平成８年度　学位論文

作図問題について

― 古代ギリシャの３大作図不能問題 ―

兵庫教育大学大学院　学校教育研究科
教科・領域教育専攻　自然系コース
Ｍ９５５５２Ｄ　　井上　正雄

作図問題について —— 古代ギリシャの３大作図不能問題 ——

【目　　次】

序文

Platon によれば、完全な幾何学的図形とは直線と円だけということである。古代ギリシャの幾何学は、この信念のため幾何学的作図を行う際に用いることのできる道具を定木とコンパスだけに限定していた。ここでいう定木とは、目盛りのついていない、ただ１本のまっすぐな縁をもったもののことであった。

これら２つの道具だけを用いて、広い範囲の作図を行うことができる。しかし、幾何学的概念の中には、直観的には作図可能であるべきはずなのに、定木とコンパスだけでは不十分なものがたくさんある。その中に、ギリシャの人々ができなかった有名な３つの作図問題がある。

立方体倍積問題，円積問題，角の３等分問題がそれである。

ギリシャの人々が、これらの作図問題が非常にむずかしいと悟ったのも無理もない。これらの作図は不可能なのである。しかし、彼らは不可能であることを示す方法ももたなかったし、また解が存在しないのではないかという疑念ももたなかったように思われる。そのため、彼らはそれを解こうとして、実りのない研究にかなりの才能を浪費する結果となった。

後に、これらの問題は”古代ギリシャの３大作図不能問題”と呼ばれるようになった。

そして、長い年月を経て、１９世紀に入ってようやくこれらの未解決問題は「作図することはできない」という否定的な形で証明されることになるわけである。

円の等分問題は、角の３等分問題が証明されたころ（*1837*年）より４０年位前、ガウスによって解決されている。当時１９歳で、ゲッチンゲン大学の学生だった彼は、古代語をやるべきか、数学を選ぶべきか、決心が定まらないでいたが、この問題の解決により、喜んで数学を専門に選んだといわれている。

次に本論文の構成を述べる。

第１章では、幾何学的作図において、これから幾つかの作図問題を考えていく上で重要になってくる”作図できる数”について述べた。

第１節では、幾何学的作図における定木とコンパスの使い方の定義と基本的な作図について述べた。

第２節では、与えられた２点から出発して、定木とコンパスにより、どのような点が作図可能であるかということについて調べた。また、作図できる数と数体との関係、拡大体の定義、数体の系列等、第２章以降で取り扱う作図問題を証明していくのに必要とされる作図の基本的概念について述べた。

第２章，３章，４章では、”古代ギリシャの３大作図不能問題”について取り扱った。

第２章では、その中の１つ、倍積問題について考察した。

第１節で、倍積問題の由来について触れ、第２節で､作図不可能性を証明していくわけだが､結局は、$\sqrt[3]{2}$が作図できる数ではないということで解決した。

第３章では、円積問題について考察した。

第１節では、円積問題の由来について触れ、また、代数的数の定義、作図できる数と代数的数との関係について述べた。

第２節では、まず、あとの証明に必要となってくる基本対称式に関する定義、性質について述べ、そこから円積問題を証明していくわけだが、結局はπが超越数であることですべてが解決するものであった。

第４章では、角の３等分問題について考察した。

第１節では、角の３等分問題の由来について触れた。

第２節では、角の３等分問題が、”一般には作図不可能である”ことを証明するための例として、まず、$\theta = 60^\circ$の場合を取り上げ、その後、θの値による作図の可能・不可能の判定基準を付け加えることによって、それに幅をもたせた。

第５章では、正多角形の作図に関連した円の等分問題について取り扱った。

第１節では、円の等分問題を考えるときに基盤となる分円方程式について述べた。

第２節では、正多角形の例として、正５角形と正７角形を取り上げ、その作図可能性について調べた。

第３節では、合同記号について触れた後、方程式の既約性を調べるのに使われる *Eisen-stein* の定理、正多角形の作図と大きく関係している *Fermat* 素数について述べた。また、正ｎ角形が作図できるためのｎの条件について調べ、定理の形にまとめた。

