響きあうガロアとガウス

上野孝司

2016 年 4 月 17 日

響きあうガロアとガウス

０．はじめに－構造的数学教育の再考

正１７角形の作図方法はネットでも多く取り上げられているが、残念ながらその多くが技巧的なものに限定されたものであり、その詳細を一般的な理論として理解しているひとは意外と少ないようだ。実際にはこの問題の全容を知るには、ガロアの理論やガウスの f 項周期（いわゆるベクトル空間の基底）といった深い知識が必要とされる。しかし、それに至るには実に長い時間と労力、忍耐力を要する。筆者が体験した現代の数学教育（東京大学教養学部と理学部数学科の数学教育）では、高校の数学を終えて大学に入ると、１、２年の教養課程でストークスの定理までを扱う解析学やジョルダンの標準型までの線形代数、位相や集合論などといった“基礎”を学んだ後に専門課程で、群、環、体、留数定理に至るまでの複素解析の基礎を経てようやく“体とガロア理論”（３年次の代数学講義）の一般理論にたどりついたと思いきや、ここで正１７角形の作図を応用問題のひとつとして、いっきょにサッと終えてしまう。しかし、大学の数学科の学生ならまだしも、普通の理工系の学生にとってはこれは酷な話である。ほとんどの学生や一般の社会人は、この興味深い作図問題に至る一連の課程をこなしきれず途中で力尽き、正１７角形の問題にたどり着くことができない。結局は断念するか、せいぜいネットで一連の理論の終盤で扱う定木とコンパスによる作図といった技巧的な事柄を学ぶ程度で終わってしまうのである。筆者もこの作図問題の存在を知ったのは高校生のときであったが、実際にそれを理論として学習するまでには５年もの歳月を要した。

多くのひとがガウスの残した偉大な歴史的な遺産を学びきれないといった実に残念な状況を生み出してしまっている。これでは、ガロアやガウスも浮かばれまい。実は、正１７角形の作図問題だけならそれほど多くの事柄を知らずとも、ガロアやガウスの思想を伴って学びとることができるのである。いや、逆にこの問題を起点として議論を展開すれば、ガロアやガウスの思想の果実を具体的に学びとりながら、現代数学を習得できるのである。つまり、正多角形の作図“問題”は現代の構造的な数学教育のネガティブな影響の一端を如実に示しているのである。本稿は、以上のような経緯を踏まえて、正１７角形の作図問題をガロアの理論やガウスの思想という偉大な“おまけ”付きで、突貫工事で一挙に解決しようと試みたものである。５年の歳月を１日で再現する、いわば、“**君のための数学原論**”である。必要な知識は、線形代数の初歩、群と体の定義くらいである。

＊本サイトでも、正 17 角形の作図問題が扱われているが、本稿では、オイラーの関数を基に基礎から結論まで一気に述べたことやガロア理論の一般理論を展開したことに加えて、ガウスの f 項周期（拡大体の基底）を明示的に述べたなどの点で、より総括的、一般的な論考となっている。

1．正１７角形の作図問題ー背景に円分体

正 17 角形が作図できることはよく知られた事実である。一般的に正多角形を定木とコンパスだけを用いて作図する問題は古来から知られている。正三角形、正四角形は容易に作図でき、また正５角形、正６角形を作図したことのある読者もおられるだろう。ところが後述するように正７角形は作図できない。そして数学の歴史のなかで一番大きな問題となっていたのが正１７角形の作図問題であった。多くの数学者を悩ませていたのだが、数学界の王者ガウスが１７９６年、朝目覚めたときに作図法を思いついたといわれ、この問題を肯定的に解決した。

本質は円分体、つまり、有理数体 Q に方程式 $X^{17}=1$ の根（原始根 ζ）を付加した拡大体 Q（ζ）の Q 上のベクトル空間としての次元が 16 で、これが 2 の冪乗であること。17 そのものより 1 引いた数が 16 で、これが 2 の 4 乗であることに意味がある（本稿を読み進むと、１引いた数が重要なのではなく、17 と互いに素な整数の個数が 16 でこれが重要であると言ったほうが妥当というべきであることがわかる)。整然とした群や体の理論が明確でない時代にガウスは、拡大体を有理数体上のベクトル空間とみたとき、その基底（いわゆるｆ項周期）を明らかにしたというのだから、驚異の天才だ。ガウスは群論や体論を知っていたのだろうかーーという疑問は常に残る。

円分体はまたガロア理論の格好の題材となる。ガロア理論によって円分体は有機的、普遍的な命を与えられることになる。ガロアの基本定理によって、円分体の部分体とガロア群と呼ばれる群の部分群には一対一の対応が存在し、円分体の情報はガロア群の構造の分析におきかわる。ガロアとガウスが響きあうようにして、方程式 $X^{17}=1$ が $\cos\dfrac{2\pi}{17}$ に収束する様は初等整数論の圧巻だ。筆者も実際に正 17 角形の作図問題に取り組んだことがあるが、それは 17 乗根 ζ の添字と冪乗 ζ_i^j との延々と続く格闘だった。

2. 円分体のＭＡＰ

本稿では円分体について、ガロア理論やガウスの方法を駆使してその基本的構造の一般論を展開し、その応用問題のひとつとして正多角形の作図問題、特に正 17 角形の作図法を示す。道のりは長いので論理展開の方向性を簡単に俯瞰しておく。

以下、読者は抽象的な理論がいかにして具体的な応用問題の解決法に結実するかをみることができよう。初等的な技巧によって正 17 角形を単体の問題として作図することもできようが、それが群論や体とガロアの理論を背景とした構造的なものでなければ関心はない。それが本稿の意図するところである。なお、扱う事項が多いので、本論の展開から考えて些末と思われる事柄については詳細な説明、証明はつけない。あくまで論理展開の文脈を重要視する。

■ 円分体の分析ＭＡＰ

(1) 方程式 $X^n=1$ の一般論を展開。複素平面上で解の集合が正多角形の頂点をつくることを確認。正 5 角形の作図法を復習（複素平面を用いた代数的な解法、3 角方程式 $\sin\theta=\cos 4\theta$,
$\theta=18^\circ$ を解く２通りを示す）

(2) 原始N乗根の存在とそれがオイラーの関数個だけあることを確認。

(3)$\mathbb{Z}_n$（加法群）と $\mathbb{Z}_n^*$(乗法群＝既約剰余類群）の導入
$n=p$(素数）のとき、$\mathbb{Z}_p^*$ は巡回群となる。

(4) 円周等分多項式の定義：($(X-\zeta_i)$ の積、ζ_i は原始 n 乗根)

(5) 円分体 Q（ζ）の考察：Q 上のベクトル空間としての拡大体 Q（ζ）の次数がオイラーの関数となる（円周等分多項式の既約性より)、基底の表現

(6) 正多角形の作図可能性 $\Longleftrightarrow$ 円分体の次数（オイラーの関数）が 2 のべき乗

(7) 体の自己同型群の導入、ガロア理論とその意義拡大体と基礎体の中間体とガロア群の部分群の一対一対応（中間体の構造や情報をガロア理論によって、対応する群の情報から知ることができる）

(8) 円分体のガロア群

$X^n=1$ のガロア群が $\mathbb{Z}_n^*$ に同型を確認。円分体につき、$n=5$（巡回群)、7（巡回群)、8（4 元群)、12（4 元群）などを例証で確認

(9)$n=p$（素数、ガロア群が巡回群）について、f 項周期（Q上のベクトル空間としてのQ（ζ）とその部分体の基底）を作成、$n=17$ についての解説 → 正 17 角形の作図（可能)、正 5 角形の作図（可能)、正 7 角形の作図（不能）→ f 項周期の確認 ■

３．序論– オイラーの関数

ここでは、本稿のテーマである円分体の構造を分析するうえで欠かせない整数論的関数、オイラー（Euler) の関数 φ について簡単に触れておく。以下で詳しく述べるように円分体の構造をオイラーの関数が終始一貫して密接に関与することから、始めにこれについての知識を装備することは、効率的に議論を進めるという観点から非常に重要である。

オイラーの関数 φ とは、正の整数 n について、1 から n までの整数で“n と互いに素”なものの個数である。言いかえれば、n との最大公約数が 1 である正の整数（$<n$) の個数である。

例えば、φ（7）＝#｛ 1、2、3、4、5、6｝＝6

一般に素数 p については、φ（p）＝$p-1$.

φ（8）＝#｛1、3、5、7｝＝4

φ（12）＝#｛1、5、7、11｝＝4

などである。このオイラーの関数については、次の乗法の法則が成り立つ。

φ（mn）＝$\varphi(m)\varphi(n)$（ただし、m と n は互いに素）

例えば、3 と 4 は互いに素であるから、

φ（12）＝$\varphi(3)\varphi(4)=2\times 2=4$

が成り立つ。一般的な証明は省くが読者は自ら具体例によって検証されたい。

この乗法の法則を使えば、以下の一般式が成り立つ。

整数 n の素因数分解を、

$n=p_1^{a_1}p_2^{a_2}\cdots\cdots,p_k^{a_k}$($p_i$ は素数)

とするとき、素数 p に対しては、

$\varphi(p^a)=p^a-p^{a-1}$(1 から p^α までの整数のうち、p^α、したがって p と互いに素でないものは、p の倍数 $p,2p,\cdots\cdots,p^\alpha$ だけ、つまり、$p^{\alpha-1}$ 個存在する)

であることから、

$$\begin{aligned}\varphi(n)&=\varphi(p_1^{a_1})\varphi(p_2^{a_2})\cdots\cdots\varphi(p_k^{a_k})\\&=p_1^{a_1}(1-\frac{1}{p_1})p_2^{a_2}(1-\frac{1}{p_2})\cdots\cdots p_k^{a_k}(1-\frac{1}{p_k})\end{aligned}$$

$$= n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots\cdots(1-\frac{1}{p_k})$$
$$= n\prod_{i=1}^{k}(1-\frac{1}{p_i})$$

