作図問題とGalois理論に関する教材作成の試み

林　　雄一郎
北海道情報大学

A Trial of Preparation of the Teaching Materials about the Construction Problems and the Galois Theory

Yuuichirou HAYASHI
Hokkaido Information University

平成28年 3 月

北海道情報大学紀要　第27巻　第 2 号別刷

〈研究ノート〉

作図問題と Galois 理論に関する教材作成の試み

林　　雄一郎

A Trial of Preparation of theTeaching Materials about the Construction Problems and the Galois Theory

Yuuichirou　HAYASHI*

要　旨

正７角形は初等幾何学の作図法では描画不可能であるが、折り紙で折れる。学生がこの理由を数学的に学ぶことは、意義のあることである。この状況は代数方程式を冪根で解くことにも類似している。このように、限られた操作で何かを形成することが出来るか否かの数理的な決定問題は一般に興味深いことである。

本稿では、群論の初歩や体の拡大、円分多項式と１の n 乗根、正多角形の作図問題と Galois 理論、折紙による作図についての教材を提案する。

Abstract

Regular heptagon can’t be drawn by construction method of elementary geometry, but it can be foled with ORIGAMI. It is meaningful that students can learn this reason mathematically. This situation is similar to the solution method of algebraic equations by roots.Like these, mathematical decision problems on whether or not we can make something by limited operations must be generally interesting.

In this paper, the author proposed teaching materials related to an introduction of group theory and extension of fields, cyclotomic polynomial and n-th root of unity, the problem of the geometric construction of regular polygon and the Galois theory, and drawing figures with ORIGAMI.

キーワード

回転，群, Abel 群，部分群，巡回群，位数，正規部分群，剰余群，準同型，同型，可解群,対称群，交代群，体，自己同型，添加した体，拡大体，ベクトル空間，拡大次数，体の拡大，中間体，最小分解体, Galois 拡大, Galois 群，固定体, Klein の四元群，冪根拡大，方程式の Galois 群，代数的に解ける, 1 の n 乗根，円分多項式，円分体，正７角形の作図不能,折紙作画

*北海道情報大学情報メディア学部情報メディア学科特任教授

Specially appointed Professor,Department of Information Media,Faculty of Information Media

1 はじめに

正5角形には黄金比が隠れており、学校数学の刺激的な教材である。その幾何学的作図(以下、作図という)の一つは、直角を挟む2辺の長さが1、$\frac{1}{2}$ となる直角三角形の斜辺の長さ $\frac{\sqrt{5}}{2}$ に $\frac{1}{2}$ を加えて黄金比 $\frac{1+\sqrt{5}}{2}$ を作図し、これを対角線とする5角形を描けばよい。正5角形となる証明も容易である。

次は正7角形の作図ということになる。だが、これは原理的にできない。しかし、正7角形は存在するし、折り紙の操作で折れる。

この事情は、複素係数 n 次代数方程式の根は複素数の範囲に n 個存在する(代数学の基本定理(Gauss,1799)にもかかわらず、$n \geq 5$ の場合には一般的に方程式の根が代数的演算(加減乗除、冪根)で構成できない(Abel,1826)ということに似ている。

正 n 角形の作図について、ギリシャ人は $n = 3,4,5,6,8,9,10,12,15,16$ のとき可能であることを知っていた。これらはすべて $2^p 3^q 5^r$ ($p = 0,1,2,\cdots, q = 0,1,2, r = 0,1$) の形をした数である。そのため、この形の数しか作図できないと長らく信じられてきた。$n = 17$ はこのような数で表せないから作図不能というわけである。

ところが、1796年3月30日の朝、19歳のGaussは、1の17乗根は開平だけで求められることを発見した。すなわち、「p がFermat素数 $2^m + 1$ ならば、m 回の二次方程式を解けば正 p 角形は作図可能である」ことを構成的に示した。$17 = 2^4 + 1$ だから $p = 17$ の場合二次方程式を4回解けば作図可能である。この命題の逆、「正 p 角形が作図可能ならば、p はFermat素数となる」は比較的容易に示せる。この対偶命題より、正7角形の作図不能が示せる。

本稿は、数学教師を目指す学生向けの教材となるよう意図している。代数学において群と体の架け橋となるGalois理論は方程式の解法から発しているが、作図問題とも深くかかわっており、何とも美しい理論である。短期間で容易に概観できる教材は出来ないものかと思案していたところである。

1〜**5** はGalois理論への入門教材、**6**〜**7** は作図と体の拡大、**8** は正7角形の作図不能、**9** は他の作図問題、**10** はGalois理論を用いた命題「p がFermat素数ならば、正 p 角形は作図可能である」の証明、そして **11** は折り紙を用いた正7角形、角の3等分線の作画について触れている。

2 群という考え

2.1 群の例

Galois(1811-1832)が提唱した群論の初歩的教材を提示する。身の回りの事象には様々な規則性が見出される。例えば、正3角形の美しさは、その対称性にあり、多くの数理が隠れている。対称性は、対象自体を回転軸や対称軸の周りに重ねる変換によって認識できる。そこで次の例1のように図形の移動を考察し群の概念を導入する。

例1 正葉曲線 $r = 3\sin(3\theta - \pi)$ を、原点 O を中心に $120^0, 240^0$ 左回転させる移動をそれぞれ r_1, r_2 , AA', BB', CC' (図1)を対称軸として折り返す移動をそれぞれ s_1, s_2, s_3 とし、これらと何も動かさない移動 e の集合を D_3 とする。このとき、移動の合成を考える。例えば、原点を中心に120°回転した後 AA' を対象軸として折り返す移動 $s_1 r_1$

の結果は BB' に対称の折り返し s_2 となる。合成の結果を表 1 に示す。この表から次の①～④が分かる。① D_3 の任意の移動 x, y の合成はまた D_3 のどれかの移動になる、② 3 つの移動 x, y, z の合成 xyz は xy, yz の合成順に依らず同じになる、③どの移動 x との合成もまた x になる移動 e がある、④どの移動 x にも合成した結果が e となる移動 y がある。

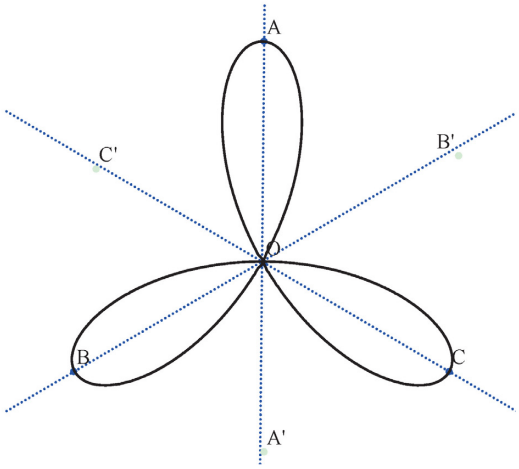

図 1　正葉曲線の回転・折り返し

D_3	e	r_1	r_2	s_1	s_2	s_3
e	e	r_1	r_2	s_1	s_2	s_3
r_1	r_1	r_2	e	s_3	s_1	s_2
r_2	r_2	e	r_1	s_2	s_3	s_1
s_1	s_1	s_2	s_3	e	r_1	r_2
s_2	s_2	s_3	s_1	r_2	e	r_1
s_3	s_3	s_1	s_2	r_1	r_2	e

