2) $ab$ について: 点 $(0, 1)$ と点 $(a, 0)$ を結ぶ直線を $\ell_1$ とする．$\ell_1$ に平行で, 点 $(0, b)$ を通る直線 $\ell_2$ は作図可能である．$\ell_2$ と $x$ 軸との交点は, $(ab, 0)$ であるため, $ab$ は作図可能である.
1-3) $a/b$ について: 点 $(0, b)$ と点 $(1, 0)$ を結ぶ直線を $\ell_1$ とする．$\ell_1$ に平行で, 点 $(0, a)$ を通る直線 $\ell_2$ は作図可能である．$\ell_2$ と $x$ 軸との交点は, $(a/b, 0)$ であるため, $a/b$ は作図可能である.
(2) (1) より, $-1, (a-1)/2 \in \mathcal{C}$ である．よって, $(a-1)/2$ を中心とした円

$$\left(x - \frac{a-1}{2}\right)^2 + y^2 = \left(\frac{a+1}{2}\right)^2$$

は作図可能である．この円と $y$ 軸の交点が $(0, \pm\sqrt{a})$ であることは容易に確認できる．よって, $\sqrt{a}$ は作図可能である.
(3) 作図可能性の定義により, $S$ に加えられる点は, 操作 3 によって定義されている．その際, 交点に用いる円または直線に関して, 操作 1 および操作 2 において用いる点 $A, B$ を考察する．ある体 $K(\subset \mathbb{R})$ が存在して, 用

いる点 $A, B$ の $x$ 成分および $y$ 成分すべて $K$ の元であるとする．このとき, 新たに加わる点の $x$ 成分および $y$ 成分は, $K$ の元に平方を取るという操作および加減乗除で得ることができることを示せば, (3) が示される．

例えば, 直線と直線の交点を考える．2 直線は,

$$\begin{cases} ax + by = c \ (a, b, c \in K), \\ dx + ey = f \ (d, e, f \in K) \end{cases}$$

のように表せる．よって交点の $x$ 成分および $y$ 成分も $K$ の元である．一方, 円は以下のように表すことができる:

$$(x - \alpha)^2 + (y - \beta)^2 = \gamma^2 \ (\alpha, \beta, \gamma^2 \in K).$$

ここで, $\gamma^2 \in K$ であることは三平方の定理により従う．よって, 円と直線の交点の $x$ 成分および $y$ 成分は, $K$ の元に平方を取るという操作および加減乗除で得ることができる．円と円の交点についても同様である． □

**補足 1.4.** $K \subset L$ を $\mathbb{C}$ の部分体とする．このとき, 以下の 2 条件は同値である:

条件 1　$[L : K] = 2$.

条件 2　ある $z \in L \backslash K$ で, $z^2 \in K$ かつ $L = K(z)$ を満たすものが存在する．

**証明.** まず条件 2 が成立すると仮定すると, $z$ の $K$ 上の次数が 2 であるため, 条件 1 が成立する．逆に条件 1 が成立すると仮定する．すると, $K$ 上の次数 2 の元 $w \in L$ が存在して, $L = K(w)$ である．さて, $w$ の $K$ 上最小多項式を $X^2 + bX + c$ とする $(b, c \in K)$．すると,

$$w \in \left\{ \frac{-b + \sqrt{b^2 - 4c}}{2}, \frac{-b - \sqrt{b^2 - 4c}}{2} \right\}$$

である．よって, $z = \sqrt{b^2 - 4c}$ と置けばよい． □

さて, 次に

$$\widetilde{\mathcal{C}} = \{z \in \mathbb{C} \mid z \text{ は作図可能 }\}$$

とおく．$\mathcal{C}$ は体であるため, 補足 1.3 により以下が成立する:

$$\widetilde{\mathcal{C}} = \{x + yi \mid x, y \in \mathcal{C}\} = \mathcal{C}(i).$$

特に $\widetilde{\mathcal{C}}$ は体である．定理 1.1 より以下が従う．

**定理 1.2.** (1) 任意の $z \in \widetilde{\mathcal{C}}$ について, $\sqrt{z} \in \widetilde{\mathcal{C}}$. ただし, $\sqrt{z}$ は $(\sqrt{z})^2 = z$ を満たす複素数であるが, 一意には定まらない. (2) 任意の $z \in \widetilde{\mathcal{C}}$ について, 以下を満たす体の拡大の列

$$K_1 = \mathbb{Q} \subset K_2 \subset \cdots \subset K_n \subset \mathbb{C}$$

が存在する: $z \in K_n$ かつ, 任意の $j = 1, 2, \ldots, n-1$ に対して, 正の実数 $y_j \in K_j$ が存在して, $K_{j+1} = K_j(\sqrt{y_j})$.

**証明.** (2) は定理 1.1 の (3) より従う. さて, (1) を証明する.
$\sqrt{z} = x + yi (x, y \in \mathbb{R})$, $z = a + bi$ $(a, b \in \mathcal{C})$ とおく. すると, $(\sqrt{z})^2 = (x^2 - y^2) + 2xyi$ より,

$$\begin{cases} x^2 - y^2 = a \\ 2xy = b \end{cases}$$

である. $b = 0$ の場合は, $x = 0$ または $y = 0$ であるため, 定理 1.1 の (2) より, $x, y \in \mathcal{C}$ であることがわかる. 以下, $b \neq 0$ とする. $y = (b/2) \cdot x^{-1}$ を $x^2 - y^2 = a$ に代入すると,

$$x^4 - ax^2 - \frac{b^2}{4} = 0$$

となる. $x^2$ は 2 次方程式 $t^2 - at - \frac{b^2}{4} = 0$ の根であることに注意する. 2 次方程式の解の公式により, 再び定理 1.1 の (2) を用いると, $x^2 \in \mathcal{C}$ および $x \in \mathcal{C}$ であることがわかる (補足 1.4 も参照). このとき, $y = (b/2) \cdot x^{-1} \in \mathcal{C}$ も成立する. □

## 2 作図不可能な数の例

**系 2.1.** 任意の $z \in \widetilde{\mathcal{C}}$ は代数的数である. さらに, ある非負整数 $k$ が存在して, $[\mathbb{Q}(z) : \mathbb{Q}] = 2^k$ を満たす.