が成り立つ。例えば、

720$= 2^4 \times 3^2 \times 5$

だから、

$\varphi(720) = 720(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5}) = 192$

となる。

４．$X^n = 1$ と正多角形

正の整数 n に対して、方程式 $X^n = 1$ の解は n 個あり、それらは複素平面上で、原点Oを中心とした半径１の円を n 等分する n 個の点で表される。つまり、解の集合が正 n 角形の n 個の頂点に対応するといったよく知られた事実にいきつく。念のために簡単に証明しておく。

解 X の絶対値は１であるから、$X = \cos\theta + i\sin\theta$($i$ は虚数単位 $\sqrt{-1}$) とおける。ド・モアブルの定理によって、

$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta = 1$　　から

$n\theta = 2k\pi$　となり、$\theta = \frac{2k\pi}{n}(k = 0, 1, \cdots\cdots, n-1)$ から n 個の解は、原点を中心とする半径１の円の円周を n 等分する正 n 角形の頂点となる。

初等的な応用問題として、正５角形を作図してみよう。以下、（１）$X^5 = 1$ を代数的に解く、（２）３角関数を用いるーーーの２通りの方法を示しておく。(1)、(2) とも高校数学までの学習で解くことができる。さらに読者は、ガロアの理論とガウスの方法による一般的な解法を本稿末でみることができよう。

(1) $X^5 = 1$ を解く方法

この方程式は以下のように簡単に解くことができる。$360 \div 5 = 72$ であるから $\cos 72^\circ (= \cos\frac{2}{5}\pi)$ を求めることを目標とする。

$X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + X + 1) = 0$

問題は、$\cos 72^\circ + i\sin 72^\circ$

を求めることで、$\cos 72^\circ$ を求める。

$X \neq 1$ なので、

$X^4 + X^3 + X^2 + X + 1 = 0$

両辺を X^2 で割ると、

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

ここで、$t = X + \frac{1}{X}(= 2\cos 72^\circ)$ とおくと、上式は

$(X^2 + \frac{1}{X^2}) + (X + \frac{1}{X}) + 1 = 0$　より、

$t^2 + t - 1 = 0$

と変形できる。これを解いて、$t = \frac{-1 \pm \sqrt{5}}{2}$

$t = 2\cos 72^\circ$ だから、

$\therefore \cos 72^\circ = \frac{-1 + \sqrt{5}}{4}$

$\sqrt{5}$ は簡単に作図できるので（垂直な２辺の長さが $1,2$ である直角三角形の斜辺の長さが $\sqrt{5}$ となる）、$\cos 72^\circ$ も作図できる。よって、正５角形も作図できる。

（2）３角関数を用いる方法

ここでも、$\cos 72^\circ$ を求めることを目標とする。$\theta = 18^\circ$ とおけば、$\sin\theta = \cos 4\theta$ が成り立つ。この３角方程式を解いて、$\sin\theta(= \cos 4\theta) = \cos 72^\circ$ を求める。

２倍角の公式、

*$\cos 2\theta = \cos^2\theta - \sin^2\theta = 1 - 2\sin^2\theta$

*$\sin 2\theta = 2\sin\theta\cos\theta$

より、

$$\begin{aligned}\cos 4\theta &= 1 - 2\sin^2 2\theta \\ &= 1 - 2(2\sin\theta\cos\theta)^2 \\ &= 1 - 8\sin^2\theta\cos^2\theta \\ &= 1 - 8\sin^2\theta(1 - \sin^2\theta)\end{aligned}$$

$\sin\theta = t$ とおくと、$\Leftrightarrow$

$t = 1 - 8t^2(1 - t^2)$

整理すると、

$8t^4 - 8t^2 - t + 1 = 0 \quad \Leftrightarrow (t-1)(2t+1)(4t^2+2t-1) = 0$

$t \neq 1, -\dfrac{1}{2}$ より、$t = \dfrac{-1+\sqrt{5}}{4}$

これより、当然ながら、（1）と同じ結論を得る。

５．原始N乗根の存在

方程式 $X^n = 1$ の解は、複素平面上で n 個存在するが、この解のなかで、n 乗してはじめて１になる解を原始N乗根という。例えば、$X^8 = 1$ の場合、

$\zeta = \cos\dfrac{2}{8}\pi + i\sin\dfrac{2}{8}\pi$ と置くと当然ながら、ζ は原始N乗根のひとつである。８個の解は、$\zeta^i (i = 0, 1, 2, \cdots 7)$ で表現される。そのなかで例えば $\zeta^2 = i$ は原始N乗根ではない。なぜなら、$i^4 = 1$、すなわち４乗してすでに１になってしまうからだ。一方、ζ^3 は原始８乗根である。なぜなら、実際に累乗を計算してみると、

$(\zeta^3)^1 = \zeta^3,\ (\zeta^3)^2 = \zeta^6,\ (\zeta^3)^3 = \zeta,\ (\zeta^3)^4 = \zeta^4,$

$(\zeta^3)^5 = \zeta^7,\ (\zeta^3)^6 = \zeta^2,\ (\zeta^3)^7 = \zeta^5,\ (\zeta^3)^8 = 1$

となり、８乗してはじめて１になることがわかる。実は、ζ^i が原始８乗根となるためには、“i と８が互いに素”であることがわかる。実際に上記の例でいうなら、３と８は互いに素であるが、２と８は互いに素ではない。よって、原始８乗根は、$\zeta, \zeta^3, \zeta^5, \zeta^7$ の４個である。

一般的には、方程式 $X^n = 1$ の原始N乗根は、$\zeta = \cos\dfrac{2}{n}\pi + i\sin\dfrac{2}{n}\pi$ とすると、

集合 $\{\zeta^i\}$ （i はn と互いに素）

で表され、その個数は、オイラーの関数個、つまり、$\varphi(n)$ 個存在することがわかる。

円周等分多項式など後述するように、円分体の構造の分析には、“オイラー関数個ある原始N乗根”が決定的に重要な役割を果たす。

６．$\mathbb{Z}_n$（加法群）と$\mathbb{Z}_n^*$(乗法群＝既約剰余類群）

正の整数 n に対して、“n を法として”、整数の加法は群をつくる。これは巡回群である。“n を法として”とは、n で割った商の余りが同じときには、それらの整数を同じ類（仲間）とみなすということである。この加法群を $\mathbb{Z}_n$ で表す。例えば、$n = 4$ のときには、$\{0, 1, 2, 3\}$ は 4 を法として、（位数 4 の）加法群 $\mathbb{Z}_4$ をつくる。具体的には、以下のようになる。

*$\mathbb{Z}_4$

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

では、整数 n で、$\{1, 2, \cdots\cdots, n-1\}$ につき、乗法の場合はどうであろうか。同じように群をつくるのであろうか。答えは、群をつくらない。たとえば、$n = 8$ の場合、

２・１＝２、２・２＝４、２・３＝６、２・４＝０、２・５＝２、２・６＝４、２・７＝６（mod ８）

というように、０がでてきてしまうし、２・２＝２・６＝４となり、２と６は同じ類ではないにもかかわらず、２＝６＝２ $^{-1}$・４となってしまうなど至るところで、矛盾が生じてしまうからである。実は、結果からいうと、“n と互いに素な整数”が群をつくるのである。これを“法 n の既約剰余類群”といい、$\mathbb{Z}_n^*$ で表す。例えば、$n = 8$ の場合には、

８と互いに素な整数 $\{1, 3, 5, 7\}$ が法８として群をつくる。具体的に乗積表をつくると、

$\mathbb{Z}_8^*$

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

となる。このような構造を持つ位数４の群を“クラインの４元群”という。逆に、位数４の群は巡回群かクラインの４元群の２通りだけに限られる。**既約剰余類群の位数は、オイラーの関数**であり、後に述べるように、拡大体 Q（ζ) にかかわる自己同型群（ガロア群）の位数ともなるのでこの剰余類群は重要である。。

７．円周等分多項式

本節では、方程式 $X^n = 1$ の根を解に持つ方程式の一般論を展開する。例えば、$X^3 = 1$ の１ではない３乗根 (原始３乗根）は、$X^2 + X + 1 = 0$ の解であり、$\dfrac{-1 \pm \sqrt{3}i}{2}$ となることは周知の事実である。さらにこの多項式 $X^2 + X + 1$ は原始３乗根を零化する最小の既約多項式となる。これを一般化して、原始N乗根を解に持つ最小次数の既約多項式を考えるのである。

結論から先にいえば、オイラーの関数個ある原始N乗根 $\zeta^i(\zeta = \cos\dfrac{2}{n}\pi + i\sin\dfrac{2}{n}\pi)$ について、$X - \zeta^i$ の積、つまり、

$\Phi(X) = \prod(X - \zeta^i)(i$ **と**n **は互いに素）**

i

なる多項式は、ζ^i を零化する最小次数の整数係数の既約多項式であることが知られている。この多項式を円周等分多項式または円分多項式といい、円分体の分析で重要な役割を果たす。その次数はいうまでもなく、原始N乗根の数、つまり、オイラーの関数 $\varphi(n)$ である。整数係数の既約多項式であることの証明はやや複雑であり省略するが、$n = 20$ くらいまで次数 $\varphi(n)$ を念頭に $X^n - 1$ を実際に因数分解して円周等分多項式 Φ を求められたい。これは高校数学の範囲で導くことができる。既約性の証明も重要であるが、読者自ら試行錯誤しながら円周等分多項式を求める練習をすることが重要であると筆者は考える。また、円周等分多項式を求める公式が存在するが本稿では触れない。より専門的な書物を参照されたい。