表 1　群 D_3 の乗積表

2.2　群の定義

集合 G がその元 a, b に対して積と呼ばれる G の元 ab を対応させる演算をもち次の①～③を満たすとき G は群をなすという。

① $G \ni a, b, c$ に対して、次式が成り立つ［結合法則］
$(ab)c = a(bc)$

②単位元と呼ばれる元 e があり、$G \ni a$ に対して $ae = ea = a$ となる

③ $G \ni a$ に対して逆元と呼ばれる元 a^{-1} が定まり $aa^{-1} = a^{-1}a = e$ となる

単位元、逆元は唯 1 つある。群の元の個数をその群の位数といい $|G|$ と記す。有限の位数を持つ群を有限群という。交換法則 $ab = ba$ が成り立つ群を Abel 群または加法群という。また、群 G の部分集合 H が G の積で群となるとき、H は G の部分群という。

表 1 は移動の合成を演算とする積を表にしたものであり乗積表と呼ばる。これより、D_3 は群をなすことが分かる。有限群は乗積表で表される。$R_3 = \{e, r_1, r_2\}$ は D_3 の部分群であり、Abel 群となる。

一般に、置換とは $\{1, 2, 3, \cdots, n\}$ からそれ自身への 1:1, 上への対応である。図 1 で頂点 A, B, C を $1, 2, 3$ とすると、D_3 の回転、折り返しは次のような対応する置換で表現できる。この置換の集合を S_3 と記す。

$$r_1 \leftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123) \quad r_2 \leftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$$

$$s_1 \leftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23) \quad s_2 \leftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13)$$

$$s_3 \leftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12) \quad e \leftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1)$$

置換 $\begin{pmatrix} 1 & 2 & 3 \\ i & j & k \end{pmatrix}$ は対応 $\{1 \to i, 2 \to j, 3 \to k\}$ を表し、巡回置換 (ijk) は対応 $\{i \to j, j \to k, k \to i\}$ を表す。(ij) を互換という。n 文字の置換の群は n 次対称群といい S_n と記す。S_3 の乗積表は D_3 と構造が同じになる

から群となる。S_3 は 3 次対称群である。

$(123)=(13)(12),(132)=(12)(13)$ のように偶数個の互換の積となる置換を偶置換という。S_n の偶置換全体は部分群となる。これを n 次交代群といい A_n と記す。R_3 に対応する $\{(1),(123),(132)\}$ は S_3 の部分群で 3 次交代群 A_3 となり Abel 群である。

例 2 $F(x_1,x_2,x_3)=x_1x_2+x_2x_3+x_1x_3$ という文字式の添数を S_3 の元の作用で動かしても不変である。この式は対称式といわれ、$x_1+x_2+x_3$ や $x_1x_2x_3$ も同様である。

例 3 整数の集合 Z は加法群となる。単位元は 0、a の逆元は $-a$ となる。有理数全体 Q、実数全体 R、複素数全体 C も加法に関して群になる。また、0 を除く有理数全体、実数全体、複素数全体は乗法に関して群(乗法群という)になる。このとき、単位元は 1、a の逆元は $1/a$ である。

例 4 $\zeta_k=\cos\left(\frac{2k\pi}{3}\right)+i\sin\left(\frac{2k\pi}{3}\right)$ に対して、$\{\zeta_0,\zeta_1,\zeta_2\}$ は乗法群になり、単位元は ζ_0、ζ_k の逆元は ζ_{-k} である。一般に、群 G のすべての元が、ある元 a の冪で表されるとき G を巡回群といい、a をその生成元という。この群を $<a>$ と記す。この例では $\zeta_2=\zeta_1^2$ だから $\{\zeta_0,\zeta_1,\zeta_2\}$ は ζ_1 を生成元とする巡回群となり $<\zeta_1>=\mu_3$ と記す。μ_3 は Abel 群で $|\mu_3|=3$ となる。。

2.3 剰余群、正規部分群、指数

H を群 G の部分群、$G\ni a$ とする。

$aH=\{ah\,|\,h\in H\}$ とおく。このとき G の元はどれかの aH に属し、$aH\cap bH=\phi$ と $aH\neq bH$ は同値だから G は部分集合 aH で類別される。a_r を含む類 a_rH は H を法とする左剰余類という。右剰余類も同様に定義される。集合 A,B に対して $A\cap B=\phi$ のとき、$A\cup B$ を $A+B$ と記し A と B の直和という。$a_iH\cap a_jH=\phi,i\neq j$ だから、群 G は左剰余類の直和に分解される。

$$G=H+a_2H+a_3H+\cdots+a_rH.$$

このとき剰余類の個数 r は、H の G に対する指数といい $(G:H)$ と記す。

任意の $a\in G$ に対して $aH=Ha$ が成り立つとき、H を G の正規部分群といい $H\triangleleft G$ と記す。このとき、剰余類の集合 $\{H,aH,bH,\cdots\}$ に積 $(aH)(bH)=abH$ を定義すれば群になる。単位元は H, aH の逆元は $a^{-1}H$ である。これを G の H による剰余群といい G/H と記す。

$G\supset M\supset H$ で H,M が G の部分群のとき、$(G:H)=(G:M)(M:H)$ が成り立ち、部分群 M の位数は、G の位数の約数となる(Lagrange)。

2.4 群の準同型、同型

群 G から群 G' への写像 f が次の条件を満たすとき準同型という。

$$G\ni a,b,\ f(ab)=f(a)f(b)$$

$G\triangleright H$ のとき、群 G から剰余群 G/H への

写像を$G \ni a, \psi(a) = aH$と定義するとき

ψはGからG/Hへの自然な準同型という。また、準同型ψが1:1、上への対応のときGの同型写像という。

二つの群G, G'の間に同型な写像があるとき、GとG'は同型といい$G \cong G'$と記す。このとき２つの群は同じ構造を持つ。例えば一方がAbel群ならば他方もAbel群となるし、位数も同じとなる。

例５　$D_3 \cong S_3$.　$R_3 \cong A_3 \cong \mu_3$

$D_3 = R_3 + s_i R_3 = R_3 + R_3 s_j, i = 1,2,3$

より　$s_i R_3 = R_3 s_i$　$\therefore R_3 \lhd D_3$.

$s_i R_3 = \{s_1, s_2, s_3\}$に$(1\,2)A_3$が対応する。

$S_3 = A_3 + (12)A_3 = A_3 + A_3(12)$　$\therefore A_3 \lhd S_3$

$S_3 \supset A_3 \supset \{e\}, \{e\} \lhd A_3 \lhd S_3$.・・①

$S_3 / A_3 = \{A_3, (12)A_3\}, A_3 / \{e\}$はAbel群になる　・・②

2.5 可解群とその例

次の条件を満たす部分群の列を持つ群Gを可解群という。

$G = N_r \supset N_{r-1} \supset \cdots \supset N_1 = \{e\}$.

$N_i \rhd N_{i-1}, N_i / N_{i-1}$はAbel群

2.4の①，②より３次対称群S_3は可解群になる。４次対称群S_4も可解群となる。

３　体とその拡大

3.1　体という考え

加減乗除の演算で閉じている集合を考える。例えば、有理数全体は加法$a+b$と乗法abで閉じている。一般に、２種類の演算$a+b, a \cdot b$が定義され、次の①～③を満たす集合を体という。これをKと記す。

①　$a+b$について加法群となる。

②　$a \cdot b$について、集合$K^{\times} = K - \{0\}$

Abel群となる。1：乗法単位元

③　分配法則が成り立つ。

$$a \cdot (b+c) = a \cdot b + a \cdot c$$
$$(a+b) \cdot c = a \cdot c + b \cdot c.$$

例６ 有理数全体Q,実数全体R,複素数全体Cは加法、乗法で体となる。

体Kから体K'への写像ψが1:1,上への対応で次の条件を満たすとき同型という。

$$\psi(x+y) = \psi(x) + \psi(y), \psi(xy) = \psi(x)\psi(y)$$

このときK, K'は体の演算に関して同じ構造を持つ。また、$K = K'$のとき同型ψをKの自己同型という。

例７　素数pで割った余りが同じ整数の集合をpを法とする剰余類といい、その全体をF_pまたはZ/pZと記す。このとき、

余りが$k\,(0 \le k \le p-1)$の剰余類を$\overline{k}$と記す。$\overline{k} = \{a \mid a \equiv k \bmod p, a \in Z\}$.