最後に、日頃より懇切にご指導いただいた渡辺金治先生に、この場をかりて深謝の意を表します。また、修士課程在学中にお世話になりました諸先生方に、心より感謝します。

第１章　作図

第１節　作図とは

古代ギリシャからの伝統の中に、与えられた条件を満足する図形を作図するのに、用具を定木とコンパスに限るという約束事があった。

これから述べていく”作図”とは、すべて、道具として定木とコンパスのみを用いて、描いていくものである。

まず、定木とコンパスの使い方を定義する。

定義１．１．　定木とコンパスは、以下の用い方のみ使用可能とする。

［１］「定木」は、与えられた２点を通る直線を、描くことができる。

［２］「コンパス」は、与えられた点を中心として、与えられた長さを半径とする円を描くことができる。

つまり、許された作図は次の通りである。

（ｉ）与えられた２点を通る直線を描くこと

（ii）与えられた点を中心として、与えられた半径の円を描くこと

（iii）２直線の交点を定めること

（iv）直線と円の交点を定めること

（ｖ）２つの円の交点を定めること

（vi）与えられた２点にコンパスの針をあて、その距離を変えずに他の位置へ移すこと

以下、本論文においては、次のものを作図可能であるとして議論を進めていく。

（ｉ）与えられた線分ＡＢの垂直２等分線を描くこと。
（ii）与えられた任意の角の２等分線を描くこと。
（iii）直線ｌと点Ｐが与えられているとき、Ｐを通り、ｌに垂直な線を描くこと。
（iv）直線ｌとｌ上にない点Ｐが与えられているとき、Ｐを通りｌに平行な線を描くこと。
（ｖ）与えられた、同一直線上にない、３点Ａ，Ｂ，Ｃを通る円を描くこと。
（vi）円Ｏと円外の点Ｐが与えられているとき、Ｐより円Ｏへの接線を描くこと。

このような厳格な条件は、*Platon* の主張するところより始まる。幾何学の作図では、直線・円以外を用いるべきではないという主張である。

尚、第２節で取り扱う諸命題の証明は、『数学への誘い』，羽鳥　裕久著，培風館、『不可能の証明』、津田　丈夫著、共立出版社を参考にさせていただいた。

第２節　作図できる数全体

作図問題では、ｘｙ平面上にαを１つの正数として、２点（０，０），（α，０）が与えられている状態から出発する。そこから、定木とコンパスのみを用いて、一体どのような数が作図できるかをこれから調べていくことにする。

本論文においては、点（ａ，０）が作図できることを”ａという数が作図できる”と表現する。もし、点（ａ，ｂ）が作図できたのなら、ｘ座標、ｙ座標の両方が作図できるので”ａ，ｂという数が作図できる”と表現するわけである。

また、複素数ａ＋ｂｉが作図できるとは、複素平面をｘｙ平面と同一視させて考えて、点（ａ，ｂ）が作図できることを意味する。

定義１．２．　ｘ，ｙ平面において、２点（０，０），（α，０）から出発して、定木とコンパスを有限回用いて作図できる数全体の集合を、複素数体Ｃの部分集合と考えて、F_αと表す。

$F_\alpha = \{0, \alpha, \cdots\cdots\}$

まず、原点から出発して、ｘ軸の正の方向に、コンパスによってαずつ区切っていくことによって、αａ（ａは自然数）という数が作図できる。同様にｘ軸の負の方向に区切っていくことによって作図できる数はαａ（ａは整数）と拡張される。

ここで、数体について少し触れておく。

複素数体Ｃの部分集合Ｋ（Ｋは空でない）の任意の元ａ，ｂに対して、ａ±ｂ∈Ｋ，ａｂ∈Ｋ、ａ／ｂ∈Ｋ（ただしｂ≠０）であるとき集合Ｋを数体であるという。

今後、本論文中に出てくる記号Ｑ，Ｒ，Ｃは、有理数全体からなる集合，実数全体からなる集合，複素数全体からなる集合を意味し、それぞれ有理数体，実数体，複素数体を表すものとする。