**例 2.1.** $\sqrt[3]{2}$ は作図不可能である. この事実は, 立方体の倍積問題と関連が深い. 立方体の体積を 2 倍するには, 1 辺の長さを $\sqrt[3]{2}$ 倍する必要がある. この問題はプラトンによって数学的な課題としてとらえられた. 系 2.1 により, この課題は, "コンパスと定規では不可能" と結論付けることができる.

**例 2.2.** 与えられた円と同じ面積を持つ正方形はコンパスと定規で作図可能であるか, という問い (円積問題) が古代ギリシャで考えられた. 円積問題は, 円周率の平方根 $\sqrt{\pi}$ が作図可能かという問題に言い換えることができる. さらに, これは円周率 $\pi$ 自身が作図可能かどうかという問題と等価である. 1882 年にリンデマンが $\pi$ は代数的数ではない (超越数である) ことを証明した. これにより, 円積問題は不可能であると結論付けることができる. $\pi$ の超越性の証明に関しては, 例えば文献 [3] に書かれている.

**例 2.3.** 角の二等分がコンパスと定規で可能である一方, 実は角の三等分は常に可能であるとは限らない. 以下, 三等分不可能な例を紹介する. 角度 $\theta(0 < 3\theta < \pi/2)$ で, $\cos 3\theta = 3/16$ を満たすものを考える. $\sin^2 3\theta = 1 - \cos^2 3\theta$ より, 点 $(\cos 3\theta, \sin 3\theta)$ は作図可能である. よって角度 $3\theta$ は作図可能である. 一方, 角度 $\theta$ は作図不可能である. 実際, 角度 $\theta$ が作図可能であると仮定すると, コンパスを用いることで (原点中心, 半径 1 の円を描く) 点 $(\cos\theta, \sin\theta)$ は作図可能である. 特に, $\cos\theta \in \mathcal{C}$ である. 一方, 3 倍角の公式より,

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta = \frac{3}{16}$$

が成立する. さて, $\alpha = 4\cos\theta$ とおくと, $\alpha \in \mathcal{C}$ である.

一方, $64\cos^3\theta - 48\cos\theta - 3 = 0$ より

$$\alpha^3 - 12\alpha - 3 = 0$$

である. さて, 素数 3 に関してアイゼンシュタインの既約判定法を用いると, $X^3 - 12X - 3$ は $\mathbb{Z}[X]$ における既約元, さらには $\mathbb{Q}[X]$ における既約元であることもわかる (ガウスの補題). よって,

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$$

となるが, これは $\alpha \in \mathcal{C}$ に矛盾する. 以上により, 角度 $\theta$ は作図不可能である.

**補足 2.1.** 系 2.1 の逆は成立しない. つまり, 代数的数 $\alpha$ について, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$ を満たす整数 $m$ が存在するからといって, $\alpha$ が作図可能とは限らない. 実際, $\alpha$ が作図可能であれば, 定理 1.2(2) により, "平方根" を用いて, $\alpha$ を表す表示式がある. ところが, 特に $m \geq 3$ の場合, "ほとんどの場合, 平方根はおろか, $n$ 乗根を用いても $\alpha$ を表示できない" ことが知られて

いる．この表現はあいまいであるため, Galois 理論を知っている方のために, Galois 群を用いた表現をする．$n$ を正整数とする．また, $H$ を正整数とする．$A_H$ で, 以下の性質を満たす $n$ 次多項式 $P(X) \in \mathbb{Z}[X]$ の個数を表す: 各係数の絶対値が $H$ 以下．$B_H$ で, 上記の性質に加えて, $P(X) = 0$ に関する Galois 群が $S_n$($n$ 次対称群) であるものの個数を表す．すると,

$$\lim_{H \to \infty} \frac{B_H}{A_H} = 1$$

が成立する．

# 3　作図可能な正 $n$ 角形

本章以降, 正 $n$ 角形といえば $n$ は 3 以上の整数とする．また, 複素数 $\zeta_n$ を

$$\zeta_n := \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$$

とおく．また, 指数関数 exp を用いると, $\zeta_n = \exp(2\pi i/n)$ と書くこともできる．

**定義 3.1.** 正 $n$ 角形が作図可能とは,

$$\{\zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}, \zeta_n^n (= 1)\} \subset \widetilde{\mathcal{C}}$$

が成り立つことと定義する．なお, 上記の数式の左辺は実際に複素平面上における正 $n$ 角形であることに注意する．

**補足 3.1.** $\widetilde{\mathcal{C}}$ が体であることから, 正 $n$ 角形が作図可能とは, $\zeta_n \in \widetilde{\mathcal{C}}$ であることに他ならない．さらに, $\cos^2(2\pi/n) + \sin^2(2\pi/n) = 1$ であることから, これは $\cos(2\pi/n) \in \mathcal{C}$ であることに他ならない．

**命題 3.1.** $m_1, m_2$ はともに 3 以上の整数で, 互いに素であるとする．すると, 以下の 2 条件は互いに同値である:

条件 1.　正 $m_1 m_2$ 角形は作図可能である．

条件 2.　正 $m_1$ 角形および正 $m_2$ 角形は, ともに作図可能である．

**証明.** まず, 条件 1 を仮定する. このとき, $\zeta_{m_1m_2} \in \widetilde{\mathcal{C}}$ である. $\widetilde{\mathcal{C}}$ が体であることから,

$$(\zeta_{m_1m_2})^{m_2} = \exp\left(\frac{2\pi i}{m_1m_2}\right)^{m_2} = \exp\left(\frac{2\pi i}{m_1}\right) = \zeta_{m_1} \in \widetilde{\mathcal{C}},$$
$$(\zeta_{m_1m_2})^{m_1} = \exp\left(\frac{2\pi i}{m_1m_2}\right)^{m_1} = \exp\left(\frac{2\pi i}{m_2}\right) = \zeta_{m_2} \in \widetilde{\mathcal{C}}$$

である. よって条件 2 が成立する.