剰余類全体は$F_p = \{\overline{0}, \overline{1}, \cdots, \overline{p-1}\}$となる。

F_pに加法＋と乗法・を次のように定義する。$F_p \ni \overline{a}, \overline{b}$　$\overline{a} + \overline{b} = \overline{a+b}$　$\overline{a} \cdot \overline{b} = \overline{ab}$

この定義が可能なのは

$a \equiv a' \bmod p, b \equiv b' \bmod p$　から

$a + a' \equiv b + b' \bmod p, ab \equiv a'b' \bmod p$が成

り立つからである。

・加法に関して以下が成り立つ。

$\overline{a}+\overline{0}=\overline{a+0}=\overline{0+a}=\overline{0}+\overline{a}=\overline{a}.$ $\overline{0}$:零元

$\overline{a}+\overline{-a}=\overline{a+(-a)}=\overline{0}.$ $-\overline{a}=\overline{-a}$:逆元

したがって、F_p は加法群になる。

・乗法に関して以下が成り立つ。

$\left(\overline{a\cdot b}\right)\cdot\overline{c}=\overline{a\cdot b\cdot c}=\overline{a}\cdot\left(\overline{b}\cdot\overline{c}\right).$

$\overline{a}\cdot\overline{b}=\overline{ab}=\overline{b}\cdot\overline{a}.$

・$\overline{1}$ を乗法の単位元とすると $\overline{a}\overline{1}=\overline{1}\overline{a}=\overline{a}.$

・$\overline{a}\neq\overline{0}$ で a,p が互いに素のとき、不定方程式 $ax+py=1$ は整数解をもつ。したがって、$ax\equiv 1 \bmod p$ となり、これは $\overline{a}\overline{x}=\overline{1}$ だから $\overline{a}$ の逆元が存在する。

よって、$F_p-\left\{\overline{0}\right\}=F_p^{\times}$ は乗法群になり Abel 群である。これを法 p の既約剰余類群という。この群の位数は、Euler 関数 $\varphi(m)$（m 以下の正整数で m と素なものの個数を表す)を用いると次のように表せる。 $\left|F_p^{\times}\right|=\varphi(p)=p-1.$

・分配法則が成り立つ。

$\overline{a}\cdot\left(\overline{b}+\overline{c}\right)=\overline{a\cdot b+a\cdot c}=\overline{a}\cdot\overline{b}+\overline{a}\cdot\overline{c}.$

$\left(\overline{a}+\overline{b}\right)\cdot\overline{c}=\overline{a\cdot c+b\cdot c}=\overline{a}\cdot\overline{c}+\overline{b}\cdot\overline{c}.$

以上から、F_p は体(可換体)となる。

3.2 体の拡大

有理数体 Q に無理数 $\sqrt{2}$ を加えた数の集合 $\{a+b\sqrt{2}\mid a,b\in Q\}$ を考える。

$Q\ni a,a',b,b'$ のとき、この集合の元に対して加減乗除を考える。

$$(a+b\sqrt{2})\pm\left(a'+b'\sqrt{2}\right)$$
$$=(a\pm a')+(b\pm b')\sqrt{2}.$$
$$\left(a+b\sqrt{2}\right)\left(a'+b'\sqrt{2}\right)$$
$$=(aa'+2bb')+(ab'+a'b)\sqrt{2}.$$
$$\frac{a+b\sqrt{2}}{a'+b'\sqrt{2}}=\frac{aa'-2bb'+(a'b-ab')\sqrt{2}}{a'^2-2b'^2}$$

が成り立ち、四則演算で閉じていることが分かり、この数の集合は体となる。これは $\sqrt{2}$ を含む最小の体であり、Q に $\sqrt{2}$ を添加した体といい $Q\left(\sqrt{2}\right)$ と記す。

一般に、体 K と K に属さない数 α を含む最小の体を K に α を添加した体といい $K(\alpha)$ と記す。また、$\alpha_1,\alpha_2,\cdots,\alpha_n$ を添加した体は $K(\alpha_1,\alpha_2,\cdots,\alpha_n)$ と記す。体 L の部分集合 K が L における演算で体となるとき、K は L の部分体、L は K の拡大体といい、L/K と記す。$K(\alpha)$ は K の単純拡大といい、$K(\alpha)/K$ と記す。

例 8 $Q\left(\sqrt{2}\right)$ は Q の単純拡大、Q は $Q\left(\sqrt{2}\right)$ の部分体である。複素数体は実数体に $i=\sqrt{-1}$ を添加した拡大体である。

3.3 体の拡大と拡大次数

体 K と加法群 V において、K の元 a と V の元 x の積 ax が定義され、次の条件を満たすとき V を K 上のベクトル空間という。 $K\ni a,b$ $V\ni x,y$

$a(x+y)=ax+ay,(a+b)x=ax+bx.$
$(ab)x=a(bx),1x=x.$

$B=\{x_1,x_2,\cdots,x_n\}$ において、$\sum_{i=1}^{n}a_ix_i=0$ ならば $a_i=0$ が成り立つとき B は1次独立という。さらに、V の任意の元 x が1次結合 $\sum_{i=1}^{n}a_ix_i$ で表されるとき B は V の基底という。このとき、$a_i(i=1,2,\cdot\cdot,n)$ は一意的に定まる。基底は必ず存在する。また、その個数 n も一意的に決まる。n を V の次元という。

拡大 L/K において、体 L は体 K 上のベクトル空間になる。L が n 個の元からなる基底を持つとき K は n 次拡大という。n は拡大次数といい、$[L:K]$ と記す。

M が L の部分体で K の拡大体のとき、M は L と K の中間体という。このとき、$[L:\mathrm{M}][M:K]=[L:K]$ が成り立つ。

例9　$L=Q(\sqrt{2})$ は、加法、積が定義され Q 上のベクトル空間となる。$\sqrt{2}$ が無理数より $Q\ni a,b,a\cdot1+b\sqrt{2}=0\Rightarrow a=b=0.$

$\{1,\sqrt{2}\}$ は1次独立で L の基底となり、L の元は $a\cdot1+b\sqrt{2}$ と一意的に表される。$Q(\sqrt{2})$ は2次拡大で $[Q(\sqrt{2}):Q]=2.$

例10　$Q(\sqrt{2},\sqrt{3})$ の基底は $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ となる。その元は $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ と一意的に表される。これを確かめる。

$Q(\sqrt{2},\sqrt{3})=Q(\sqrt{2})(\sqrt{3})\ni x=y+z\sqrt{3}$ に対して

$y,z\in Q(\sqrt{2})$ だから、y,z は次のように書ける。$y=a+b\sqrt{2},z=c+d\sqrt{2}\quad a,b,c,d\in Q$

$$\therefore\ x=(a+b\sqrt{2})+(c+d\sqrt{2})\sqrt{3}$$
$$=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}.$$

一意性は次が成り立つことをいえばよい。
$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}=0\Rightarrow a=b=c=d=0$
もし $c=d=0$ でないとすると、式変形し
$\frac{a+b\sqrt{2}}{c+d\sqrt{2}}=-\sqrt{3}$　　左辺は $Q(\sqrt{2})$ の元だから、$\sqrt{3}\notin Q(\sqrt{2})$ となり矛盾する。よって $c=d=0$ となる。したがって、与式は $a+b\sqrt{2}=0$ となるが、これは例9で考察している。よって $a=b=0$ となる。