命題１．３．　αａ，αｂがF_αの元ならば、α（ａ±ｂ），α（ａｂ），α（ａ／ｂ）もF_αの元である。ただし、ｂ≠０とする。

［証明］ａ，ｂをつぎの３つの場合に分けて証明する。

（ｉ）ａ，ｂ＞０のとき（ａ≧ｂとして考える）

次の図１，２，３よりα（ａ±ｂ），αａｂ，α（ａ／ｂ）はＦ$_{\alpha}$の元であることがわかる。

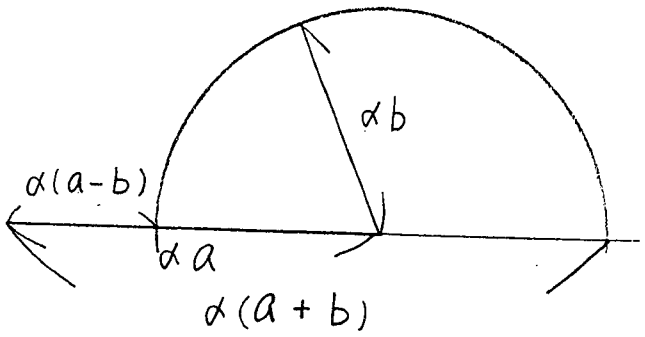

図１

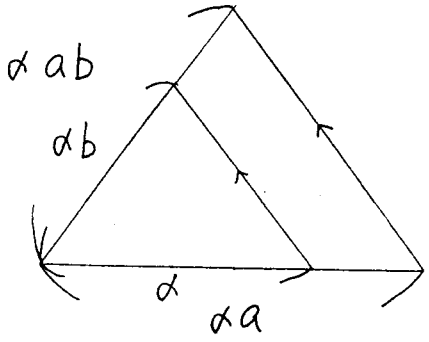

図２

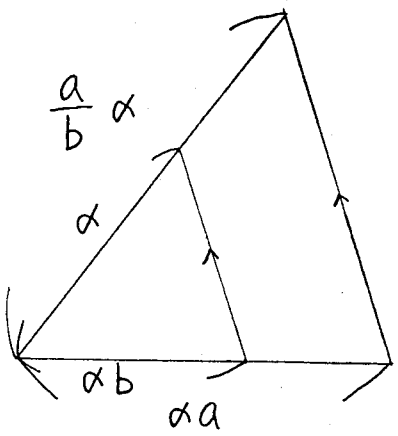

図３

（ii）ａ，ｂ∈Ｒのとき

（ｉ）の場合を除くａｂ＜０、又はａ，ｂ＜０のときを考えればよい。

これらの数の演算α（ａ±ｂ）の結果は、次のいずれかになる。

α（|ａ|±|ｂ|），$-\alpha$（|ａ|±|ｂ|）

αａ∈Ｆ$_{\alpha}$のとき、$-\alpha$ａ∈Ｆ$_{\alpha}$は明らかなので、これらはすべてＦ$_{\alpha}$の元であることがわかる。

また

α（ａｂ）＝$\pm\alpha|a||b|\in F_\alpha$　　α

（ａ／ｂ）＝$\pm\alpha$（$|a|/|b|$）$\in F_\alpha$

である。

（iii）ａ，ｂ∈Ｃのとき

ａ＝$a_1+a_2 i$，ｂ＝$b_1+b_2 i$（a_1，a_2，b_1，$b_2\in R$）とおくと

α（ａ±ｂ）＝$\alpha\{(a_1\pm b_1)+(a_2\pm b_2)\,i\}$

となる。

ここで、$\alpha a\in F_\alpha \Leftrightarrow \alpha a_1$，$\alpha a_2\in F_\alpha$である。

（ii）より$\alpha(a_1\pm b_1)$，$\alpha(a_2\pm b_2)\in F_\alpha$なので、$\alpha$（ａ±ｂ）$\in F_\alpha$となる。