上述したように、$\Phi_3 = X^2 + X + 1$ である。また、$\varphi(5) = 4$ であるから、
$\Phi_5 = X^4 + X^3 + X^2 + X + 1$
また、$X^8 - 1 = (X^4 + 1)(X^4 - 1)$ と分解でき、$\varphi(8) = 4$ であるから、$\Phi_8 = X^4 + 1$ となる。以下、参考までに Φ_{15} までを示しておく。
$\Phi_3 = X^2 + X + 1$
$\Phi_4 = X^2 + 1$
$\Phi_5 = X^4 + X^3 + X^2 + X + 1$
$\Phi_6 = X^2 - X + 1$
$\Phi_7 = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1,$
$\Phi_8 = X^4 + 1$
$\Phi_9 = X^6 + X^3 + 1$
$\Phi_{10} = X^4 - X^3 + X^2 - X + 1$
$\Phi_{11} = X^{10} + X^9 + X^8 + \cdots\cdots + X^3 + X^2 + X + 1$
$\Phi_{12} = X^4 - X^2 + 1$
$\Phi_{13} = X^{12} + X^{11} + X^{10} + \cdots\cdots + X^3 + X^2 + X + 1$
$\Phi_{14} = X^6 - X^5 + X^4 - X^3 + X^2 - X + 1$
$\Phi_{15} = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$

８．円分体Q（ζ）の基底

有理数体Qに $X^n - 1$ の原始N乗根のひとつを付加してできる数を円分体Q（ζ）という。未知数で素性のわからないものをQに付加するとは一体どんなことでいかなるものに仕上がるかイメージしにくいかもしれないが、代数学の基本定理より、ζ は確かに存在する。要するに有理数と ζ からなる集合の元の間で四則演算をおこなってできる数の集合が Q（ζ）となると理解すればよいのである。さらに、Q（ζ）は自然にQ上のベクトル空間とみることができる。例えば、Q（$\sqrt{2}$）$= \{a + b\sqrt{2} | a, b \in$ Q $\}$ と表すことができ、１、$\sqrt{2}$ がベクトル空間の基底となる。すなわち、a_i を有理数とすれば、Q（ζ）の任意の元 α は、α_i を基底としたとき、
$\alpha = \sum a_i \alpha_i (i = 1, 2, \cdot\cdot\cdot, k.k$ はQ（ζ）の次元）
と一意的に表すことができる。Q（ζ）では、以下の定理が基本的に重要である。
【定理】ベクトル空間Q（ζ）は有限次元で、その次元は $\varphi(n)$, 部分集合 $\{\ 1, \zeta, \zeta^2, \cdots\cdots, \zeta^{\varphi(n)-1}\}$ 、または、$\{\zeta, \zeta^2, \cdots, \zeta^{\varphi(n)}\}$ はどちらもQ（ζ）の基底となる。ただし、φ はオイラーの関数とする。
(証明）ポイントは前述の円周等分多項式の存在。まず、一次独立であることは円周等分多項式の次数、既約性から明らかである。次に、Q（ζ）のいかなる元もこれらの基底の一次結合で表せるのは、どの元も ζ と

有理数の加減乗除、つまり、ζ の多項式 f で表現でき（除には**有理化の原理：いかなるζ の（$\varphi(n)-1$) 次の多項式の逆数も、ζ の多項式で表現できる）**、さらにいかなる多項式 f（X) も、f = R・Φ+r(R、 r はそれぞれ、商と余り）で表現されるから、円周等分多項式の定義から、f(ζ)= r（ζ）となる。そこで Φ の次数がオイラーの関数 φ であることから、 r は ζ のたかだか（$\varphi(n)-1$) 次の多項式で表される。もし、他に $\varphi(n)$ 個の一次独立な部分集合があったら線形代数の一般論（n 次元ベクトル空間で、n 個の一次独立な部分集合があったら、それは基底となる）から直ちにこの部分集合は基底であることが導かれる。

＊有理化の原理：g を（$\varphi(n)-1$) 次の多項式とする。Φ と g は互いに素であるから、$u\Phi+vg=1$ となる多項式 u,v が存在する。しかるに、$\Phi(\zeta)=0$ であるから、$v(\zeta)g(\zeta)=1$ となる。よって、$1/g(\zeta)=v(\zeta)$ となる）■

9．正多角形の作図可能性

正多角形の作図問題は古代から存在する。正３角形、正６角形などは容易に作図できる。本稿の第１節では正５角形の作図方法を示した。しかし、この問題の一般論を扱うのは結構難しく、体論や群論を応用するのでやや複雑である。本節では、正 N 角形が作図できる条件を考える。

作図問題は、定木とコンパスだけを用いるので、作図に出てくる点は、直線と直線、直線と円、あるいは円と円の交点であるから、解析幾何学の用語を用いれば、直線や円の方程式だけが存在する世界となる。だからその交点は、たかだか１次か２次方程式の解として描かれる。つまり、そこに出てくる数は有理数か平方根号 $\sqrt{a}$ や $\sqrt{\sqrt{a}+b}$(a,b は有理数）などの世界である。だからたとえば、２の３乗根 $\sqrt[3]{2}$ は作図することはできない。以上のように単純に考えただけでも、正７角形は作図不能であることがわかる。なぜなら、$X^7=1$ の解には無理数となる有理数の３乗根が現れることは容易に想像でき、３乗根は作図不能であるから（$\sqrt[3]{8}$ などは除く)、正７角形は作図不能であることがわかる。ただ、$X^7=1$ を代数的に解くことはできる。

正 N 角形が作図できるとは、第１節で述べたように、$\cos\dfrac{2\pi}{n}$ が作図できること、または同じことだが原始 N 乗根 $\zeta=\cos\dfrac{2}{n}\pi+i\sin\dfrac{2}{n}\pi$ が作図できることに他ならない。いま、拡大体の列

$Q\subset F_1\subset F_2\subset\cdot\cdot\cdot\subset F_r(Q\ (\zeta))$

とするとき、ζ が作図できるためには、体の列が２次拡大の連鎖になっていることが必要十分であることがイメージできよう。Q の２次拡大には２次方程式が関与するからである。つまり、

$(F_i:F_{i-1})=2$

であることが必要十分である。このとき、

$(Q\ (\zeta):Q)=2^{\nu}$

が成立する。上記５でみたように、$(Q\ (\zeta):Q)=\varphi(n)$ であったから、正 N 角形が作図できるためには、

$\varphi(n)=2^{\nu}$

が成立しなければならない。ここが作図問題のポイントである。よく、n や $n-1$ が２のべき乗であることと勘違いしやすいが、正しくは、**オイラーの関数が２のべき乗**であるような整数につき作図可能であることに留意されたい。後は、計算だけである。いま、n の素因数分解を

$n=2^{\varepsilon}p_1^{\varepsilon_1}p_2^{\varepsilon_2}\cdots p_k^{\varepsilon_k}$

とする。ここで、p_j は奇の素数である。このとき、第３節でみたように

$\varphi(n)=2^{\varepsilon-1}p_1^{\varepsilon_1-1}(p_1-1)\cdots p_k^{\varepsilon|-1}(p_k-1)$

これが２のべき乗となるための条件は、

$\varepsilon_1 = \varepsilon_2 = \cdots = \varepsilon_k = 1$　かつ

$p_i = 2^\mu + 1$

となることが必要十分である。そして、p_i が $2^\mu + 1$ なる素数となるためには、μ がまた 2 のべき乗であることが必要である（**なぜか**）。

つまり、奇の素因数は、

$$p_i = 2^{2^\rho} + 1$$

という形をしていなくてはならない。$\rho = 0, 1, 2, 3, 4$ に対応する素数は、

$3, 5, 17, 257, 65537$

となる。ここで本稿の主役たる 17 がようやく顔を現した。なお、ここまでの過程を振り返ったときに、既約剰余類群、円周等分多項式、Q（ζ）、正多角形の作図問題のいずれにもオイラーの関数が出現し、さらにそれが問題のカギを握っていることがわかる。3 節 (序論）でオイラーの関数をはじめに説明したのも納得されよう。

10．体とガロア理論

本節からいよいよ本稿の主題の核心に迫る。まず、ガロア理論の中心的な定理ーー体と群の一対一対応ーーを概説して、それを円分体に適用する。いわゆるガロア理論はいくつかの主要な定理から構成されるが、本節ではなかでも中心的で応用範囲の広い定理を述べる。参考までに、ガロア理論全体の構成の概略を本節末に示しておく。本稿では、正 17 角形を作図することが目的であるから、ガロア理論の詳細は述べない。詳しくはガロア理論の専門書を参照されたい。

ここで、体論の用語を簡単に説明しておく。E を体とする。このとき、E の部分集合 K でそれ自体で体の構成要件を満たすとき、K を E の部分体という。逆に K からみたとき、E を K の拡大体という。さらに、体 K を固定してその拡大体を論じるとき、K を基礎体という言い方をすることがある。

円分体の議論では、Q や Q（ζ）（ζ は 1 の原始 N 乗根）を基礎体とすることが多い。また、群ではその部分群の列を論じることが多いのに対して、体では拡大体の列を論じる場合が多い。

(1) 体の自己同型

E を体とするとき、E から E の全単射の写像で同型となるもの、すなわち、体の二つの演算、和と積を保存するもの、つまり、E の任意の元、a, b に対して、

$$\begin{cases} \sigma(a+b)) = \sigma(a) + \sigma(b) \\ \sigma(ab) = \sigma(a)\sigma(b) \end{cases}$$

が成り立つ写像 σ を E の自己同型（写像）という。E の自己同型写像の集合は、写像の合成を演算として群を作ることは容易にわかり、これを E の自己同型群といい、$Aut(E)$ で表す。

また、K を E の部分体とするとき、K の元を不動にするような E の自己同型の集合は $Aut(E)$ の部分群となり、これを、“E の K 上の自己同型群”といい、$G(E/K)$ で表す。特に E **が**K **のガロア拡大という条件**を満たすとき、自己同型群をガロア群と呼ぶ。円分体の理論では、Q（ζ）は Q のガロア拡大となり、$Q(\zeta)$ の Q 上の自己同型群 (これは、ガロア群である）$G(Q(\zeta)/Q)$ を考えることが主要なテーマとなる。