また、以下が成り立つことは明らか。

$$Q(\sqrt{2},\sqrt{3})\supset Q(\sqrt{2})\supset Q.$$
$$Q(\sqrt{2},\sqrt{3})\supset Q(\sqrt{3})\supset Q.$$
$$Q(\sqrt{2},\sqrt{3})\supset Q(\sqrt{6})\supset Q.$$

$Q(\sqrt{2}),Q(\sqrt{3}),Q(\sqrt{6})$ は $Q(\sqrt{2},\sqrt{3})$ と Q の中間体である。

4　Galois 拡大と Galois 群

4.1　Galois 拡大

有限次拡大 L/K が、体 K の元を係数とする重根のないある多項式 $F(x)$ のすべての根を K に添加した体（K と根を含む最小の体、$F(x)$ の最小分解体という。）であるとき K の Galois 拡大であるという。

このとき、Lの自己同型でKの元を動かさないもの全体は写像の合成で群となる。

これをLのGalois群といい$Gal(L/K)$と記す。

一般に、自己同型群Hの元で動かされないLの元の集合は部分体となりHによる固定体という。これをL^Hと記す。
$K = L^{Gal(L/K)}$となるのは明らかである。

また、$[L:K] = |Gal(L/K)|$が成り立つ。

例11　$Q(\sqrt{2})$はx^2-2のQ上の最小分解体で、QのGalois拡大となる。２つの根の置換から構成される自己同型写像を
$\sigma : Q \ni a \to a, \sqrt{2} \to -\sqrt{2}$とおく。

$G = \{e, \sigma\}$はGalois群となる。

例12　x^3-2の複素数の範囲の因数分解は

$$x^3-2 = \left(x-\sqrt[3]{2}\right)\left(x-\sqrt[3]{2}\omega\right)\left(x-\sqrt[3]{2}\omega^2\right)$$

となる。ただし、$\omega^2+\omega+1=0.$

$Q(\sqrt[3]{2}) = \left\{a+b\sqrt[3]{2}+c\sqrt[3]{2^2} \mid a,b,c \in Q\right\}$は、根$\sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$を含まないので$x^3-2$の最小分解体ではないから、Galois拡大ではない。

$Q(\sqrt[3]{2}, \omega)$はGalois拡大となる。Galois群は３つの根の置換で構成される自己同型全体であり、S_3と同型となる。

4.2　Galoisの基本定理

「有限次Galois拡大L/Kにおいて、LとKの中間体Mに対して、L/MはGalois拡大となり、$Gal(L/M)$は$Gal(L/K)$の部分群になる。逆に、$Gal(L/K)$の部分群Hに対して、Hによる固定体L^HはLとKの中間体になる。こうして、LとKの中間体とGalois群$Gal(L/K)$の部分群とが1:1に対応する（Galois対応という）。」

このとき、$[L:M] = |Gal(L/M)|$が成り立つ。

例13　$K = Q(\sqrt{2}, \sqrt{3})$は$Q$上で既約な２つの多項式$x^2-2, x^2-3$の最小分解体となり、Galois拡大となる。$K$の自己同型を

$\sigma_1 : Q(\sqrt{3}) \ni x \to x, \sqrt{2} \to -\sqrt{2}$
$\sigma_2 : Q(\sqrt{2}) \ni x \to x, \sqrt{3} \to -\sqrt{3}$
$\sigma_3 : Q(\sqrt{6}) \ni x \to x, \sqrt{2} \to -\sqrt{2}, \sqrt{3} \to -\sqrt{3}$
$e : K \ni x \to x$

で与えると、乗積表は表２となる。

V_4	e	σ_1	σ_2	σ_3
e	e	σ_1	σ_2	σ_3
σ_1	σ_1	e	σ_3	σ_2
σ_2	σ_2	σ_3	e	σ_1
σ_3	σ_3	σ_2	σ_1	e

表２　KのQ上のGalois群

表から、$G = \{e, \sigma_1, \sigma_2, \sigma_3\}$はAbel群になる。$\sigma_i$は$Q$の元を動かさないから、$G$は$Gal(K/Q)$となり、部分群$G_i = \{e, \sigma_i\}$を持つ。Galoisの基本定理にでてくる部分群$G_i$に対応する中間体$M_i$はどういう集合になるか考察する。

例えば、M_3を求める。$Q \ni a,b,c,d$として、$K \ni x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$に対して

$\sigma_3(x) = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}$となる。

$\sigma_3(x) = x$ から　$b = c = 0$ となる。

$$\therefore M_3 = Q\left(\sqrt{6}\right) = K^{G_3}$$

K / M_3はGalois拡大となり、G_3がGalois群になる。

同様にM_1, M_2についても

$$Gal\left(K / M_1\right) = Gal\left(K / Q\left(\sqrt{3}\right)\right) = G_1$$

$$Gal\left(K / M_2\right) = Gal\left(K / Q\left(\sqrt{2}\right)\right) = G_2$$

が成り立つ。

G_i, M_iのGalois対応を図２で示す。

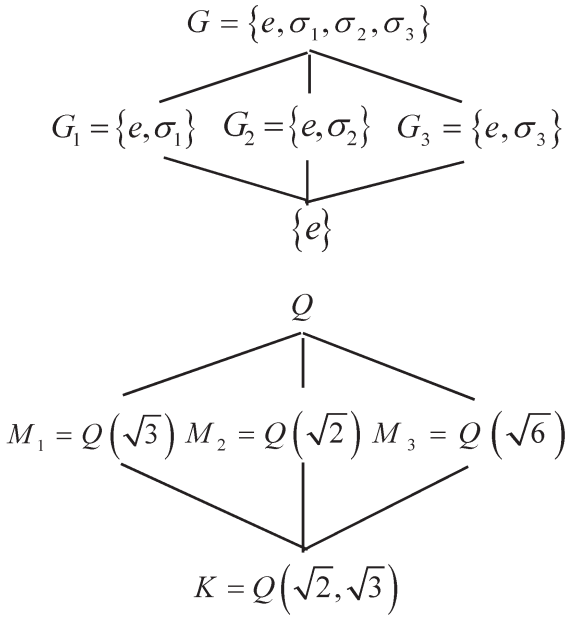

図２　中間体とGalois群のGalois対応

また、次式が成り立つ。

$$\left[K : M_i\right] = \left|G_i\right| = 2.$$

$$\left[K : Q\right] = \left|Gal\left(K / Q\right)\right| = 4.$$

５　代数方程式のGalois群

5.1 方程式のGalois群

L をK 上の重根を持たない多項式$F(x)$の最小分解体とするとき、L / KはGalois拡大となる。このとき、$Gal\left(L / K\right)$を方程式$F(x) = 0$のGalois群という。

例14　例11の$Gal\left(Q\left(\sqrt{2}\right) / Q\right) = \{e, \sigma\}$は方程式$x^2 - 2 = 0$のGalois群である。

5.2　冪根拡大、代数的に解ける

一般に、体L / Kに対して次のような拡大列があるときL / Kを冪根拡大という。

$$K \subset L_1 \subset L_2 \subset \cdots \subset L_r, L \subset L_r$$

$$L_i = L_{i-1}\left(\alpha_i\right), \alpha_i^{m_i} \in L_{i-1}\left(i = 1,2,\cdots,r\right)$$

L を体K 上の$F(x)$の最小分解体とし、L / Kが冪根拡大とする。このとき、$F(x)$のすべての根はK の元の有理演算と冪根で構成される。このとき、$F(x) = 0$は代数的に解けるという。

例15　例12で触れたように$Q\left(\sqrt[3]{2}, \omega\right)$は$x^3 - 2$ の最小分解体である。この冪根拡大は $Q \subset Q\left(\sqrt[3]{2}\right) \subset Q\left(\sqrt[3]{2}, \omega\right)$ となる。