逆に条件 2 を仮定すると, $\zeta_{m_1}, \zeta_{m_2} \in \widetilde{\mathcal{C}}$ が成立する. さて, $m_1$ と $m_2$ は互いに素であるため, ある整数 $a, b$ が存在して, $am_1 + bm_2 = 1$ が成立する. このとき,

$$\frac{2\pi i}{m_1m_2} = b\frac{2\pi i}{m_1} + a\frac{2\pi i}{m_2}$$

であることに注意する. したがって,

$$\begin{aligned}\zeta_{m_1m_2} &= \exp\left(\frac{2\pi i}{m_1m_2}\right)\\ &= \exp\left(b\frac{2\pi i}{m_1} + a\frac{2\pi i}{m_2}\right) = \zeta_{m_1}^b\zeta_{m_2}^a \in \widetilde{\mathcal{C}}\end{aligned}$$

であり, 条件 1 が成立する. □

角の 2 等分と関連して, 次の命題も成立する:

**命題 3.2.** $n$ は 3 以上の整数とする. すると, 以下の 2 条件は互いに同値である:

条件 1. 正 $2n$ 角形は作図可能である.

条件 2. 正 $n$ 角形は作図可能である.

**証明.** 条件 1 から条件 2 に関する証明は, 命題 3.1 の証明と同様に $\zeta_{2n}^2 = \zeta_n$ より従う. 逆の証明は, 角の 2 等分が常に可能であることより従う. □

命題 3.1 および命題 3.2 により, いつ正 $n$ 角形が作図可能であるかを考察するためには, $n = p^\ell$($p$ は奇素数, $\ell$ は正整数) の形に限定すればよいことがわかる. 実は $\ell = 1$ のときのみを考察すればよい. 詳細は述べないが, $\ell \geq 2$ のときにどのようなことが生じるかについて書く. $\zeta_{p^\ell}$ の ($\mathbb{Q}$ 上の) 次数は, 実は

$$p^\ell - p^{\ell-1} = p^{\ell-1}(p-1)$$

であり,

$$p \mid [\mathbb{Q}(\zeta_{p^\ell}) : \mathbb{Q}] = p^{\ell-1}(p-1)$$

が成立する．よって, 系 2.1 により, $\zeta_{p^\ell}$ は作図不可能である．$\ell = 1$ の場合, $\zeta_p$ の次数は $p-1$ である．
※ $\zeta_p$ の ($\mathbb{Q}$ 上の) 最小多項式は $X^{p-1} + X^{p-2} + \cdots + X + 1$.
$n = p$($p$ は奇素数) のときは, 以下の事実が成立する:

**定理 3.1** (Gauss)**.** $p$ を奇素数とする．正 $p$ 角形が作図可能となる必要十分条件は, ある非負整数 $n$ が存在して, $p = 2^{2^n} + 1$ となることである．このような $p$ はフェルマー素数と呼ばれる．

**例 3.1.** $F_n = 2^{2^n} + 1$ とおく．$F_n (0 \leq n \leq 4)$ は素数であることが知られている．以下に, 数値を書く:

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537.$$

フェルマー素数が無限に存在するかどうかは知られていない．さらには, 上記の例以外にフェルマー素数が存在するかどうかについても有名な未解決問題である．

定理 3.1 について, 必要条件に関しては比較的容易に証明できる．実際,

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$$

に注意すると, 系 2.1 によりある正整数 $k$ が存在して,

$$p = 2^k + 1$$

が成立する．$k$ が 2 のベキであることを示せばよい．そのためには, ある奇素数 $q$ が存在して, $q$ が $k$ を割り切ると仮定して矛盾を導けばよい．$k = qt (t \in \mathbb{Z}, t \geq 1)$ と書く．整数 $p = 2^k + 1 = 2^{qt} + 1$ は以下のように式変形できることに注意する:

$$p = 2^{qt} + 1 = (2^t + 1)\big(2^{(q-1)t} - 2^{(q-2)t} + - \cdots + 2^{2t} - 2^t + 1\big).$$

よって, $p$ が素数という仮定に矛盾する．

定理 3.1 については, 十分条件が本質である．本ファイルでは $p \leq 17$(特に $p = 17$) の場合を中心に扱う．一般の素数 $p$ に関する定理 3.1 の証明は, 文献 [2] を参照．本ファイルでガウス周期を用いて議論するが, [2] ではガ