(2) ガロア理論の基本定理

基礎体 K とその拡大体 E があり、この拡大がガロア拡大という条件を満たすとき、K と E の中間体 M とガロア群（E の K 上の自己同型群）$G(E/K)$ の部分群 H には一対一対応が存在する。この体と群の対応という体と群を結びつける定理を**ガロア理論の基本定理**という。この定理で複雑な体の情報が、構造がわかりやすい群の情報に置きかわり、この群を分析すればよいことがわかる。基本定理は独立した定理で、方程式論や円分体の構造、正多角形の作図問題にも応用できる重要な定理である。。**K がE のある有限自己同型群G の固定体となっているとき、E をK のガロア拡大という。**このとき、**E 内に解を持つような$K[x]$ の任意の既約多項式はE 内で分解する**。ガロア拡大は重要だがその詳細は述べない。読者はまずは、体と群が一対一対応するという点に着眼していただきたい。

体と群の対応規則は、

＊ $G\,(E/M) = H$(E の M 上の自己同型群）

＊ $M = E_H$(H の固定体）

で与えられる。ここで固定体とは、G の部分群（部分集合でもよい）H に対して、すべての $\sigma \in H$ に対して、$\sigma(a) = a$ となるような $a \in E$ の全体からなる集合は E の部分体となり、これを H の固定体というのである。

ガロアの基本定理－体と群の対応

$$\begin{array}{ccc} E & === & e \\ | & & | \\ M & === & H \\ | & & | \\ K & === & G \end{array}$$

φ : 中間体の集合＜ーーーーー＞部分群の集合

$$M <\text{ーーーーーーーー}> H$$

$\varphi(M) = G(E/M)$(E の M 上の自己同型群）

$\varphi^{-1}(H) = E_H$(H の固定体）

ガロア拡大についての詳細な説明は長くなるので省略するが、円分体 $Q(\zeta)$ の議論ではガロア拡大は成立するので読者はまずは、“円分体 $Q(\zeta)$ の部分体とガロア群 $G(Q(\zeta)/Q)$ の部分群が一対一対応する”という点を念頭に置いて論理展開に注目されたい。

【参考】ガロア理論の論点整理

ガロア理論は壮麗な交響楽のようで、その理論構成は見事としかいいようがないのだが、あまりの重層的な創りに見方を誤ると迷路から抜け出せないという危うさを常に孕んでいる。

そこで、理論の論点をまとめてみた。ガロア理論の解説書は多くみられるが、いずれも難解なものばかりで論点をまとめて提示するなど教育に配慮した書物は少ない。だから自分がいま、どこの山場の何合目にいるかという立ち位置がわからず、迷子になってしまうのである。その場合、必ず下記の四つの山場のいずれかに迷い込んでいることは間違いない。この参考を自らの立ち位置を確認するものとして使っていただきたい。

まず第一の柱が (1) ガロアの基本定理：基礎体 K とその拡大体 E があり、この拡大がガロア拡大という条件を満たすとき、K と E の中間体とガロア群（E の K 上の自己同型群）の部分群には、一対一対応が存在するーーーという体と群を結びつける美しい定理で、複雑な体の情報が、構造がわかりやすい群の情報に置き換

わり、この群を分析すればよいことがわかる。(1) は代数学で独立した重要な定理で、方程式論のほか、円分体の構造や正多角形の作図問題にも応用できる重要な定理である。筆者はときどき、このガロアの基本定理を“代数学の基本定理”といい、通常の代数学の基本定理（実数係数の多項式は解を持つ）を“解析学の基本定理”と呼んだほうが妥当と思うことがあるが、そうなったら、代数学の基本定理を理解できるひとがほとんどいなくなってしまい、教育上好ましくないから、今のままでよいのだ、などと思っている。

第２の山場 (2) 代数方程が代数的に解ける（解が係数の四則演算とべき根で表現できる）ことと方程式のガロア群が可解群（商群が巡回群であるような正規部分群の列が存在する群）であることが同値である。これがガロア理論の最大の山場で、これは難解だが、その基になるのが、(3) 基礎体（１の原始 N 乗根を含むとする）のガロア拡大が巡回拡大（ガロア群が巡回群となるような体の拡大）ならば、この拡大は冪根拡大（基礎体に正の定数 a の n 乗根を付加した体）である。逆も成り立つ。つまり、冪根拡大ならばガロア群は巡回群となるーーーという定理が基本的かつ決定的に重要である。(2) はイメージしにくいのだが、(3) は数学的に美しく、納得性があるというか、イメージしやすい特徴があると筆者は思っている。ここに可解群の原型をみることができる。

これを越えたならば、最後の山場が (4)n 次の一般代数方程式のガロア群は、n 次の対称群 (置換群）S_n で、n が４以下ならば可解群、５次以上ならば非可解群ーーとなり、(2) と (4) から、ガロアが見破った『５次以上の代数方程式には解の公式がない』、つまり、係数の四則演算と冪根では表現できない、という結論に到達する。現代のガロア理論では、(1)〜(4) を総称してガロア理論と呼んでいるようだ。ここで、注意すべきは、(1)、(3)、(4) はそれぞれ独立した定理であることである。(2) を (1)、(3) を用いて証明することがガロア理論の最大の山場となる。また、群の可解性という言葉にも注意が必要だ。この可解群という表現は、方程式の可解性に結びつけて、後追いで定義された、とってつけたような表現になっていることがガロア理論をかえってわかりにくくしているようだ。

果たして、ガロアはどのようにしてこれらを導いたのであろうか。現代の数学では、構造主義の影響をうけて理路整然と構成されているが、ガロアは (1) から (4) を順序付けて構築したのか、それともガロアの情熱とともに渾然一体と感じながら総合的に導いたのか。たとえば、(4) は、(1)〜(3) がわからずとも理解できるひとつの定理（交換子群と巡回置換、偶置換の関連から導かれる）なのだが、(1)〜(3) があってはじめて存在意義があるものでもある。私個人的にはガロア群が巡回群であることと方程式の可解性の関係を感じとったのではないかと思う。その際、ガロア群として具体的な代数方程式の置換群 (対称群）を考えたのである。いや、代数方程式の解の置換という行為から群の概念が生み出されたのであり、それを構造的に構築しなおしたものが現代のガロア理論なのである。そして、これこそがガロアが後世に残した最大の遺産である。そもそも、群という概念は、ガロアの時代には一般論として存在せず、上述したように置換群から原始的な群の概念がおこったと考えられる。このあたりは、現在、ガロアの原論文の邦訳が出ているので、興味ある方はそれを参照されたい。■

11．円分体のガロア群

本節では、円分体のガロア群が既約剰余類群 $\mathbb{Z}_n^*$ と同型でることを示し、それを用いて次節で n が素数であるときの円分体 $Q(\zeta)$ の Q 上の基底、いわゆる“ガウスの f 項周期”を導き出し、これから一気に正 17 角形の作図問題を解決する。ここに抽象的なガロア理論がいかにしてガウスが示した具体的事象に結実するかをみることができよう。読者は、ガロアとガウスが響きあうようにして問題の核心に迫るドラマチックな過程に注目されたい。

円分体、つまり、有理数体 Q に方程式 $X^n = 1$ の原始 N 乗根を付加してできる体 Q（ζ）の自己同型はどんな形をした写像であろうか。

まず、自己同型は、１の n 乗根をまた１の n 乗根に写す。なぜなら、任意の自己同型に対して、

$\{\sigma(\zeta)\}^n = \sigma(\zeta^n) = \sigma(1) = 1$

が成り立つからである。（任意の σ は、有理数体を不動とする。なぜか）

よって、円分体の自己同型は、

$\sigma_i : \zeta - \rightarrow \zeta^i$ (i は n と互いに素)

なる形をしており、その個数は原始 n 乗根の数、つまり、オイラーの関数 $\varphi(n)$ 個ある。よって、円分体の自己同型群（ガロア群）G（Q (ζ)/Q）の位数は、$\varphi(n)$ である。では、そのガロア群はいかなる構造をしているのだろうか。いま、２つの自己同型 $\sigma_{i,}\sigma_j$ に対して、

$$\begin{aligned}\sigma_i\sigma_j(\zeta) &= \sigma_i(\zeta^j) = \{\sigma_i(\zeta)\}^j = (\zeta^i)^j = \zeta^{i\times j} \\ &= \sigma_{i\times j}(\zeta)\end{aligned}$$

よって、

$\sigma_i\sigma_j = \sigma_{i\times j}$

が成り立つ。つまり、自己同型の合成の演算は法 n の既約剰余類群 $\mathbb{Z}_n^*$ と同型となることがいえる。

(1)$n = 5$ の場合、ガロア群は位数４の巡回群。真部分群は位数２の巡回群。

(2)$n = 7$ の場合、ガロア群は位数６の巡回群。真部分群は位数２、３の巡回群。

(3)$n = 8$ の場合、ガロア群は位数４のクラインの４元群。真部分群は位数２の巡回群。

(4)$n = 12$ の場合、ガロア群は位数４のクラインの４元群。真部分群は位数２の巡回群。

(5)$n = 17$ の場合、ガロア群は位数 16 の巡回群。真部分群は位数 2、4、8 の巡回群。

読者は群 $\mathbb{Z}_n^*$ の乗積表をつくって、自ら詳細に分析されたい。

＊ $\mathbb{Z}_5^*$

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

＊ $\mathbb{Z}_8^*$

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

＊ $\mathbb{Z}_7^*$

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

12．正 17 角形の作図

12-1 原始根による原始p 乗根の表現

以下、p を素数として

円周等分多項式

$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots\cdots + X^2 + X + 1$

を考える。

ζ を以下の原始 p 乗根とする。

$$\zeta = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$$

$\varphi(p) = p - 1$ より、

Q（ζ）はQ上で、$(p-1)$ 次元ベクトル空間であり、Q（ζ）のQ上の自己同型群 G（Q（ζ)/Q）は位数 $p-1$ の巡回群となる。

８節より、Q（ζ）のQ上の基底として、

$\{1,\zeta,\zeta^2,\cdots,\zeta^{p-2}\}$ あるいは、$\{\zeta,\zeta^2,\cdots,\zeta^{p-1}\}$