よって、$x^3 - 2 = 0$ は代数的に解ける。

5.3　代数方程式の不可解性

5 次以上の一般の代数方程式が代数的に解けないことが次の命題 1 ～ 3 から分かる。

1　n 次代数方程式 $F(x)=0$ が代数的に解けるためには、$F(x)=0$ の Galois 群が可解群となることが必要十分である。

2　n 次代数方程式の Galois 群は、n 個の根のあらゆる置換から成り、対称群 S_n と同型である。

3　$n \geq 5$ のとき、n 次対称群 S_n は可解群ではない。

すなわち、一般の n 次代数方程式は、その Galois 群 S_n が $n \geq 5$ では可解群ではないことから、代数的に解けないことになる。

6　作図と体の拡大

作図では、定規は与えられた 2 点を通る線分（直線）を引き、コンパスは 1 点を中心とし与えられた点を通る円を描く。座標平面上で作図をし、初めに与えられた点の座標はすべて有理数とする。定規を使って求めた新たな点の座標は有理数係数の連立二元 1 次方程式の解であるから有理数である。そこで有理数体 Q を基礎体に選ぶ。コンパスを使って線分と円の交点、円と円の交点を求めた新たな座標は、二次方程式の解である。平方根が現れたときは Q に平方根を添加した体を考える。

例えば、交点 S の座標が $(1+\sqrt{11},-2-\sqrt{11})$ であれば、$\sqrt{11}$ を Q に添加した $Q(\sqrt{11})$ を考える。$Q \subset Q(\sqrt{11})$　$\left[Q(\sqrt{11}):Q\right]=2$ である。さらなる作図で交点の座標に $\sqrt{5}$ が現れれば $\sqrt{5}$ を添加した体 $Q(\sqrt{11},\sqrt{5})$ を考える。

$$Q \subset Q(\sqrt{11}) \subset Q(\sqrt{11},\sqrt{5})$$
$$\left[Q(\sqrt{11},\sqrt{5}):Q\right]=2\times 2=2^2$$

このように、作図によって生成する点の座標を表す数の集合を体の拡大で捉える。

有限回の作図により有理数体 Q に含まれない実数 $a_1,a_2,\cdots,a_n$ を添加した体の拡大次数は $\left[Q(a_1,a_2,\cdots,a_n):Q\right]=2^n$ となる。

例 16　正五角形の作図における体の拡大

直線 CP の方程式は $y=2x-2$　、円 P の方程式は $(x-1)^2+y^2=1$　となり、これを連立させて点 Q の座標を求める。これから $CQ=\sqrt{5}-1$ を得る。

次に、円 O 、円 C の二元二次方程式から点 F の座標を求める。

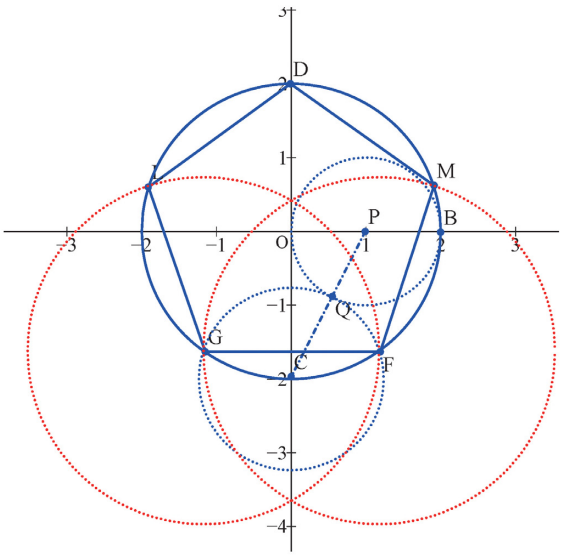

図 3　正五角形の作図

$O: x^2+y^2=4, \mathrm{C}: x^2+(y+2)^2=\left(\sqrt{5}-1\right)^2$.

これから $GF=\sqrt{10-2\sqrt{5}}$ を得る。

こうして、二次方程式を 2 回解いて拡大体 $Q\left(\sqrt{5},\sqrt{10-2\sqrt{5}}\right)$ を構成したことになる。

拡大次数は $2^2=4$ である。

7　円分多項式

7.1　1 の n 乗根、原始 n 乗根

複素数平面上の単位円に内接する正 n 角形を考える。各頂点は

$$\cos\frac{2\pi k}{n}+i\sin\frac{2\pi k}{n}\quad(k=0,1,2,\cdots,n-1)$$

で与えられる。

$\zeta_n=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$ とおく。

自然数 k に対して

$$\zeta_n{}^k=\cos\frac{2\pi k}{n}+i\sin\frac{2\pi k}{n}.$$

$$(\zeta_n{}^k)^n=\left(\cos\frac{2\pi k}{n}+i\sin\frac{2\pi k}{n}\right)^n$$

$$=\cos 2\pi k+i\sin 2\pi k=1$$

となる。

したがって、ζ_n^k は方程式 $x^n-1=0$ の根であり、これを 1 の n 乗根という。1 の n 乗根の作る集合 $\mu_n=\left\{1,\zeta_n,\zeta_n{}^2,\cdots,\zeta_n{}^{n-1}\right\}$ は、

ζ_n を生成元とする巡回群 $\mu_n=<\zeta_n>$ となる。このうち、n 乗して初めて 1 になる根を 1 の原始 n 乗根という。$\zeta_n{}^k$ が 1 の原始 n 乗根となるための必要十分条件は k,n が互いに素であることである。1 の原始 n 乗根は $\varphi(n)$ 個ある。p が素数のとき、1 の原始 p 乗根は $\Phi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1$ の根である。この多項式の次数は $\varphi(p)=p-1$ となる。

例 17　1 の原始 3 乗根は次の 2 つの根である。$\Phi_3(x)=x^2+x+1$.

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

$$\zeta_3^2=\cos\frac{4\pi}{3}+i\sin\frac{4\pi}{3}=\frac{-1-\sqrt{3}i}{2}$$

このとき、$\varphi(3)=2$

7.2　円分多項式

多項式 $\Phi_p(x)$ は、p 次の円(周等)分多項式という。p が素数のとき、これは有理数体 Q 上で既約である。すなわち Q でこれ以上因数分解できない。これを確かめるには $\Phi_p(x+1)$ の既約性がいえれば十分である。多項式の既約性の判定には次の定理を使う。

「p が素数のとき、整数係数の多項式において、最高次の項の係数は p の倍数でなく、それ以外の項の係数は p の倍数で、定数項は p の倍数だが p^2 の倍数でないとき、この多項式は Q で既約である（Eisenstein の判定基準)」

$$\Phi_p(x+1)=\frac{(x+1)^p-1}{(x+1)-1}=x^{p-1}+px^{p-2}+\cdots+p.$$

上式で最高次の項以外の項の係数は素数 p の倍数だが、定数項は p^2 の倍数とならない。したがって、Eisenstein の判定基準から

上式は既約となる。

$\Phi_p(x)$ を複素数の範囲で因数分解すると、

$$\Phi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1 \\ =\left(x-\zeta_p\right)\left(x-\zeta_p{}^2\right)\cdots\left(x-\zeta_p{}^{p-1}\right). \quad \cdots①$$

$p=7$ のときは次式となる。

$$\Phi_7(x)=x^6+x^5+\cdots+x+1 \\ =\left(x-\zeta_7\right)\left(x-\zeta_7^2\right)\cdots\left(x-\zeta_7^6\right).$$

7.3 円分体

ζ_p を 1 の原始 p 乗根とするとき、$Q\left(\zeta_p\right)$ は Q 上の円分体という。これは x^p-1 の最小分解体となるから、Q の Galois 拡大である。この Galois 群は **10.2** で示すように法 p の既約剰余類群と同型になる。