ウス和とヤコビ和を用いて議論がされている．これらを定義するためには, 有限アーベル群の指標群について議論する必要がある．
※ $p=3$ の場合は,

$$\zeta_3 = \frac{-1+\sqrt{3}i}{2}$$

であるため, 定理 1.2 より作図可能性は明らか．$p=5,17$ の場合を扱う．

# 4 ガウス周期の定義と例

## 4.1 定義

これ以降, 特に断りがない限り $p$ を奇素数とする．$U_p := \{\zeta_p^n \mid n \in \mathbb{Z}\}$ とおく．3で定義した通り, 正 $p$ 角形が作図可能であるかを調べるためには, $U_p$ の性質を調べる必要がある．$U_p$ について, 別の視点を導入する．$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ を (元の個数が $p$ 個の) 有限体とする．$F_p$ の元は, $\overline{m}(= m + p\mathbb{Z})(m \in \mathbb{Z})$ のように書くことができる．さて, $\zeta_n^p = 1$ であることに注意する．すると,

$$\zeta_p^{\overline{m}} = \zeta_p^m$$

と定義できる．つまり, 左辺の値は, $\overline{m}$ の代表元 $m$ の取り方によらず一意に定まる．また, 写像 $\varphi : \mathbb{F}_p \to U_p$ を $\varphi(\overline{m}) = \zeta_p^{\overline{m}}$ と置くと, $\varphi$ は全単射である．この全単射を通じて, $U_p$ を $\mathbb{F}_p$ と同一視する．つまり, $U_p$ の元は $\zeta_p^{\overline{m}}(\overline{m} \in \mathbb{F}_p)$ の形に一意的に書くことができる．つまり, $U_p$ の元を指定したければ．べき乗の箇所の $\overline{m}$ を指定すればよい．

さて, 以下簡略化のために, $\overline{m} \in \mathbb{F}_p$ を $m$ と略記する．ガウス周期とは, $U_p$ の適切な元 $m_1, m_2, \ldots, m_k$ に対する和 $\zeta_p^{m_1} + \zeta_p^{m_2} + \cdots + \zeta_p^{m_k}$ である．以下, 詳細な定義を述べる．そのためには, $\mathbb{F}_p$ の乗法群 $\mathbb{F}_p^\times = \mathbb{F}_p \backslash \{0\}$ について補足をする必要がある．$\mathbb{F}_p^\times$ は有限アーベル群である．さて, 以上の準備のもと, ガウス周期の定義をする．

**定義 4.1.** $H$ を乗法群 $\mathbb{F}_p^\times$ の部分群とする．$a \in \mathbb{F}_p$ に対して,

$$[a]_H := \sum_{x \in H} \zeta_p^{ax} \in \mathbb{C}$$

とおく．この形の複素数 $[a]_H$ をガウス周期と呼ぶ.

以下, $\mathbb{F}_p^\times$ の性質を利用して, ガウス周期の具体例を述べる. 実は, $\mathbb{F}_p^\times$ は巡回群であることが知られている. つまり, ある $g \in \mathbb{F}_p^\times$ が存在して,

$$\mathbb{F}_p^\times =< g > (= \{g^m \mid m \in \mathbb{Z}\}) \tag{4.1}$$

であることが知られている. 式 (4.1) を満たす $g \in \mathbb{F}_p^\times$ を「$p$ を法とする原始根」や「$\mathbb{F}_p^\times$ の原始根」等と呼ぶ.
※原始根の存在の証明は, 本ファイルでは扱わない. しかし, 以下扱う具体例では, 具体的に $g$ の値を記述する. $g$ の値がわかれば, (4.1) が成立することは, 手計算で確認することができる. 実際, 次の例 4.1 で紹介する有限体の乗法群が巡回群であることがわかれば, 本ファイルを読むためには充分である.

**例 4.1.** (1) $p = 5$. この場合, $g = 2$ が原始根の一つである. 実際, $\mathbb{F}_5$ において, $2^n (n = 1, 2, 3, 4)$ は, 以下のように計算される:

| $n$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| $2^n$ | 2 | 4 | 3 | 1 |

(4.2)

(2) $p = 7$. この場合, $g = 3$ が原始根の一つである. 実際, $\mathbb{F}_7$ において, $3^n (n = 1, 2, \ldots, 7)$ は, 以下のように計算される:

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $3^n$ | 3 | 2 | 6 | 4 | 5 | 1 |

(4.3)

(3) $p = 17$. この場合, $g = 3$ が原始根の一つである. 実際, $\mathbb{F}_{17}$ において, $3^n (n = 1, 2, \ldots, 16)$ は, 以下のように計算される:

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $3^n$ | 3 | 9 | 10 | 13 | 5 | 15 | 11 | 16 |

(4.4)

| $n$ | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|
| $3^n$ | 14 | 8 | 7 | 4 | 12 | 2 | 6 | 1 |

(4.5)

※ $\mathbb{F}_{17}$ において $3^8 = -1$ であるため, $3^n + 3^{n+8} = 0 (n = 1, 2, \ldots, 8)$ であることに注意.

## 4.2 $\mathbb{F}_p^\times$ の部分群

有限体 $\mathbb{F}_p$ の剰余群 $\mathbb{F}_p^\times$ は巡回群 $< g >$ であった ($g$ は $p$ を法とする原始根). これにより, $\mathbb{F}_p^\times$ は $\mathbb{Z}/(p-1)\mathbb{Z}$ と同型である. したがって, $\mathbb{F}_p^\times$ の部分群の形を決定できる. 具体的には, $p-1$ の正の約数 $d$ が存在して,

$$H_d = \{g^{dm} \mid m \in \mathbb{Z}\}$$

の形の集合が $\mathbb{F}_p^\times$ の部分群である (巡回群の部分群は巡回群).

$$H_d = \{g^d, (g^d)^2, \ldots, (g^d)^{(p-1)/d} = g^{p-1} = 1\}$$

より, Card $H_d = (p-1)/d$ であることに注意する. なお, 原始根 $g$ の取り方は一意には定まらない. しかし, (原始根は複数存在する)$H_d$ は, $g$ の取り方に依存せず一意に定まる. この事実については, $\mathbb{F}_p^\times$ そのものを調べるよりも, 同型な群 $\mathbb{Z}/(p-1)\mathbb{Z}$ を考察するほうがわかりやすい. 実際, $\mathbb{Z}/(p-1)\mathbb{Z}$ の部分群で, 位数が $(p-1)/d$ となるものは一意に定まる.