また

$\alpha ab=\alpha\{(a_1b_1-a_2b_2)+(a_1b_2-a_2b_1)\,i\}\in F_\alpha$

$$\alpha\left(\frac{a}{b}\right)=\alpha\left(\frac{a_1b_1+a_2b_2}{b_1^2+b_2^2}+\frac{a_2b_1-a_1b_2}{b_1^2+b_2^2}\,i\right)\in F_\alpha$$

も（ii）より導き出すことができる。

したがって、F_αのすべての元をαで割った集合（１／α）F_αは数体である。

０でない元を含む数体として、最小のものは、有理数体Ｑなので、F_αはαのＱ倍の元をすべて含む集合である。

よって、作図できる数は、αa（ａは有理数）と拡張される。

命題１．４．　αaがF_αの元ならば$\alpha\sqrt{a}$もF_αの元である。

［証明］命題１，３と同様に３つの場合に分けて考えていく。

（ｉ）ａ＞０のとき

図４のように、直径が（ａ＋１）である円を描き、αaとαの間に垂線を立て、左右２つの直角３角形を作ると、これらは相似になるので、対応する辺の比から、

$\alpha a : x = x : \alpha$

ｘ＞０より、$x=\alpha\sqrt{a}$

よって、$\alpha\sqrt{a}\in F_\alpha$となる。

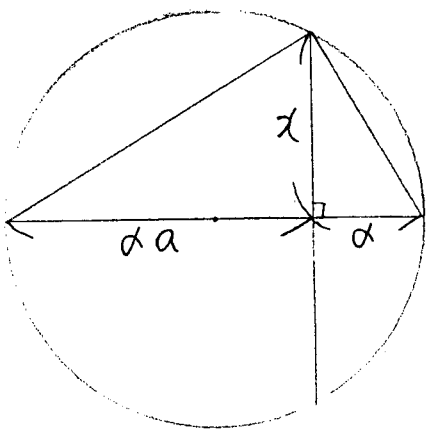

図４

（ii）ａ∈Ｒのとき

$a<0$の場合を考えればよいので、$\alpha\sqrt{a}=i\alpha\sqrt{|a|}$となる。

$i\in F_\alpha$、（i）より$\alpha\sqrt{|a|}\in F_\alpha$なので、命題１．３を用いると$i\alpha\sqrt{|a|}\in F_\alpha$が得られる。

よって、$\alpha\sqrt{a}\in F_\alpha$となる。

（iii）$a\in C$のとき

$a=a_1+a_2 i$（a_1, $a_2\in R$）とおく。

複素平面における図５より、$\alpha\sqrt{a}\in F_\alpha$がわかる。

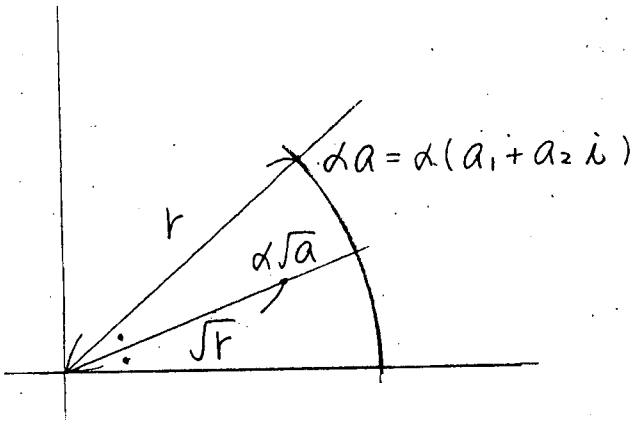

図５

命題１．５． Kを数体、βをKの元で、βの正の平方根$\sqrt{\beta}$がKの元でないとき、集合

$K'=\{y+z\sqrt{\beta}\,;\,y,\ z\in K\}$

はKと$\sqrt{\beta}$を含む最小の数体である。

［証明］y_1, y_2, z_1, $z_2\in K$, $y_2+z_2\sqrt{\beta}\neq 0$とすると、

$$(y_1+z_1\sqrt{\beta})\pm(y_2+z_2\sqrt{\beta})=(y_1\pm y_2)+(z_1\pm z_2)\sqrt{\beta}\in K'$$