また、$\left[Q\left(\zeta_p\right):Q\right]=\varphi(p)$ となる。これは、円分多項式 Φ_p の次数 $\varphi(p)$ が $Q\left(\zeta_p\right)$ の拡大次数と等しいことを意味する。

なお、$Q\left(\zeta_p\right)$ の元は $a_0+a_1\zeta_p+\cdots+a_{p-1}\zeta_p^{p-1}$, $a_i\in Q$ と一意的に表される。

$p=7$ のとき $\left[Q\left(\zeta_7\right):Q\right]=\varphi(7)=6$ となる。

8　正 7 角形の作図不能性

8.1 作図可能性の必要条件

1 で述べた $n=2^p3^q5^r$ を一般化した式 $n=2^e p_1{}^{e_1}p_2{}^{e_2}\cdots p_m{}^{e_m}$（$p_i$ は 2 以外の素数、$i=1,2,\cdots,m$）を考える。

$$\varphi(n)=\varphi\left(2^e\right)\varphi\left(p_1^{e_1}\right)\cdots\varphi\left(p_m^{e_m}\right) \\ =\left(2^e-2^{e-1}\right)\cdots\left(p_m{}^{e_m}-p_m{}^{e_m-1}\right) \\ =2^{e-1}p_1{}^{e_1-1}\cdots p_m{}^{e_{m-1}}\left(p_1-1\right)\cdots\left(p_m-1\right).$$

この式変形では p,q が素数のとき

$$\varphi(pq)=\varphi(p)\varphi(q),\varphi\left(p^e\right)=p^{e-1}(p-1)$$

が成り立つことを使っている。

$\varphi(n)$ が 2 の冪となるのは、$p_i=2^{n_i}+1$ が異なる Fermat 素数(現在、見つかっている Fermat 素数は 3,5,17,257,65537)であって、$e_i=1$ となることである。このとき

$$n=2^e p_1p_2\cdots p_m,\varphi(n)=2^{e-1+r_1+r_2+\cdots+r_m} \quad \cdot\cdot②$$

が成り立つ。これが円周の n 等分可能な必要条件である。　以上をまとめると、

「正 n 角形が作図可能

$\Rightarrow \left[Q\left(\zeta_n\right):Q\right]=\varphi(n)$ が 2 の冪乗

$\Leftrightarrow$　②が成り立つ」

この対偶を取れば、次のようになる。

「$\varphi(n)\neq 2^r$　$\Rightarrow$　正 n 角形は作図不能」

8.2　正 7 角形の作図と体の拡大

$n=7$ のとき、$\varphi(7)=6$ で 2 の冪ではないから **8.1** で述べたことより作図不能がいえるが、その原因を体の拡大で探ってみる。

複素数平面上の単位円 O に内接する正 7 角形を作図するため、**7.1** で述べた ζ_7 の実部 $\alpha=\cos\dfrac{2\pi}{7}$ が作図できれば、数 $\sin\dfrac{2\pi}{7}$ は式 $\sin\dfrac{2\pi}{7}=\sqrt{1-\alpha^2}$ を用いれば作図でき

る。そこでαの作図を考える。その作図で扱う数は$Q(\alpha)$に含まれるから、正7角形の作図のプロセスは有理数体Qから円分体$Q(\alpha)$への体の拡大となる。

$Q(\alpha)/Q$の拡大次数を求める。ζ_7を根に持つ$Q(\alpha)$上の既約多項式は

$$\zeta_7+\zeta_7^{-1}=2\alpha,\zeta_7\zeta_7^{-1}=1$$

なので $x^2-2\alpha x+1$ である。

$$\therefore\left[Q(\zeta_7):Q(\alpha)\right]=2.$$

これは、2次の拡大である。

他方、$Q\subset Q(\alpha)\subset Q(\zeta_7)$だから

$$\left[Q(\zeta_7):Q\right]=\left[Q(\zeta_7):Q(\alpha)\right]\left[Q(\alpha):Q\right]$$

が成り立つ。**7.3**で述べたことから

$\left[Q(\zeta_7):Q\right]=\varphi(7)=6$ なので、

$$\left[Q(\alpha):Q\right]=\frac{\varphi(7)}{2}=3.$$

すなわち、3次の拡大となる。3は2の冪乗ではないからαの作図は不能となる。以上から 3 次の拡大が作図不能の原因であることが分かった。

8.3　正7角形の作図と方程式

8.2で述べた体の拡大を、具体的な方程式で探ってみる。$\zeta_7=\zeta$とおく。

$\eta_1=\zeta+\zeta^6,\eta_2=\zeta^2+\zeta^5,\eta_3=\zeta^3+\zeta^4$

という式（Gaussの2項周期）を使えば、

$\{\zeta,\zeta^6\},\{\zeta^2,\zeta^5\},\{\zeta^3,\zeta^4\}$ はそれぞれ二次方程式 $t^2-\eta_i t+1=0\quad(i=1,2,3)$ の解となる。さらに$\eta_i\,(i=1,2,3)$ には

$$\eta_1+\eta_2+\eta_3=-1,$$
$$\eta_1\eta_2+\eta_2\eta_3+\eta_3\eta_1=-2$$
$$\eta_1\eta_2\eta_3=1$$

が成り立つことが確かめられるから

η_1,η_2,η_3は次の三次方程式の異なる解である。　$t^3+t^2-2t-1=0.$

したがって、正7角形の作図とは、Qに三次方程式、二次方程式の解を添加して3次、2次の体の拡大を構成し$Q(\zeta_7)$に至ることが分かる。

なお、η_1,η_2,η_3の値を求めると次式となる。

$$\eta_1=2\cos\frac{2\pi}{7}>0,\eta_2=2\cos\frac{4\pi}{7}<0$$

$$\eta_3=2\cos\frac{6\pi}{7}<0.$$

9　他の作図問題

9.1 角の3等分問題

一般の角が与えられたとき、これを3等分する問題が角の3等分問題である。

複素数平面において、単位円周上の点$A(\cos3\theta+i\sin3\theta)$が与えられたとき、3等分線との交点$B(\cos\theta+i\sin\theta)$を作図するには点Bの$x$座標が作図できればよい。

$x=\cos\theta,a=\cos3\theta$ とおくと、

$\cos3\theta=4\cos^3\theta-3\cos\theta$ の公式を利用すれば $4x^3-3x-a=0$ が成り立つ。例えば、

$a=\frac{3}{5}$となる角θを考えるとすれば方程式

$20x^3-15x-3=0$ を得る。左辺の多項式はEisensteinの判定基準からQ上で既約であ

る。その根をαとすれば$\left[Q(\alpha):Q\right]=3$となり、2の冪になっていないので$\cos\theta$は作図不能である。これがこの問題の反例となるから、一般の角の3等分は作図不能となる。

9.2 立方体倍積問題

デロス島の人々が疫病絶滅の祈願をしたとき、祭壇の大きさを2倍にせよと命じる神託が降った。これは$\sqrt[3]{2}$の作図であり当時の数学者たちを悩ませた。問題は、x^3-2を満たす根を作図することである。例11で述べたようにこの多項式はQ上で既約である。

作図には体の拡大$Q\left(\sqrt[3]{2}\right)$が必要となるが、

$\left[Q\left(\sqrt[3]{2}\right):Q\right]=3$となり2の冪でないため作図不可能である。

１０　作図問題と Galois 理論

8.1の条件②の十分性が証明できれば、

$\varphi(n)=2^r$から数ζ_nが作図可能となる。

例えば、$n=17$のときは$\varphi(17)=16=2^4$

なので正17角形の作図可能性がいえる。

Gaussは、1のp乗根(p:Fermat素数)が開平のみで求められることを二次方程式の構成によって証明した（高木,1931)。

ここでは、Gauss以後に発展したGalois理論を用いた証明を与える。Galois拡大においては、Galoisの基本定理からGalois対応する中間体とGalois群の関係が使える。