**例 4.2.** ※例 4.1 参照.
(1) $p = 5$ とする. $p - 1 = 4$ の約数は $d = 1, 2, 4$ である. $H_d$ を計算するために $g = 2$ とおく. $H_1 =< 2 >= \mathbb{F}_5^\times$, $H_4 = \{1\}$ である. また,

$$H_2 =< 2^2 >= \{2^2, 2^4\} = \{4, 1\}$$

である.
(2) $p = 7$ とする. $p - 1 = 6$ の約数は $d = 1, 2, 3, 6$ である. $H_d$ を計算するために $g = 3$ とおく. $H_1 =< 3 >= \mathbb{F}_7^\times$, $H_6 = \{1\}$ である. また,

$$H_2 =< 3^2 >= \{3^2, 3^4, 3^6\} = \{2, 4, 1\},$$
$$H_3 =< 3^3 >= \{3^3, 3^6\} = \{6, 1\}$$

である.
※ $p=17$ の場合は 5 章で必要であり, その際に改めて述べる. ここでは, $p-1=16$ の約数はすべて 2 のべき乗であることだけに注意する.

$\mathbb{F}_p^\times$ の部分群が明らかになったので, それを利用してガウス周期に関する新たな記号を導入する.

**定義 4.2.** $d$ を $p-1$ の約数とする. $\mathbb{F}_p^\times$ において, 位数 $(p-1)/d$ の部分群 $H_d$ に関するガウス周期 $[a]_{H_d}$ を単に $[a]_d$ と略記する. すなわち,

$$[a]_d := \sum_{x\in H_d} \zeta_p^{ax} \in \mathbb{C}$$

である. この形の複素数 $[a]_d$ を $d$ 次のガウス周期と呼ぶ.

## 4.3 ガウス周期の具体例

4.2 節と同様に, $\mathbb{F}_p^\times$ における位数 $(p-1)/d$ の部分群を $H_d$ と書く. すると, $d$ 次のガウス周期の定義より,

$$[0]_d = \sum_{x\in H_d} 1 = \frac{p-1}{d}$$

である. 一方, $a\in\mathbb{F}_p^\times$ とする. 群論の記法

$$aH_d = \{ax \mid x\in H_d\}$$

を思い出す. この記法を用いると,

$$[a]_d = \sum_{y\in aH_d} \zeta_p^y \tag{4.6}$$

であることがわかる. 式 (4.6) の右辺は, 指数の箇所が剰余類によって記述されていることがわかる. 以上の準備のもと, ガウス周期の例において, 様々な性質を調べる.

**例 4.3.** ※例 4.2 参照.
(1) $p=5$ とする. $p-1$ の約数として, $d=2$ を選ぶ. 計算の便宜上, 原始根の一つ $g=2$ を選んでおく. $\mathbb{F}_5^\times$ の部分群 $H_2 =< 2^2 >= \{1,4\}$ を考える. 剰余群 $\mathbb{F}_5^\times/H_2$ の元は, 以下の通りである:

$$H_2=\{1,4\}=4H_2,\quad 2H_2=\{2,8\}=\{2,3\}=3H_2.$$

よって, これらの剰余類に対応するガウス周期は以下のように記述される:

$$[1]_2 = \zeta_5^{1} + \zeta_5^{4} = [4]_2,$$
$$[2]_2 = \zeta_5^{2} + \zeta_5^{3} = [3]_2.$$

さて, $[1]_2, [2]_2$ の間に成立する関係を調べよう. $1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0$ より,

$$[1]_2 + [2]_2 = \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = -1 \tag{4.7}$$

である. 一方, $\zeta_5^5 = 1$ より, 積 $[1]_2[2]_2$ は, 以下のように整理をすることができる:

$$\begin{aligned}[1]_2[2]_2 &= (\zeta_5 + \zeta_5^4)(\zeta_5^2 + \zeta_5^3) \\ &= \zeta_5^3 + \zeta_5^4 + \zeta_5^6 + \zeta_5^7 \\ &= \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = -1. \end{aligned} \tag{4.8}$$

よって, 2 次方程式の根と係数の関係により, $[1]_2, [2]_2$ は
方程式 $X^2 + X - 1 = 0$ の根である. よって, $[1]_2, [2]_2 \in \widetilde{\mathcal{C}}$ である.
さて, 再び $\zeta_5^5 = 1$ より,

$$[1]_2 = \zeta_5 + \zeta_5^{-1} = 2\cos\left(\frac{2\pi}{5}\right) \in \widetilde{\mathcal{C}}.$$

よって $\cos(2\pi/5) \in \widetilde{\mathcal{C}}$ であり, 正 5 角形が作図可能であることがわかる.
(2) $p = 7$ とする. $p - 1$ の約数として, $d = 3$ を選ぶ. 計算の都合上, 原始根の一つ $g = 3$ を選んでおく. $\mathbb{F}_7^\times$ の部分群 $H_3 =< 3^3 >= \{1, 6\}$ を考える. 剰余群 $\mathbb{F}_7^\times / H_3$ の元は, 以下の通りである:

$$\begin{aligned} H_3 &= \{1, 6\} = 6H_3, \\ 3H_3 &= \{3, 18\} = \{3, 4\} = 4H_3, \\ 3^2H_3 &= 2H_3 = \{2, 12\} = \{2, 5\} = 5H_3. \end{aligned}$$

よって, 各剰余類に対応するガウス周期は以下のように記述される:

$$[1]_3 = \zeta_7^{1} + \zeta_6^{6} = [6]_3, \tag{4.9}$$
$$[3]_3 = \zeta_7^{3} + \zeta_6^{4} = [4]_3, \tag{4.10}$$
$$[2]_3 = \zeta_7^{2} + \zeta_6^{5} = [5]_3 \tag{4.11}$$