$$(y_1+z_1\sqrt{\beta})\ (y_2+z_2\sqrt{\beta})=(y_1y_2+z_1z_2\beta)+(y_1z_2+y_2z_1)\sqrt{\beta}\in K'$$

$$\frac{(y_1+z_1\sqrt{\beta})}{(y_2+z_2\sqrt{\beta})}=\frac{(y_1y_2-z_1z_2\beta)+(y_2z_1-y_1z_2)\sqrt{\beta}}{y_2^{\,2}-z_2^{\,2}\beta}\in K'$$

したがって、集合K'はKと$\sqrt{\beta}$を含む最小の数体である。

定義１．６． Kを数体、βをKの元で、βの正の平方根$\sqrt{\beta}$がKの元でないとき、集合

$K'=\{y+z\sqrt{\beta}\,;\,y,\ z\in K\}$

をK（$\sqrt{\beta}$）と表わし、Kに$\sqrt{\beta}$を付加して得られる数体という。

また、数体K（$\sqrt{\beta}$）の元が、$y+z\sqrt{\beta}$，$y'+z'\sqrt{\beta}$（y，z，y'，$z'\in K$）のように、２通りに表されたとすると

$y+z\sqrt{\beta}=y'+z'\sqrt{\beta}$

$(y-y')=(z-z')\sqrt{\beta}$

となる。$z\neq z'$と仮定すると

$$\sqrt{\beta}=\frac{y-y'}{z-z'}\in K$$

となり矛盾するので、

$z=z'$，$y=y'$

つまり、数体K（$\sqrt{\beta}$）の元の表し方は、ただ１通りである。（表現の一意性）

ところで、定木とコンパスによる作図では、作図を進めていく段階で、新たに作図できる数になるものとして、２直線の交点，２つの円の交点，円と直線との交点があるが、これらの交点がどのような集合に属するかを、次に調べていく。

（Ⅰ）２直線の交点

異なる２点A（αx_1，αy_1），B（αx_2，αy_2）を通る直線１と異なる２点C（αx_3，αy_3），D（αx_4，αy_4）を通る直線mが１点（αp，αq）で交わる場合、p、qはx_1，・・・，x_4，y_1，・・・，y_4を含む最小の数体に属する。

なぜならば、l，mの方程式は

l：$ax+by=\alpha c$ ---------- （１）

m：$a'x+b'y=\alpha c'$ ---------- （２）

とかける。ただし、$a=y_2-y_1$，$b=x_1-x_2$，$c=x_1(y_2-y_1)-y_1(x_2-x_1)$

$a'=y_4-y_3$，$b'=x_3-x_4$，$c'=x_3(y_4-y_3)-y_3(x_4-x_3)$とする。

したがって

$$p=\frac{b'c-bc'}{ab'-a'b}$$

$$q=\frac{ac'-a'c}{ab'-a'b}$$

となる。

（Ⅱ）円と直線との交点

（Ⅰ）における直線１と中心C（αx_3，αy_3），半径αrの円Oが（αp，αq）で交わる場合、x_1，・・・，x_3，y_1，・・・，y_3，rを含む最小の数体Kのある元s＞

0をとれば、p、qはK（$\sqrt{s}$）に属する。

なぜならば、円Oの方程式は

O：$(x-\alpha x_3)^2+(y-\alpha y_3)^2=(\alpha r)^2$ ---------- （3）

とかける。

したがって、pはxの方程式

$Lx^2+2\alpha Mx+\alpha^2 N=0$

の解となる。ただし、L，M，Nはkの元である。

ゆえに、pは$s=M-LN$とするとK（$\sqrt{s}$）の元である。

（Ⅲ）2つの円の交点

（Ⅱ）における円Oと中心A（αx_1，αy_1），半径αtの円O′が（αp，αq）で交わる場合、x_1，x_3，y_1，y_3，r，tを含む最小の数体Kのある元$s>0$をとれば、p，qはK（$\sqrt{s}$）に属する。