そこで次の命題の証明を考える。

「p が Fermat 素数ならば、正p角形は作図可能である」

7.3 により円分体$K=Q(\zeta_p)$はGalois拡大である。

次のようなKの自己同型を定義する。

$$\sigma_m : Q \ni a \to a, \zeta_p \to \zeta_p^m, m \in Z.$$

この全体はKのGalois群となる。この群を$Gal(K/Q)$とおく。この群から$F_p^{\times}$への次のような写像ψを考える。

$$\psi : Gal(K/\mathrm{Q}) \ni \sigma_m \to \overline{m} \in F_p^{\times}.$$

$\psi(\sigma_m)=\overline{m}$は一意的に決まる。

$$(\sigma_m\sigma_n)(\zeta_p)=\sigma_m\left(\sigma_n(\zeta_p)\right)=\sigma_m\left(\zeta_p^n\right)$$
$$=\left(\sigma_m(\zeta_p)\right)^n=\left(\zeta_p^m\right)^n=\zeta_p^{mn}.$$
$$\therefore \psi(\sigma_m\sigma_n)=\overline{mn}=\overline{m}\,\overline{n}=\psi(\sigma_m)\psi(\sigma_n).$$

$\psi(\sigma_m)=\psi(\sigma_n)$ ならば $\overline{m}=\overline{n}$ $\therefore \sigma_m=\sigma_n$

ψは1：1で、上への対応は明らかとなるから同型となる。$\therefore Gal(K/Q)\cong F_p^{\times}$.
すなわち、円分体のGalois群は法pの既約剰余類群と同型になる。

$F_p^{\times}$は位数$p-1$のAbel群だから、

$Gal(K/Q)$も位数$p-1$のAbel群となる。

仮定から$p-1=2^r$より$Gal(K/Q)$の位数は2^rとなる。

ところで、有限Abel群は、その位数の任意の約数を位数とする部分群をもつ。

よって、$Gal(K/Q)$は位数2^{r-1}の部分群

H_1をもつ。このとき $(Gal(K/Q):H_1)=2.$

$r>1$ ならば、同様に群 H_1 の部分群 H_2 で

$H_2 \subset H_1,\ (H_1 : H_2) = 2$ となるものがある。これを繰り返し続けていくと、部分群 H_i $(i = 1, 2, \cdots, r)$ の列ができる。

$$H_1 \supset H_2 \supset \cdots \supset H_r = \{e\}, (H_{i-1} : H_i) = 2.$$

これに対応する H_i の固定体を

$K_i = K^{H_i} = \{x \mid x^\sigma = x, \sigma \in H_i\}$ とおく。

K/Q に Galois の基本定理を適用すると、次の中間体の列が生成される。

$$Q \subset K_1 \subset K_2 \subset \cdots K_r = K.$$
$$[K_i : K_{i-1}] = (H_{i-1} : H_i) = 2.$$

よって、Q から K への 2 次拡大の列を得るから、作図可能となる。□

１１　折り紙による作画

11.1　折り紙による３次方程式の解法

折り紙の操作で任意の三次方程式の解が求められる(Geretschlager,2008)。すなわち、一般に $a > 0, d \neq 0$ のとき次の２つの放物線 C_1, C_2 の共通接線の傾き t は、三次方程式①の解となる。これを確かめる。

$$ax^3 + bx^2 + cx + d = 0 \quad \cdots ①$$

$$C_1 : 4d(x+b) = (y-c)^2, C_2 : 4ay = x^2.$$

共通接線と C_1, C_2 の接点の座標をそれぞれ $(p, q), (r, s)$ とおくと次式が成り立つ。

$$s - q = t(r - p).$$
$$4d(p+b) = (q-c)^2, 4as = r^2.$$

C_1, C_2 を x で微分し $t = \dfrac{2d}{(q-c)} = \dfrac{r}{2a} \neq 0$ を得る。これから　$q - c = \dfrac{2d}{t}, a = \dfrac{r}{2t},$

$$b = -p + \frac{(q-c)^2}{4d} = -p + \frac{d}{t^2}, c = q - \frac{2d}{t}.$$

$a = \dfrac{r^2}{4s} = \dfrac{r}{2t}$ だから $2s = tr$ となる。

$s - tr = q - pt$ より $q + s - pt = 0$ となる。

よって、次に示すように t は①の解となる。

$$at^3 + bt^2 + ct + d$$
$$= \frac{r}{2t} \cdot t^3 + \left(\frac{d}{t^2} - p\right)t^2 + \left(q - \frac{2d}{t}\right)t + d$$
$$= \left(\frac{r}{2} - p\right)t^2 + qt = t(q + s - pt) = 0.$$

正７角形を“折る”ためには、**8.3** で述べた η_1 を２つの放物線の共通接線の傾きとして求めればよい。

11.2　正７角形の折り紙作画

図４で点 $A(-2, -1), B(0, 2)$ をそれぞれ y 軸上と x 軸上に同時に乗るように折り返す。それぞれの点を U, T とする。このときできる折れ線 l は点Ａが焦点で y 軸を準線とする放物線 C_1 と点Ｂが焦点で x 軸を準線とする放物線 C_2 の共通接線となることは容易にわかる。

$l, \mathrm{C}_1, \mathrm{C}_2$ の方程式を次のようにする。

$$l : y = tx + m$$
$$C_1 : -4(x+1) = (y+1)^2$$
$$C_2 : 4(y-1) = x^2.$$

l, C_1 の接点 (x_1, y_1) で l の傾き t を考えると

$$t = \frac{-2}{y_1 + 1}. \therefore x_1 = -1 - \frac{1}{t^2}, y_1 = -1 - \frac{2}{t}.$$

l, C_2 の接点 (x_2, y_2) で l の傾き t を考えると

$t = \frac{x_2}{2}$.　$\therefore\ x_2 = 2t, y_2 = t^2 + 1$.

$m = y_1 - tx_1 = t - \frac{1}{t} - 1, m = y_2 - tx_2 = 1 - t^2$.

これから、$t^3 + t^2 - 2t - 1 = 0$ を得る。
この正の解を η_1 とおく。共通接線 l は
$y = \eta_1 x + 1 - \eta_1^2$ となる。l と x 軸との交点 D の x 座標は $x = \eta_1 - \frac{1}{\eta_1}$.　点 $(-4, 0)$ と点 D の中点の座標は $\left(\frac{\eta_1}{2} - \frac{1}{2\eta_1} - 2, 0\right)$ となる。

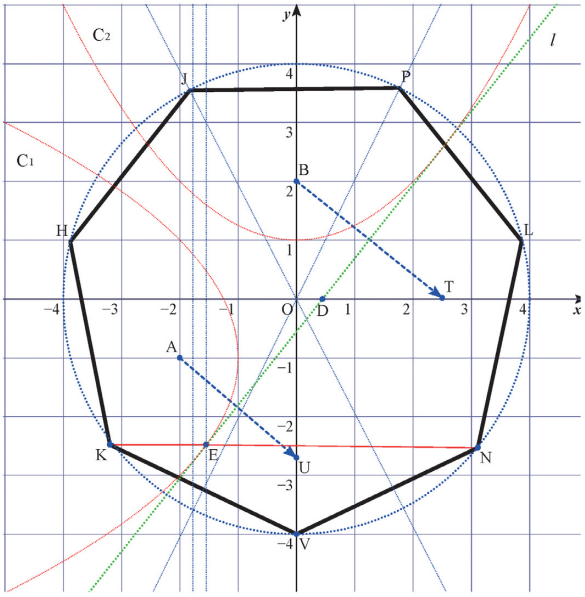

図 4　正 7 角形の折り紙による作画

さらに、この中点に関して点 $(-2, 0)$ を折り返した点の座標は $\left(\eta_1 - \frac{1}{\eta_1} - 2, 0\right)$ となる。
直線 $x = \eta_1 - \frac{1}{\eta_1} - 2$ と共通接線 l の交点を点 E とする。この点の y 座標は $-2\eta_1$ となる。

$-2\eta_1 = -4\cos\frac{2\pi}{7}, OU = 4\cos\frac{2\pi}{7}$.