さて, $[1]_3, [2]_3, [3]_3$ の間に成立する関係を調べよう. $1+\sum_{j=1}^{6}\zeta_7^j=0$ より,

$$[1]_3+[2]_3+[3]_3=\sum_{j=1}^{6}\zeta_7^j=-1 \tag{4.12}$$

である. 次に, 積 $[1]_3[2]_3, [2]_3[3]_3, [3]_3[1]_3$ を計算する. $\zeta_7^7=1$ より, 以下が成立する:

$$\begin{aligned}
[1]_3[2]_3&=\zeta_7^3+\zeta_7^6+\zeta_7+\zeta_7^4=[3]_3+[1]_3,\\
[2]_3[3]_3&=\zeta_7^5+\zeta_7^6+\zeta_7+\zeta_7^2=[1]_3+[2]_3,\\
[3]_3[1]_3&=\zeta_7^4+\zeta_7^5+\zeta_7^2+\zeta_7^3=[2]_3+[3]_3.
\end{aligned} \tag{4.13}$$

よって, (4.12) より,

$$[1]_3[2]_3+[2]_3[3]_3+[3]_3[1]_3=2([1]_3+[2]_3+[3]_3)=-2 \tag{4.14}$$

であることがわかる. 最後に積 $[1]_3[2]_3[3]_3$ を計算する. (4.9) および (4.11) より,

$$[1]_3[2]_3[3]_3=([3]_3+[1]_3)[3]_3=[3]_3^2+[2]_3+[3]_3$$

である. $\zeta_7^7=1$ より

$$[3]_3^2=\zeta_7+\zeta_7^6+2=[1]_3+2$$

を利用すると, 再び (4.12) より

$$[1]_3[2]_3[3]_3=[1]_3+[2]_3+[3]_3+2=1 \tag{4.15}$$

となる. さて, 3 次方程式の根と係数の関係

$$\begin{aligned}
&(X-\alpha)(X-\beta)(X-\gamma)\\
&=X^3-(\alpha+\beta+\gamma)X^2+(\alpha\beta+\beta\gamma+\gamma\alpha)X-\alpha\beta\gamma
\end{aligned}$$

に注意する. すると, (4.12),(4.14),(4.15) より, $[1]_3, [2]_3, [3]_3$ は 3 次方程式

$$X^3+X^2-2X-1=0$$

の根であることがわかる. なお, $X^3+X^2-2X-1$ は $\mathbb{Q}[X]$ の既約な元であるため, $[1]_3=2\cos(2\pi/7)$ は次数 3, 特に $\zeta_7$ および正 7 角形が作図不可能であることがわかる.
※正 7 角形が作図不可能であることはすでに示していたが, ガウス周期を用いると具体的な方程式を導くことができるということを紹介したかったので, 上記の例で紹介した.

# 5　ガウス周期を用いた正 17 角形の作図可能性

## 5.1　積公式

記号は前の章と同じものを用いる．例 4.3 ではガウス周期の間に成立する関係式を考察した．その際に用いた式 (4.7) および式 (4.12) を一般化する．

**命題 5.1.** $p$ を奇素数とする．$d$ を $p-1$ の約数とする．また, $g$ を $\mathbb{F}_p^\times$ における原始根の一つとする．このとき,

$$\sum_{j=0}^{d-1}[g^j]_d = -1$$

が成立する．

**証明.** 剰余群 $\mathbb{F}_p^\times/H_d$ の元は, 以下のように羅列できる: $g^jH_d \quad (j=0,1,\ldots,d-1)$. $g^jH_d$ に属する元 $g^j$ に対応するガウス周期は

$$[g^j]_d = \sum_{x_j \in g^jH_d} x_j$$

である．よって,

$$\begin{aligned}\sum_{j=0}^{d-1}[g^j]_d &= \sum_{j=0}^{d-1}\sum_{x_j\in g^jH_d}\zeta_p^{x_j} = \sum_{x\in\mathbb{F}_p^\times}\zeta_p^x \\ &= \sum_{h=1}^{p-1}\zeta_p^h = -1\end{aligned}$$

となり, 命題 5.1 が示された．　□

ガウス周期の積に関する一般の公式を紹介する．

**命題 5.2** (積公式)**.** $p$ を奇素数とする．$d$ を $p-1$ の約数とする．このとき, 任意の $x, y \in \mathbb{F}_p$ に対して, 以下が成立する:

$$[x]_d[y]_d = \sum_{\beta\in H_d}[x+y\beta]_d.$$

**証明.** $[x]_d[y]_d$ を以下のように計算する:

$$\begin{aligned}[x]_d[y]_d &= \sum_{\alpha\in H_d}\zeta_p^{\alpha x}\sum_{\beta\in H_d}\zeta_p^{\beta y} = \sum_{\alpha\in H_d}\sum_{\beta\in H_d}\zeta_p^{\alpha x+\beta y}\\ &= \sum_{\alpha\in H_d}\sum_{\beta\in H_d}\zeta_p^{\alpha(x+\alpha^{-1}\beta y)}. \end{aligned} \tag{5.1}$$

さて, $\alpha\in H_d$ を固定するごとに, 写像 $\varphi_\alpha : H_d\to H_d$ を $\varphi_\alpha(\beta)=\alpha^{-1}\beta$ により定める. すると, $\varphi_\alpha$ は全単射である. よって, 5.1 により, 以下が成立する:

$$\begin{aligned}[x]_d[y]_d &= \sum_{\alpha\in H_d}\sum_{\gamma\in H_d}\zeta_p^{\alpha(x+\gamma y)}\\ &= \sum_{\gamma\in H_d}\underbrace{\sum_{\alpha\in H_d}\zeta_p^{\alpha(x+\gamma y)}}_{[x+\gamma y]_d} = \sum_{\gamma\in H_d}[x+\gamma y]_d. \end{aligned}$$