が考えられる。つまり、Q（ζ）の任意の元αは、

$\alpha = b_0 + b_1\zeta + b_2\zeta^2 + \cdots + b_{p-2}\zeta^{p-2}$

あるいは、

$= c_1\zeta + c_2\zeta^2 + \cdots + c_{p-1}\zeta^{p-1}$

と表現される（$b_i, c_i \in$ Q）

いま、法 p の原始根のひとつを g とする。

集合 $\{1, g, g^2, \cdots g^{p-2}\}$ は法 p として、

集合として、$\{1, 2, 3, \cdots, p-1\}$ に一致する（順序は対応しないことに注意）

たとえば、$p = 7$ とすると、$g = 3$ は原始根となり、

$g^i = n (\mathrm{mod}\, 7)$ の対応は、

i	0	1	2	3	4	5
n	1	3	2	6	4	5

となる（読者は検証されたい）

いま、

$\zeta_i \equiv \zeta^{g^i}$

と定義する。原始根 g によるこの原始 p 乗根の表記は、以下、本稿で一貫して出てくるので、はじめはわかりにくいかもしれないが、ぜひともこの表記に慣れていただきたい。

$\{\zeta_0,\zeta_1,\zeta_2,\cdots,\zeta_{p-2}\} =$

$\{\zeta, \zeta^2, \zeta^3, \cdots, \zeta^{p-1}\}$
となるので、

$\{\zeta_0, \zeta_1, \cdots, \zeta_{p-2}\}$ はQ（ζ）のQ上の基底となる。つまり、Q（ζ）の任意の元αは、
$\alpha = a_0\zeta_0 + a_1\zeta_1 + \cdots + a_{p-2}\zeta_{p-2}(a_i \in \mathrm{Q})$

と一意的に表現することができる。
なお、
$\zeta_{p-1} = \zeta_0$ に注意されたい。
$\because g^{p-1} \equiv 1 (\mathrm{mod}\, p)$(フェルマーの小定理）より、
$\zeta_{p-1} = \zeta^{g^{p-1}} = \zeta^1 = \zeta^{g^0} = \zeta_0$

12．2 Q（ζ）の部分体の基底（ｆ項周期）
いま、Q（ζ）の自己同型 σ を、
$\sigma(\zeta_0) = \sigma(\zeta^{g0}) = \zeta^{g^1} = \zeta_1$
と定義する。
すると、
$\sigma(\zeta_i) = \sigma(\zeta^{g^i}) = \sigma(\zeta)^{g^i} = (\zeta^g)^{g^i} = \zeta^{g \cdot g^i} = \zeta^{g^{i+1}} = \zeta_{i+1}$
よって、
$\sigma(\zeta_i) = \zeta_{i+1}$ よって
$\sigma^2(\zeta_i) = \sigma(\zeta_{i+1}) = \zeta_{i+2}$
より、

$\sigma^\nu(\zeta_i) = \zeta_{i+\nu}$

が成り立つ。つまり、σ^ν は、ζ_i の添字を ν 個ずらすことになる。
これからいよいよ、Q（ζ）の部分体のQ上の基底、いわゆるｆ項周期を前述の自己同型とガロアの理論によって求める。
$p-1 = ef$ とおくと、$G = (Q(\zeta)/Q)$ には各 f に対して、位数 f の部分群（巡回群）H_f が存在し、ガロアの理論によって、体と群の一対一対応が存在する。
$M_f <------> H_f$

$$\begin{array}{ccc} Q(\zeta) & - & e \\ | & & | \\ M_f & === & H_f \\ | & & | \\ Q & - & G = Q(Q(\zeta)/Q) \end{array}$$

H_f は巡回群で、σ を生成元とすると、
$H_f = \left\{\sigma^e, \sigma^{2e}, \cdot\cdot\cdot, \sigma^{fe}\right\}$
と表される。ただし、$\sigma^{fe} = \sigma^{p-1} \equiv$ 恒等写像
ガロア対応の規則より、

M_f は H_f の固定体であるから、
α $\in M_f \iff \forall\psi \in H_f \quad \psi(\alpha) = \alpha$

12.1 から、任意の α ∈ Q（ζ）に対して、
α $= a_0\zeta_0 + a_1\zeta_1 + a_2\zeta_2 + \cdot\cdot\cdot + a_{p-2}\zeta_{p-2}$

と一意的に表すことができる。
$\alpha \in M_f$ とすると
$\sigma^e(\alpha) = \alpha$・・・(∗)
が成り立つ。前述の $\sigma^\nu(\zeta_i) = \zeta_{i+\nu}$ より、(∗) を満たす α の表現を具体的に明確化しよう。
α $= \quad a_0\zeta_0 + a_1\zeta_1 + a_2\zeta_2 + \cdot\cdot\cdot + a_{p-2}\zeta_{p-2}$
$\sigma^e(\alpha) = a_0\zeta_e + a_1\zeta_{1+e} + a_2\zeta_{2+e} + \cdot\cdot\cdot + a_{p-2}\zeta_{p-2+e}$
ここで、

$\zeta_{p-1} = \zeta^{g^{p-1}} = \zeta^1 = \zeta^{g^0} = \zeta_0 (g^{p-1} \equiv 1)$
$\zeta^{p-2+e} = \zeta^{g^{p-2+e}} = \zeta^{g^{(p-1)+(e-1)}}$
$= (\zeta^{g^{p-1}})^{g^{e-1}} = (\zeta^1)^{g^{e-1}}$
など　$\zeta^{g^{e-1}} = \zeta_{e-1}$
などを用いて、α_i の係数を比較すると、
$a_0 = a_e$
$a_1 = a_{e+1}$
$a_2 = a_{e+2}$
$\vdots \qquad \vdots$
$a_{p-2-e} = a_{p-2}$
$a_{p-1-e} = a_0$
$\vdots \qquad \vdots$
$\vdots \qquad \vdots$
$a_{p-2} = a_{e-1}$

を得た。例として、$p = 17, e = f = 4$ とすると
$a_0 = a_4$
$a_1 = a_5$
$a_2 = a_6$
$a_3 = a_7$
$a_4 = a_8$
$a_5 = a_9$
$a_6 = a_{10}$
$a_7 = a_{11}$
$a_8 = a_{12}$
$a_9 = a_{13}$
$a_{10} = a_{14}$

$a_{11} = a_{15}$
$a_{12} = a_0$
$a_{13} = a_1$
$a_{14} = a_2$
$a_{15} = a_3$
よって、
$a_0 = a_4 = a_8 = a_{12}$
$a_1 = a_5 = a_9 = a_{13}$
$a_2 = a_6 = a_{10} = a_{14}$
$a_3 = a_7 = a_{11} = a_{15}$
よって、

$$\begin{aligned}\alpha = a_0(\zeta_0 + \zeta_4 + \zeta_8 + \zeta_{12}) + \\ a_1(\zeta_1 + \zeta_5 + \zeta_9 + \zeta_{13}) + \\ a_2(\zeta_2 + \zeta_6 + \zeta_{10} + \zeta_{14}) + \\ a_3(\zeta_3 + \zeta_7 + \zeta_{11} + \zeta_{15})\end{aligned}$$

と表現できる。実は、この各々のカッコが実は、$M_f = M_4$ の基底となっているのである。これこそがガウスが発見したｆ項周期の原始的な姿である。

以上、ガロアの理論と自己同型写像の考えを用いて、円分体の基底を求める考え方を示したが、これをふまえて一般の素数次方程式 $X^p = 1$ の円分体の基底を明示的に求めてみよう。まず、以下の巡回群についての基本的な定理を確認しておこう。

【定理】位数 n の巡回群Ｇにおいて、n の約数 d に対して、位数 d の部分群（巡回群）がただひとつ存在する（証明略)■

$X^p = 1(p:$ 素数）のガロア群Ｇは位数 $p-1$ の巡回群となる。再度、$p-1 = ef$ とおくと、上の定理から位数 f の部分群 G_f が存在し、それは、
$G_f = \left\{\sigma^e, \sigma^{2e}, \sigma^{3e}, \cdots, \sigma^{ef}\right\}$
である。ただし、σ^{ef} は恒等写像、σ^e は群の生成元である。G_f の固定体 M_f はＱ上で e 次元のベクトル空間（Ｑ（ζ）の部分体）であり、Ｑ上の基底を**ｆ項周期**と呼ぶ。くり返すと、ｆ項周期とは“位数 f の部分群の固定体（Ｑ上 e 次元）の基底”である。M_f のＱ基底はこれまでの議論から具体的には、

$$\begin{array}{ccccccccccccc}
\eta_0 & = & \zeta_0 & + & \zeta_e & + & \zeta_{2e} & + & \cdots & \cdots & + & \zeta_{(f-1)e} \\
\eta_1 & = & \zeta_1 & + & \zeta_{1+e} & + & \zeta_{1+2e} & + & \cdots & \cdots & + & \zeta_{1+(f-1)e} \\
\vdots & & & \vdots & & \vdots & & \vdots & & & \vdots & \\
\eta_i & = & \zeta_i & + & \zeta_{i+e} & + & \zeta_{i+2e} & + & \cdots & \cdots & + & \zeta_{i+(f-1)e} \\
\vdots & & & \vdots & & \vdots & & \vdots & & & \vdots & \\
\eta_{e-1} & = & \zeta_{(e-1)} & + & \zeta_{(e-1)+e} & + & \zeta_{(e-1)+2e} & + & \cdots & \cdots & + & \zeta_{(e-1)+(f-1)e}
\end{array}$$

と表せる。これは本稿で最も重要な数式である。これこそ、ガウスが発見した**ｆ項周期**の具体的な表現である。このｆ項周期が天下り的にいきなり与えられたら、読者はさぞかし困惑するであろうが、これまでのガロ

アの理論や自己同型の議論によって、ｆ項周期が自然に導出されることに合点がいくであろう。ここにガロアとガウスが響きあいながら融合するのである。

＊ガロアとガウスの融合

$$\begin{array}{ccc} Q(\zeta) & === & e \\ | & & | \\ M_f & === & G_f \\ | & & | \\ Q & === & G = G(Q(\zeta)/Q) \end{array}$$