これから点 K, N が決まり、正 7 角形が描画できる。実際の作画は図 5 となる。

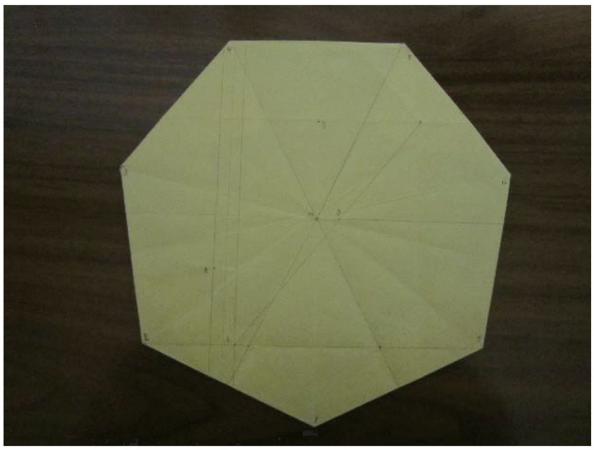

図 5 折り紙作画による正 7 角形

11.3　角の 3 等分線の折り紙作画

折り紙の操作で任意の角の 3 等分線が引ける（阿部,2003）。**9.1** で述べたことから $t = \cos\theta$ とおけば $4t^3 - 3t - \cos 3\theta = 0$ となる。11. 1 で述べたように、任意の三次方程式の解は折紙で求められる。角の 3 等分の数学的議論は計算が複雑になるので割愛する。

折り紙操作と証明は次の通りとなる。

図 6 で、$\angle TOB$ が与えられた任意の角とする。$\angle FOB = 90^0$，G は FO の中点、G で OB に平行な線分 l を引く。

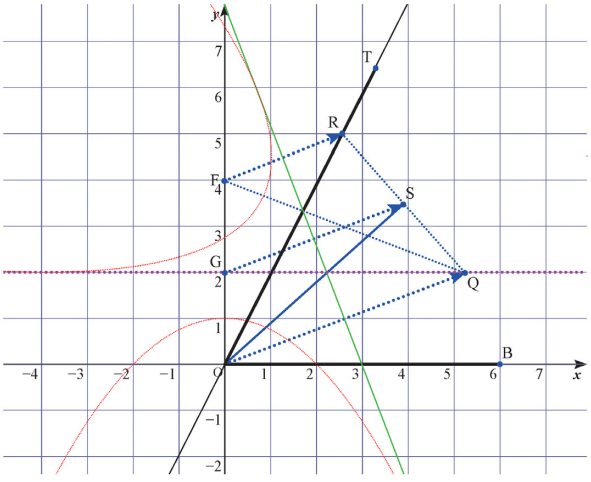

図 6　任意の角の三等分の作画

次に、点 F,O を緑線を折れ線として折りそれぞれ TO,l 上に同時にくるように重ねる。それらを、それぞれ点 R,Q とする。点 G は線分 RQ 上にくる。この点を S とする。

$FG=OG, FO\perp GQ$ より ΔQOF は二等辺三角形となる。$FR//GS, GS//OQ$ から

$RS=SQ, \angle OSQ=90^0$ だから ΔOQR も二等辺三角形となる。

したがって、$\angle ROS$ と $\angle QOS$ は等しい。また、$\angle QOS=\angle GQO$、

$GQ//OB$ より $\angle GQO=\angle QOB$　よって、線分 OS,OQ は $\angle TOB$ の 3 等分線になる。

実際の作画を図７に示す。

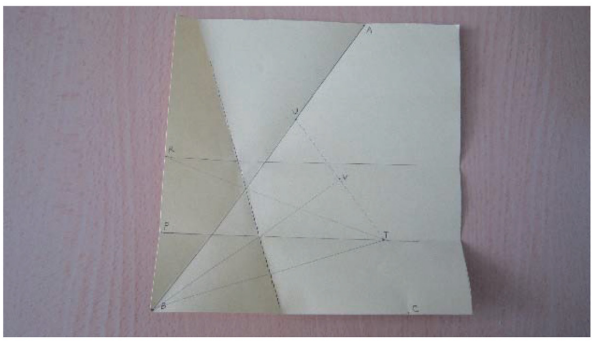

図７　折り紙作画による角の三等分

12　おわりに

高校数学の代数的な教材の単元は、「数と式」（数学Ⅰ）、「いろいろな式」（数学Ⅱ）、「整数の性質」（数学A）、「複素数平面」（数学Ⅲ）であるが、「いろいろな式」では高次方程式が、また「複素数平面」では１の n 乗根が扱われている。したがって、これらの高校代数にひき続く発展的な代数学を大学で学ばせる教材が必要となる。

本稿の教材は、幾何学的作図問題を発端にして、作図可能性を数学的に考察するものである。そのため、群、体、体の拡大、Galois 拡大、Galois 群、Galois の基本定理などの入門程度の知識を確認し、作図問題と体の関連や正７角形の作図不能、正多角形が作図可能な条件へと歩を進める。こうして、Galois 理論を頂点とする代数学のいろいろな概念と体系を概観できることになる。

数学に十分慣れていない学生も対象とするためいくつかの重要な定理や命題の煩雑な証明は避けている。その代り、概念理解のための例を多く提示するとともに、全体の概念構成の流れを重視した。数学の本質は証明にあるから証明を抜くことには異論があるかもしれないが、こういう学び方があっていいのではないかと考えられる。丁度、“微分積分は二度学ぶ。一度目は計算・応用の馴れ重視で学び、二度目は精密で体系的な概念構成を重視して学ぶ” 方式と似ている。本稿での命題や定理の証明に興味を持った学生には参考文献に当って本格的に学習するようになればよいと考える。

著者は、学生時代に恩師服部昭先生の整数論の講義で Galois 理論を学んだが、体論の separable,splitting field,normal extention などの概念を積み上げていく箇所は恥ずかしながら十分には理解できなかった。しかし、高校数学の教材研究で作図問題を考察するうち *Galois* 理論に目覚め、勉強し直すことになった。丁度、服部先生の御本がでた頃である。こうした経験から、数学の学習には初めから抽象的な内容に挑戦するよりも特殊な問題で十分イメージアップを図ったのちに、一般的な理論へと歩を進める「特殊から一般へ」は理解の早道であると考えている。

参考文献

[1]阿部恒(2003):すごいぞ折り紙-折り紙の発想で幾何を楽しむ、日本評論社
[2]稲葉栄次(1958):整数論,基礎数学講座、共立出版
[3]彌永・布川(1968):代数学,現代数学演習叢書、岩波書店
[4]彌永健一(1979):ガロア理論とは,代数学への招待、数学セミナー増刊,日本評論社
[5]R.Geretschlager(2008):折紙の数学-ユークリッドの作図法を超えて-,森北出版
[6]高木貞治(1931):初等整数論講義,共立出版
[7]服部昭(1975):初等ガロア理論,宝文館出版
[8]J.B.FRALEIGH(1971):A FIRST COURSE IN ABSTRACT ALGEBRA, ADDISON-WESLEY PUBLISHING CO.
[9]S.Lang(1970):ALGEBRA,ADDISON-WESLEY PUBLISHING CO.