□

**例 5.1.** (1) ※例 4.3(1) と同じ記号を用いる.
式 (4.7) は命題 5.1 の一例である.
また, 積公式の応用として, 式 (4.8) を命題 5.2 から導く. $H_2=\{1,4\}$ であった. よって,

$$[1]_2[2]_2 = [1+2\cdot 1]_2+[1+2\cdot 4]_2 = [3]_2+[4]_2 = [1]_2+[2]_2 = -1.$$

※ $[1]_2=[4]_2$ および $[2]_2=[3]_2$ を思い出す. (2) ※例 4.3(2) と同じ記号を用いる.
式 (4.12) は命題 5.1 の一例である.
また, 積公式の応用として, 式 (4.13) を命題 5.2 から導く. $H_3=\{1,6\}$ であった. よって,

$$[1]_3[2]_3 = [1+2\cdot 1]_3+[1+2\cdot 6]_3 = [3]_3+[6]_3 = [1]_3+[3]_3.$$

※式 (4.9),(4.10),(4.11) も参照.

## 5.2 2 次のガウス周期

$p=17$ の場合を考察する. $\mathbb{F}_{17}^\times$ における原始根の一つとして $g=3$ を選ぶ. また, 本節において断りが無い限り, $\zeta=\zeta_{17}$ と略記する. 表 4.4 およ

び表 4.5 を再び記載する:

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $3^n$ | 3 | 9 | 10 | 13 | 5 | 15 | 11 | 16 |

(4.4)

| $n$ | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|
| $3^n$ | 14 | 8 | 7 | 4 | 12 | 2 | 6 | 1 |

(4.5)

$p-1=16$ であるため, $d=1,2,4,8,16$ に対して $d$ 次のガウス周期が考えられる. $H_8=\{1,3^8\}=\{1,16\}$ であり, 対応するガウス周期が

$$[1]_8=\zeta^1+\zeta^{16}=\zeta+\zeta^{-1}=2\cos\left(\frac{2\pi}{17}\right) \tag{5.2}$$

である. よって, $[1]_8\in\widetilde{\mathcal{C}}$ を示せばよい. しかし, 8 次のガウス周期を直接扱うことは困難であるため, まず 2 次のガウス周期を扱う.

$$H_2=<3^2>=\{3^{2m}\mid m\in\mathbb{Z}\}$$
$$3H_2=\{3^{2m+1}\mid m\in\mathbb{Z}\}$$

である. よって, 表 4.4 および表 4.5 において, $n$ の偶奇性に着目すると, 以下がわかる:

$$H_2=\{9,13,15,16,8,4,2,1\},\quad 3H_2=\{3,10,5,11,14,7,12,6\}$$

である. これらに対応して, $[1]_2=\sum_{y\in H_2}\zeta^y=[9]_2$ や $[3]_2=\sum_{y\in 3H_2}\zeta^y=[10]_2$ などが成立する.
※式 (4.6) 参照.
さて, 命題 5.1 により,

$$[1]_2+[3]_2=-1 \tag{5.3}$$

である. また, 時間をかければ積公式 (命題 5.2) により, $[1]_2[3]_2$ を計算することができる. 結論だけを述べると,

$$[1]_2[3]_2=4[1]_2+4[3]_2=-4$$

となる. 実際に上記の計算をしてみると, 良い計算練習になる. 根と係数の関係より, $[1]_2,[3]_2$ は 2 次方程式 $X^2+X-4=0$ の根である. よって, 以下が成立する:

$$[1]_2,[3]_2\in\widetilde{\mathcal{C}} \tag{5.4}$$

今回のファイルで直接使うわけではないが, 一般に以下が成立する:

**定理 5.1.** $p$ を奇素数とする．$p-1$ の約数として, $d=2$ を選ぶ．また, $g$ を $\mathbb{F}_p^\times$ における原始根の一つとする．
(1) $p$ は 4 で割って 1 余る整数とする．このとき, $[1]_2, [g]_2$ は 2 次方程式

$$X^2 + X - \frac{p-1}{4} = 0$$

の根である．
※実際は, $[1]_2 = \dfrac{-1+\sqrt{p}}{2}, [g]_2 = \dfrac{-1-\sqrt{p}}{2}$ であるが, 示すことは難しい．
(2) $p$ は 4 で割って 3 余る整数とする．このとき, $[1]_2, [g]_2$ は 2 次方程式

$$X^2 + X + \frac{p+1}{4} = 0$$

の根である．
※実際は, 再び $i$ を虚数単位とするとき, $[1]_2 = \dfrac{-1+i\sqrt{p}}{2}, [g]_2 = \dfrac{-1-i\sqrt{p}}{2}$ であるが, 示すことは難しい．

定理 5.1 の証明は, 文献 [1] 参照．なお, ガロア理論を知っている方は, 上記の証明がガロア理論と関連があることに気が付くと思う．実際に証明にガロア理論を用いて少し簡略化をすることで, 理解を深めることができる．また, 作図問題解決のための計算がある意味ガロア理論のアイディアを含んでいるともいえる．

## 5.3 $F_{17}$ における 4 次, 8 次のガウス周期

本節においても特別な断りがない限り $\zeta = \zeta_{17}$ であるとする．5.2 節で, $F_{17}$ における 2 次のガウス周期 $[1]_2$ および $[3]_2$ が作図可能であることを確かめた．目標は, $[1]_8 \in \widetilde{\mathcal{C}}$ であった．まず本節では, 2 次のガウス周期に関する情報を用いて, 4 次のガウス周期がすべて作図可能であることを示す．次に, 4 次のガウス周期の情報を利用して, $[1]_8 \in \widetilde{\mathcal{C}}$ を示す．