ｆ項周期＝位数ｆの部分群 G_f の固定体 M_f の Q 基底

M_f の情報＜ーーー＞ G_f の情報

いま、$\eta_i, \eta_j \in M_f$ の基底に対して、$\eta_i\eta_j$ を考えるが、当然、$\eta_i\eta_j \in M_f$ だから、この積は、

$\eta_0, \eta_1, \cdots \eta_{e-1}$ の一次結合で表せる。やや技術的になるが、$\eta_i\eta_j$ の具体的な計算方法を示す。これが、$X^p = 1$ の解法、つまり、正 17 角形の作図方法につながる。

いま、$p = 17, e = f = 4$ として、具体的に考えてみよう。

$$\eta_i = \zeta_i + \zeta_{i+4} + \zeta_{i+8} + \zeta_{i+12}$$
$$\eta_j = \zeta_j + \zeta_{j+4} + \zeta_{j+8} + \zeta_{j+12}$$

として、$\eta_i\eta_j$ を以下のように記述して計算する。

$$\begin{aligned} \eta_i\eta_j = &(\zeta_i\zeta_j + \zeta_{i+4}\zeta_{j+4} + \zeta_{i+8}\zeta_{j+8} + \zeta_{i+12}\zeta_{j+12}) \\ &+(\zeta_i\zeta_{j+4} + \zeta_{i+4}\zeta_{j+8} + \zeta_{i+8}\zeta_{j+12} + \zeta_{i+12}\zeta_j) \\ &+(\zeta_i\zeta_{j+8} + \zeta_{i+4}\zeta_{j+12} + \zeta_{i+8}\zeta_j + \zeta_{i+12}\zeta_{j+4}) \\ &+(\zeta_i\zeta_{j+12} + \zeta_{i+4}\zeta_j + \zeta_{i+8}\zeta_{j+4} + \zeta_{i+12}\zeta_{j+8}) \end{aligned}$$

読者はかけ算の規則性と以下に注目されたい。

・$\sigma^4 : \zeta_i\zeta_j \to \zeta_{i+4}\zeta_{j+4} \to \zeta_{i+8}\zeta_{j+8} \to \zeta_{i+12}\zeta_{j+12} \to \zeta_i\zeta_j$

・$\zeta_{16} = \zeta^{g^{16}} = \zeta^1 = \zeta^{g^0} = \zeta_0$

・$\zeta_{i+16} = \zeta^{g^{i+16}} = \zeta^{g^i g^{16}} = (\zeta^{g^{16}})^{g^i} = (\zeta^1)^{g^i}$

$\quad = \zeta^{g^i} = \zeta_i$

・$g^{16} \equiv 1 (\mathrm{mod}\, 17)$

ところで、各々のかっこをよくみると、自己同型 $\sigma^e (= \sigma^4)$ で不変となることがわかる。

１の p 乗根の積である $\zeta_{i+ke}\zeta_{j+le}$ は１または原始 p 乗根であることに注意すると、$\eta_0, \eta_1, \cdots\cdots, \eta_{e-1}$ も σ^e で不変となることから、

＊$\eta_i\eta_j$ の各々のかっこは、すべて１（この場合は$\eta_i\eta_j = 4$) または、$\eta_0, \eta_1, \cdots\cdots, \eta_{e-1}$ のいずれかに等しい！

ことがわかる。

１２．３　$p = 17$ の場合

以上の考察を $p = 17$ に適用して、正 17 角形の作図問題を解決する。本稿９節・正多角形の作図可能性で述べたように、正 17 角形は作図可能の条件を満たしている。以下、$X^{17} = 1$ を実際に解き、さらに作図方法を述べる。

法 17 の原始根として 3 をとり、
$\zeta_i \equiv \zeta^{3^i}$
と定義する。$X^{17}=1$ の 1 以外の根は、
$\zeta_i (i=0,1,\cdots,15)$ で表現される。つまり、
集合 $\{\zeta^1,\zeta^2,\zeta^3,\cdots,\zeta^{16}\}$ は、
集合 $\{\zeta_0,\zeta_1,\zeta_2,\cdots,\zeta_{15}\}$ に一致する。
下に、ζ_i と ζ^n の対応表を示しておく。これは、複雑な ζ_i の計算をわかりすくするものである。

ζ_0	ζ_1	ζ_2	ζ_3	ζ_4	ζ_5	ζ_6	ζ_7	ζ_8	ζ_9	ζ_{10}	ζ_{11}	ζ_{12}	ζ_{13}	ζ_{14}	ζ_{15}
ζ^1	ζ^3	ζ^9	ζ^{10}	ζ^{13}	ζ^5	ζ^{15}	ζ^{11}	ζ^{16}	ζ^{14}	ζ^8	ζ^7	ζ^4	ζ^{12}	ζ^2	ζ^6

以下で、ζ_i,ζ_j の計算が頻繁に出てくるが、いずれも上の表を用いれば計算は
簡単になるので、読者はこの表を丹念に検証されたい。なお、ζ_i は mod 17 で考える。例えば、
$\zeta_{16}=\zeta^{3^{16}}=\zeta^1=\zeta^{3^0}=\zeta_0$
$(3^{16}\equiv 1 (\mathrm{mod}\, 17))$
となる。

$X^{17}=1$ の円分体のガロア群 $G(Q(\zeta)/Q)$ は位数 16 の巡回群
$\{1,\sigma^2,\sigma^3,\cdots,\sigma^{15}\}$ となり、位数 2,4、8 の部分群（巡回群）$H_{2,}H_{4,}H_8$ が存在し、ガロアの理論によって、それらに $Q(\zeta)$ の部分体 $M_{2,}M_{4,}M_8$ が対応する。

＊ガロアの対応

Q（ζ)(16 次元)　===　e
|　　|
M_2(8 次元)　===　H_2(位数 2)
|　　|
M_4(4 次元)　===　H_4(位数 4)
|　　|
M_8(2 次元)　===　H_8(位数 8)
|　　|
Q　===　$G=G(Q(\zeta)/Q)$

$H_2=\left\{\sigma^8,\sigma^{16}\right\}$
$H_4=\left\{\sigma^4,\sigma^8,\sigma^{12},\sigma^{16}\right\}$
$H_8=\left\{\sigma^2,\sigma^4,\sigma^6,\sigma^8,\sigma^{10},\sigma^{12},\sigma^{14},\sigma^{16}\right\}$

（σ^{16} は恒等写像）
ここでガウスの f 項周期とは、部分体 M_i の基底であることに留意されたい。以下、$f=8,4,2$ の f 項周期を具体的に求める。
（1）8 項周期（M_8 の基底）
$16=p-1=2\times 8$
より、

$$\eta_0 = \zeta_0 + \zeta_2 + \zeta_4 + \zeta_6 + \zeta_8 + \zeta_{10} + \zeta_{12} + \zeta_{14}$$
$$\eta_1 = \zeta_1 + \zeta_3 + \zeta_5 + \zeta_7 + \zeta_9 + \zeta_{11} + \zeta_{13} + \zeta_{15}$$
$$\begin{aligned}\eta_0 + \eta_1 &= \zeta_0 + \zeta_1 + \zeta_2 + \cdots\cdots + \zeta_{15} \\ &= \zeta^1 + \zeta^2 + \cdots\cdots + \zeta^{16} \\ &= -1\end{aligned}$$

より、$\eta_0 + \eta_1 = -1$

次に、$\eta_0\eta_1$ を計算するが、これには前述の $\eta_0\eta_1$ のかけ算の規則性を用いる。

$$\begin{aligned}\eta_i\eta_j = &(\zeta_0\zeta_1 + \zeta_2\zeta_3 + \cdots\cdots + \zeta_{14}\zeta_{15})(1) \\ &+(\zeta_0\zeta_3 + \zeta_2\zeta_5 + \cdots\cdots + \zeta_{14}\zeta_1)(2) \\ &+(\zeta_0\zeta_5 + \zeta_2\zeta_7 + \cdots\cdots + \zeta_{14}\zeta_3)(3) \\ &+(\zeta_0\zeta_7 + \zeta_2\zeta_9 + \cdots\cdots + \zeta_{14}\zeta_5)(4) \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &+(\zeta_0\zeta_{15} + \zeta_2\zeta_1 + \cdots\cdots + \zeta_{14}\zeta_{13})(8)\end{aligned}$$

ここで各々のかっこは、η_0, η_1 のいずれかとなるが、それを知るには始めの項を計算することによって、η_0, η_1 のどちらになるかを確認すればよい。たとえば (1) では、

$$\zeta_0\zeta_1 = \zeta^{3^0}\zeta^{3^1} = \zeta^{1+3} = \zeta^4 = \zeta_{12}$$

となり、ζ_{12} は η_0 の項であるから、(1) のかっこは η_0 となる。同じ要領で、

$$\begin{aligned}\eta_0\eta_1 = &\ (\zeta^4 + \cdots) + (\zeta^{11} + \cdots) + (\zeta^6 + \cdots) + (\zeta^{12} + \cdots) + \\ &(\zeta^{15} + \cdots) + (\zeta^8 + \cdots) + (\zeta^{13} + \cdots) + (\zeta^7 + \cdots) \\ = &(\zeta_{12} + \cdots) + (\zeta_7 + \cdots) + (\zeta_{15} + \cdots) + (\zeta_{13} + \cdots) + \\ &(\zeta_6 + \cdots) + (\zeta_{10} + \cdots) + (\zeta_4 + \cdots) + (\zeta_{11} + \cdots) \\ = &\ \eta_0 + \eta_1 + \eta_1 + \eta_1 \\ &+\eta_0 + \eta_0 + \eta_0 + \eta_1 \\ = &\ 4(\eta_0 + \eta_1) = -4\end{aligned}$$

$\therefore \eta_0\eta_1 = -4$

以上から、

$$\begin{cases} \eta_0 + \eta_1 = -1 \\ \eta_0\eta_1 = -4 \end{cases}$$

よって、

η_0, η_1 は、$X^2 + X - 4 = 0$ の根となるから、

$$\eta_0, \eta_1 = \frac{-1 \pm \sqrt{17}}{2}$$

ここでようやく、本稿の主役である数 17 が顔をだしたことに留意されたい。

煩雑な計算が延々と続くことに辟易とする読者もおられるかもしれないが、正 17 角形の作図方法の解法は、ζ の添字とべき乗との戦いでもある。ここで、基本に戻って以下の計算方法を再度確認されたい。

$\zeta_i\zeta_j = \zeta^m\zeta^n = \zeta^{m+n} = \zeta_k$

⋮ー ー 表を用いる ーー⋮

(2) 4項周期 (M_4 の基底)

$16 = 4 \cdot 4$

$\xi_0 = \zeta_0 + \zeta_4 + \zeta_8 + \zeta_{12}$

$\xi_1 = \zeta_1 + \zeta_5 + \zeta_9 + \zeta_{13}$

$\xi_2 = \zeta_2 + \zeta_6 + \zeta_{10} + \zeta_{14}$

$\xi_3 = \zeta_3 + \zeta_7 + \zeta_{11} + \zeta_{15}$

$\xi_0 + \xi_2 = \eta_0$

$\xi_1 + \xi_3 = \eta_1$

$$
\begin{aligned}
\xi_0\xi_2 &= (\zeta_0 + \zeta_4 + \zeta_8 + \zeta_{12}) \\
&\quad \times (\zeta_2 + \zeta_6 + \zeta_{10} + \zeta_{14}) \\
&= (\zeta_0\zeta_2 + \zeta_4\zeta_6 + \zeta_8\zeta_{10} + \zeta_{12}\zeta_{14}) \\
&\quad +(\zeta_0\zeta_6 + \zeta_4\zeta_{10} + \zeta_8\zeta_{14} + \zeta_{12}\zeta_2) \\
&\quad +(\zeta_0\zeta_{10} + \zeta_4\zeta_{14} + \zeta_8\zeta_2 + \zeta_{12}\zeta_6) \\
&\quad +(\zeta_0\zeta_{14} + \zeta_4\zeta_2 + \zeta_8\zeta_6 + \zeta_{12}\zeta_{10}) \\
&= (\zeta^1\zeta^9 + \zeta^{13}\zeta^{15} + \zeta^{16}\zeta^8 + \zeta^4\zeta^2) \\
&\quad +(\zeta^1\zeta^{15} + \zeta^{13}\zeta^8 + \zeta^{16}\zeta^2 + \zeta^4\zeta^9) \\
&\quad +(\zeta^1\zeta^8 + \zeta^{13}\zeta^2 + \zeta^{16}\zeta^9 + \zeta^4\zeta^{15}) \\
&\quad +(\zeta^1\zeta^2 + \zeta^{13}\zeta^9 + \zeta^{16}\zeta^{15} + \zeta^4\zeta^8) \\
&= (\zeta^{10} + \zeta^{28} + \zeta^{24} + \zeta^6) \\
&\quad +(\zeta^{16} + \zeta^{21} + \zeta^{18} + \zeta^{13}) \\
&\quad +(\zeta^9 + \zeta^{15} + \zeta^{25} + \zeta^{19}) \\
&\quad +(\zeta^3 + \zeta^{22} + \zeta^{31} + \zeta^{12}) \\
&= (\zeta^{10} + \zeta^{11} + \zeta^7 + \zeta^6) \\
&\quad +(\zeta^{16} + \zeta^4 + \zeta^1 + \zeta^{13}) \\
&\quad +(\zeta^9 + \zeta^{15} + \zeta^8 + \zeta^2) \\
&\quad +(\zeta^3 + \zeta^5 + \zeta^{14} + \zeta^{12}) \\
&= (\zeta_3 + \zeta_7 + \zeta_{11} + \zeta_{15}) \\
&\quad +(\zeta_8 + \zeta_{12} + \zeta_0 + \zeta_4) \\
&\quad +(\zeta_2 + \zeta_6 + \zeta_{10} + \zeta_{14}) \\
&\quad +(\zeta_1 + \zeta_5 + \zeta_9 + \zeta_{13}) \\
&= \xi_3 + \xi_0 + \xi_2 + \xi_1 \\
&= -1
\end{aligned}
$$

同様に、

$$
\begin{aligned}
\xi_1\xi_3 &= (\zeta_1 + \zeta_5 + \zeta_9 + \zeta_{13}) \\
&\quad \times (\zeta_3 + \zeta_7 + \zeta_{11} + \zeta_{15}) \\
&= (\zeta_1\zeta_3 + \zeta_5\zeta_7 + \zeta_9\zeta_{11} + \zeta_{13}\zeta_{15}) \\
&\quad +(\zeta_1\zeta_7 + \zeta_5\zeta_{11} + \zeta_9\zeta_{15} + \zeta_{13}\zeta_3)
\end{aligned}
$$

$$
\begin{aligned}
&+(\zeta_1\zeta_{11}+\zeta_5\zeta_{15}+\zeta_9\zeta_3+\zeta_{13}\zeta_7)\\
&+(\zeta_1\zeta_{15}+\zeta_5\zeta_3+\zeta_9\zeta_7+\zeta_{13}\zeta_{11})\\
&=(\zeta_4+\zeta_8+\zeta_{12}+\zeta_0)\\
+&(\zeta_9+\zeta_{13}+\zeta_1+\zeta_5)\\
&+(\zeta_3+\zeta_7+\zeta_{11}+\zeta_{15})\\
&+(\zeta_2+\zeta_6+\zeta_{10}+\zeta_{14})\\
&=\xi_0+\xi_1+\xi_3+\xi_2\\
&=-1
\end{aligned}
$$

$$
\begin{cases}\xi_0+\xi_2=\eta_0\\ \xi_0\xi_2=-1\end{cases}
\begin{cases}\xi_1+\xi_3=\eta_1\\ \xi_1\xi_3=-1\end{cases}
$$

ξ_0,ξ_2 は、$X^2-\eta_0X-1=0$ の根
ξ_1,ξ_3 は、$X^2-\eta_1X-1=0$ の根

よって、
$\xi_0,\xi_2=\dfrac{\eta_0\pm\sqrt{\eta_0+4}}{2}$
$\xi_1,\xi_3=\dfrac{\eta_1\pm\sqrt{\eta_1+4}}{2}$

η_0,η_1 は８項周期ですでに求められているので、ξ_0,ξ_1,ξ_2,ξ_3 も求めることができる。
（３）２項周期
$16=8\cdot 2$
２項周期
$\lambda_0=\zeta_0+\zeta_8$
$\lambda_1=\zeta_1+\zeta_9$
$\lambda_2=\zeta_2+\zeta_{10}$
$\lambda_3=\zeta_3+\zeta_{11}$
$\lambda_4=\zeta_4+\zeta_{12}$
$\lambda_5=\zeta_5+\zeta_{13}$
$\lambda_6=\zeta_6+\zeta_{14}$
$\lambda_7=\zeta_7+\zeta_{15}$

からなる。ここで、
$\lambda_0+\lambda_4=\xi_0$
$\lambda_1+\lambda_5=\xi_1$
$\lambda_2+\lambda_6=\xi_2$
$\lambda_3+\lambda_7=\xi_3$

$$
\begin{aligned}
\lambda_0\lambda_4&=(\zeta_0+\zeta_8)(\zeta_4+\zeta_{12})\\
&=(\zeta_0\zeta_4+\zeta_8\zeta_{12})+(\zeta_0\zeta_{12}+\zeta_8\zeta_4)\\
&=(\zeta^{14}+\zeta^3)+(\zeta^5+\zeta^{12})
\end{aligned}
$$

$$
\begin{aligned}
&= (\zeta_9 + \zeta_1) + (\zeta_5 + \zeta_{13}) \\
&= \lambda_1 + \lambda_5 \\
&= \xi_1
\end{aligned}
$$

$$
\begin{aligned}
\lambda_1\lambda_5 &= (\zeta_1 + \zeta_9)(\zeta_5 + \zeta_{13}) \\
&= (\zeta_1\zeta_5 + \zeta_9\zeta_{13}) + (\zeta_1\zeta_{13} + \zeta_9\zeta_5) \\
&= (\zeta^8 + \zeta^9) + (\zeta^{15} + \zeta^2) \\
&= (\zeta_{10} + \zeta_2) + (\zeta_6 + \zeta_{14}) \\
&= \lambda_2 + \lambda_6 \\
&= \xi_2
\end{aligned}
$$

$$
\begin{aligned}
\lambda_2\lambda_6 &= (\zeta_2 + \zeta_{10})(\zeta_6 + \zeta_{14}) \\
&= (\zeta_2\zeta_6 + \zeta_{10}\zeta_{14}) + (\zeta_2\zeta_{14} + \zeta_{10}\zeta_6) \\
&= (\zeta^{24} + \zeta^{10}) + (\zeta^{11} + \zeta^{23}) \\
&= (\zeta_{11} + \zeta_3) + (\zeta_7 + \zeta_{15}) \\
&= \lambda_3 + \lambda_7 \\
&= \xi_3
\end{aligned}
$$

$$
\begin{aligned}
\lambda_3\lambda_7 &= (\zeta_3 + \zeta_{11})(\zeta_7 + \zeta_{15}) \\
&= (\zeta_3\zeta_7 + \zeta_{11}\zeta_{15}) + (\zeta_3\zeta_{15} + \zeta_{11}\zeta_7) \\
&= (\zeta^4 + \zeta^{13}) + (\zeta^{16} + \zeta^1) \\
&= (\zeta_{12} + \zeta_4) + (\zeta_8 + \zeta_0) \\
&= \lambda_4 + \lambda_0 \\
&= \xi_0
\end{aligned}
$$