証明において, $F_{17}^\times$ の部分群 $H_2, H_4, H_8$ を利用する．実は, これはガロア理論に通じる考え方である．詳細は述べないが, $F_{17}^\times$ は本質的にガロア群と呼ばれるものであり, その部分群を考察することが重要である．

さて, $H_2 =< 3^2 >$ の元は, $3^{2h}(h \in \mathbb{Z})$ の形をしている. また, $3H_2$ の元は, $3^{1+2h}(h \in \mathbb{Z})$ の形をしている. 一方, $H_4 =< 3^4 > = \{1, 4, 13, 16\}$ の元は $3^{4m}(m \in \mathbb{Z})$ の形をしている. これを利用して, $H_2$ および $3H_2$ を, 以下のように分割できることに注意する:

$$
\begin{aligned}
&H_2 = H_4 \cup 3^2 H_4,\\
&H_4 = \{1, 4, 13, 16\}, 3^2 H_4 = \{2, 8, 9, 15\},\\
&\text{つまり}, 3^{2h} \text{ の形の元は}, 3^{4m} \text{ または } 3^{4m+2} \text{ の形}.\\
&3H_2 = 3H_4 \cup 3^3 H_4,\\
&3H_4 = \{3, 5, 12, 14\}, 3^3 H_4 = \{6, 7, 10, 11\}.\\
&\text{つまり}, 3^{2h+1} \text{ の形の元は}, 3^{4m+1} \text{ または } 3^{4m+3} \text{ の形}.
\end{aligned}
$$

上の分割に応じて, 2 次のガウス周期 $[1]_2$ および $[3]_2$ も, 以下のように 4 次のガウス周期の和で表すことができる:

$$[1]_2 = [1]_4 + [2]_4 \in \widetilde{\mathcal{C}}, \quad [3]_2 = [3]_4 + [6]_4 \in \widetilde{\mathcal{C}}. \tag{5.5}$$

ただし, 例えば $3^2 H_4 = 2H_4$ であるため, これに対応する 4 次のガウス和は

$$[2]_4 = \zeta^2 + \zeta^8 + \zeta^9 + \zeta^{15}$$

である. さて, 命題 5.2 を用いて, 積 $[1]_4[2]_4$ および $[3]_4[6]_4$ を計算する. まずは, 以下の計算が成立する:

$$
\begin{aligned}
&[1]_4[2]_4\\
&= [1 + 2 \cdot 1]_4 + [1 + 2 \cdot 4]_4 + [1 + 2 \cdot 13]_4 + [1 + 2 \cdot 16]_4\\
&= [3]_4 + [9]_4 + [10]_4 + [16]_4\\
&= [3]_4 + [3^2]_4 + [3^3]_4 + [3^0]_4 = -1.
\end{aligned} \tag{5.6}
$$

ただし, 最後の等式で命題 5.1 を用いた. 同様に, 以下が成立する:

$$
\begin{aligned}
&[3]_4[6]_4\\
&= [3 + 6 \cdot 1]_4 + [3 + 6 \cdot 4]_4 + [3 + 6 \cdot 13]_4 + [3 + 6 \cdot 16]_4\\
&= [9]_4 + [10]_4 + [13]_4 + [14]_4\\
&= [3^2]_4 + [3^3]_4 + [3^0]_4 + [3]_4 = -1.
\end{aligned} \tag{5.7}
$$

よって, 式 (5.5), (5.6), (5.7) に着目し, 根と係数の関係を用いる. すると, (5.4) より 4 次のガウス周期はすべて作図可能, つまり

$$[1]_4, [3]_4, [3^2]_4, [3^3]_4 \in \widetilde{\mathcal{C}} \tag{5.8}$$

であることがわかる.

さて, $H_4$ と $3^2H_4$ を用いて $H_2$ を表示した方法と同様の手法により, $H_8 = \{1, 16\}$ と $3^4H_8$ を用いて $H_4 = \{1, 4, 13, 16\}$ を表せる. 実際,

$$\begin{aligned} H_4 &= H_8 \cup 3^4H_8, \\ H_8 &= \{1, 16\}, \quad 3^4H_8 = \{4, 13\} \end{aligned}$$

である. この分割に応じて, 4 次のガウス周期 $[1]_4$ も以下のように 8 次のガウス周期の和で表すことができる:

$$[1]_4 = [1]_8 + [4]_8. \tag{5.9}$$

一方, 積 $[1]_8[4]_8$ は命題 5.2 から以下のように計算される:

$$[1]_8[4]_8 = [1 + 4 \cdot 1]_8 + [1 + 4 \cdot 16]_8 = [5]_8 + [14]_8.$$

さて, $5H_8 = \{5, 12\}$ と $14H_8 = \{3, 14\}$ の和集合は,

$$5H_8 \cup 14H_8 = \{3, 5, 12, 14\} = 3H_4$$

である. よって, ガウス周期 $[3]_4$ は 8 次のガウス周期 $[5]_8$ と $[14]_8$ の和である. 以上により,

$$[1]_8[4]_8 = [3]_4 \tag{5.10}$$

である. (5.9) および (5.10) に着目し, 根と係数の関係を用いる. すると, (5.8) により,

$$[1]_8, [4]_8 \in \widetilde{\mathcal{C}}$$

がわかる. 特に正十七角形は作図可能である.

# 参考文献


[1] 栗原 将人, ガウスの数論世界をゆく: 正多角形の作図から相互法則・数論幾何へ, 数学書房, 2017.

[2] 小野 孝, 数論序説, 裳華房, 1987.

[3] 塩川 宇賢, 無理数と超越数, 森北出版, 1999.