以上より、８項周期、４項周期、２項周期をまとめると、

・8 項周期

$$
\begin{cases}
\eta_0 + \eta_1 = -1 \\
\eta_0\eta_1 = -4
\end{cases}
$$

$$
\eta_0, \eta_1 = \frac{-1 \pm \sqrt{17}}{2}
$$

・4 項周期

$$
\begin{cases}
\xi_0 + \xi_2 = \eta_0 \\
\xi_0\xi_2 = -1
\end{cases}
$$

$$
\xi_0, \xi_2 = \frac{\eta_0 \pm \sqrt{\eta_0^2 + 4}}{2}
$$

$$
\begin{cases}
\xi_1 + \xi_3 = \eta_1 \\
\xi_1\xi_3 = -1
\end{cases}
$$

$$
\xi_1, \xi_3 = \frac{\eta_1 \pm \sqrt{\eta_1^2 + 4}}{2}
$$

・２項周期

$$\begin{cases} \lambda_0+\lambda_4=\xi_0 \\ \lambda_0\lambda_4=\xi_1 \end{cases} \begin{cases} \lambda_1+\lambda_5=\xi_1 \\ \lambda_1\lambda_5=\xi_2 \end{cases}$$

$$\begin{cases} \lambda_2+\lambda_6=\xi_2 \\ \lambda_2\lambda_6=\xi_3 \end{cases} \begin{cases} \lambda_3+\lambda_7=\xi_3 \\ \lambda_3\lambda_7=\xi_0 \end{cases}$$

８項周期は２次方程式の解ですでにわかっており、４項周期は８項周期より、２項周期は４項周期より順次求められるから、結局、η_i, ξ_i, λ_i のすべての値を求めることができるから、結局、$X^{17}=1$

の解をすべて求めることができるのである。そして、正 17 角形の作図では、

$\zeta+\zeta^{-1}=2\cos\dfrac{2\pi}{17}$（$\zeta=\zeta_0$）

を求めればよいのであるから、

$\lambda_0=\zeta_0+\zeta_8=\zeta_0+\zeta_0^{-1}=\zeta+\zeta^{-1}$($\zeta_8=\zeta_0^{-1}$ に注意）より、

$\lambda_0=2\cos\dfrac{2\pi}{17}$ より、λ_0 がわかればよいのであるが、これはすでにわかっているので、最終的に解決できたことになる。あとは、ひたすら計算するだけであり、腕力の問題である。計算より、

$$\begin{aligned}\lambda_0&=\zeta+\zeta^{-1}\\ &=\frac{1}{16}\left(-1+\sqrt{17}+2\sqrt{\tfrac{17-\sqrt{17}}{2}}+4\sqrt{\tfrac{17+3\sqrt{17}}{4}-\sqrt{\tfrac{17+\sqrt{17}}{2}}-\tfrac{1}{2}\sqrt{\tfrac{17-\sqrt{17}}{2}}}\right)\end{aligned}$$

となる。この値は無理数として平方根しか表れていないから作図することができるので、結局正 17 角形も作図することができるのである。具体的な作図方法は、本サイトの”正 17 角形の作図”または、高木貞治の『代数学講義』を参照されたい。■

12.4　$p=5,7$ の場合

以上で、$X^{17}=1$ を解くことによって、正 17 角形が作図できることを示したが、ｆ項周期の応用として、以下で $X^5=1$(正 5 角形)、$X^7=1$(正 7 角形）について考えてみよう。

(1)$X^5=1$(正 5 角形）

$$\Phi_5=X^4+X^3+X^2+X+1=0$$

を解く。原始 5 乗根 ζ を

$\zeta=\cos\dfrac{2\pi}{5}+i\sin\dfrac{2\pi}{5}$

とおく。法 5 の原始根のひとつとして、3 をとる。

ζ_i	ζ_0	ζ_1	ζ_2	ζ_3
ζ^n	ζ^1	ζ^3	ζ^4	ζ^2

$5-1=4=2\times2$ であるから、２項周期しか存在しない。それは、

$\eta_0=\zeta_0+\zeta_2(=\zeta_0+\zeta_0^{-1})$

$\eta_1=\zeta_1+\zeta_3(=\zeta_1+\zeta_1^{-1})$

$\eta_0+\eta_1=-1$

$$\begin{aligned}\eta_0\eta_1&=(\zeta_0+\zeta_2)(\zeta_1+\zeta_3)\\ &=(\zeta_0\zeta_1+\zeta_2\zeta_3)+(\zeta_0\zeta_3+\zeta_2\zeta_1)\\ &=(\zeta^1\zeta^3+\zeta^4\zeta^2)+(\zeta^1\zeta^2+\zeta^4\zeta^3)\end{aligned}$$

$$= (\zeta^4 + \zeta^6) + (\zeta^3 + \zeta^7)$$
$$= (\zeta^4 + \zeta^1) + (\zeta^3 + \zeta^2)$$
$$= -1$$

$$\begin{cases} \eta_0 + \eta_1 = -1 \\ \eta_0\eta_1 = -1 \end{cases}$$

よって、η_0, η_1 は、$X^2 + X - 1 = 0$ の根である。

$\eta_0, \eta_1 = \dfrac{-1 \pm \sqrt{5}}{2}$

$\eta_0 = \zeta_0 + \zeta_0^{\hat{}1} = \dfrac{-1 + \sqrt{5}}{2} = 2\cos\dfrac{2\pi}{5}$ より、

$\cos\dfrac{2\pi}{5} = \dfrac{-1 + \sqrt{5}}{4}$

これより、４節と同じ結果が得られた。

（２） $X^7 = 1$(**正７角形）**

$\Phi = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$

を解く。

$\rho = \cos\dfrac{2\pi}{7} + i\sin\dfrac{2\pi}{7}$ とおく。

法７の原始根として、３をとる。

ρ_i と ρ^n との対応は、

$$\begin{vmatrix} \rho_i & \rho_0 & \rho_1 & \rho_2 & \rho_3 & \rho_4 & \rho_5 \\ \rho^n & \rho^1 & \rho^3 & \rho^2 & \rho^6 & \rho^4 & \rho^5 \end{vmatrix}$$

２項周期（$e = 3, f = 2$) を考える。

$$\begin{cases} \xi_0 = \rho_0 + \rho_3 (= \rho_0 + \rho_0^{-1}) \\ \xi_1 = \rho_1 + \rho_4 (= \rho_1 + \rho_1^{-1}) \\ \xi_2 = \rho_2 + \rho_5 (= \rho_2 + \rho_2^{-1}) \end{cases}$$

計算の結果より、

$$\begin{cases} \xi_0 + \xi_1 + \xi_2 = -1 \\ \xi_0\xi_1 + \xi_1\xi_2 + \xi_2\xi_0 = -2 \\ \xi_0\xi_1\xi_2 = 1 \end{cases}$$

より、ξ_0, ξ_1, ξ_2 が代数的に求まる。

$$\begin{cases} \rho_0 + \rho_3 = \xi_0 \\ \rho_0\rho_3 = 1 \end{cases}$$

より、ρ_0, ρ_3 は、$X^2 - \xi_0 X + 1 = 0$ の解となる。

これより、$X^7 = 1$ を解くことができる。

しかし、ξ_i は無理数となる有理数の３乗根を含み、この３乗根は作図できないので、正７角形も作図することはできない。

■コラム：やはり、人類の至宝はオイラーなのか

自然対数の底を e として、

$e^{i\pi} = -1$

なる等式が“人類の至宝”という本を見かけたことがある。小説『博士の愛した数式』（小川洋子著）の題材にもなった数式とか。。。しかし、私にとっては、オイラーの関数 $\varphi(n)$(n と互いに素な整数の個数）こそが、人類の至宝であるようなような気がする。前者は、オイラーの公式、$e^{i\theta} = \cos\theta + i\sin\theta$ と、$e^x, \sin\theta, \cos\theta$ のテイラー展開（あるいは、マクロリン展開）さえ知っていれば済むことである（ただ、それが持つ数学的な意味あるいは意義は奥深いものがあるが)。

一方、オイラーの関数のすごさは、群論、体論、初等整数論、解析、線形代数学のそれぞれの初歩を知らないとわからない。オイラーの関数が重要なのは、たとえば、方程式 $X^n = 1$ の原始 N 乗根 ζ の個数、拡大体 $Q(\zeta)$ の Q 上のベクトル空間としての次元、原始 N 乗根を解に持つ Q 上の既約な最小次数の多項式（円周等分多項式）の次数、また、$X^n = 1$ のガロア群（法 n の既約剰余類群 $\mathbb{Z}_n^*$ に同型）の位数などがいずれもオイラーの関数 $\varphi(n)$ であるなどと円分体の重要な構造をオイラーの関数が一貫して関与していることから明らかである。

このようにオイラーの関数が現代数学の重要な箇所で顔を現わすその美しさは優に芸術作品に匹敵する。正多角形の作図可能性も『オイラーの関数が２のべき乗』であることがポイントとなっていた。さらに、有名な未解決の数学の大問題リーマン予想のゼータ関数も

$$\zeta(s) = \sum_{n=1}^{+\infty} 1/n^s = \prod_{p:prime} \frac{1}{1 - \frac{1}{p^s}}$$

と表現され、この右辺もオイラー積と呼ばれている。このように考えてくると、いずれにしても人類の至宝はオイラーなのかも知れない。■

＊本稿の執筆では、

『ガロアの理論』（ポストニコフ、東京図書）

『現代代数学』（ファン・デル・ヴェルデン、東京図書）

＊ガウスの f 項周期は以上の２冊によっている。また、『現代代数学』には、具体的な作図方法がのべられている。

『代数学講義』（高木貞治、共立出版）

＊具体的な作図方法が述べられている。

『ガロワと方程式』（草場公邦、朝倉書店）

『代数系入門（松坂和夫、岩波書店)』

などを参考とした。

＊筆者経歴

東京大学理学部数学科を経て教育学部卒業。証券会社、外資系通信社で金融・資本市場の業務を経験。専門は、債券資本市場。主な著書・論文：『信用リスクを読む』（日本評論社)、『信用リスクとM＆A』（同)、『世界金融危機と信用リスク』（同)、『鎮めの文化と資本市場』（ブルームバーグ)、『金融派生商品』

メール：sakurasaku9286@willcom.com