なぜならば、円O′の方程式は

O′：$(x-\alpha x_1)^2+(y-\alpha y_1)^2=(\alpha t)^2$ ---------- （4）

とかける。

（4）－（3）を考えるとp，qは（3）式と$L'x+M'y=\alpha N'$を満たす。ただし、L′，M′，N′はKの元である。

したがって、（Ⅱ）の場合と同様の結論を得る。

（Ⅰ）～（Ⅲ）より、1回の作図操作によって生じる交点は、Kを数体、$\beta\in K$、$\sqrt{\beta}\notin K$とすると、集合$\alpha K(\sqrt{\beta})$の元となる。

以上のことから、次のことがいえる。

命題1．7． aがF_αの元でαQの元でないとき，$K_0=Q$として、次の性質をもつ数体の系列K_0，K_1，K_2，・・・，K_nが存在する。

$K_1=K_0(\sqrt{\beta_1})$，$\beta_1\in K_0$，$\sqrt{\beta_1}\notin K_0$

$K_2=K_1(\sqrt{\beta_2})$，$\beta_2\in K_1$，$\sqrt{\beta_2}\notin K_1$

$K_j=K_{j-1}(\sqrt{\beta_j})$，$\beta_j\in K_{j-1}$，$\sqrt{\beta_j}\notin K_{j-1}$（j＝1，2，・・・，n）

$a\notin\alpha K_{n-1}$，$a\in\alpha K_n$

特に、$0<a\in R$の時は$\beta_j>0$にとれる。

今までの議論から

$F_{\alpha} = \alpha F_1$

となることは明らかである。

尚、第２章以下の作図問題では、初めに与えられている点が、（０，０），（１，０）であるとして考えていくことにする。

第２章　倍積問題

第１節　倍積問題の由来

今から二千数百年前、ギリシャのデロス島で、悪疫が流行したので、神様にお伺いを立てた所、”今の立方体の祭壇を、ちょうど２倍の体積をもつものに作り変えよ”という神託があった。

ところが、柱や梁（りょう）の長さを変えて、１辺がもとの２倍の立方体の祭壇を作ってしまったので、体積は８倍になってしまい、悪疫は止むどころかますます猛威を振るったという。

そこで、*Platon* は、体積を２倍にするためには、柱や梁の長さをどのように定めればよいかを考えた。

これが倍積問題の始まりといわれている。

この伝説の神は、デロス島の守護神なので、この問題は別名『デロスの神殿の問題』と呼ばれている。

さて、この問題を幾何学的に言い換えると次のようになる。

「１辺αの立方体がある。そのちょうど２倍の体積をもつ立方体の１辺を作図せよ。」

求める立方体の１辺をｘとすれば

$x^3 = 2\alpha^3$

$x = \alpha\sqrt[3]{2}$

つまり、２点（０，０），（α，０）が与えられている時、定木とコンパスのみを用いて、$\alpha\sqrt[3]{2}$が作図可能な数かどうかということである。

ところで、第１章における命題１．７の後に述べた関係式

$F_\alpha = \alpha F_1$

より、第２節では、計算を簡素化するために、$\alpha = 1$として考えていくことにする。

尚、第２節で取り扱う諸命題の証明は、『数学への誘い』，羽鳥　裕久著，培風館を参考にさせていただいた。

第２節　作図不可能であることの証明

命題２．１．　$\sqrt[3]{2}$は無理数である

［証明］$\sqrt[3]{2}$が有理数であると仮定し、$\sqrt[3]{2}=m/n$（m，nは互いに素な自然数）とおく。

両辺を３乗すると

$2n^3=m^3$　　----------（１）

となる。

左辺は偶数なので、右辺のm^3も偶数である。

ゆえに、mは偶数となり、$m=2m'$（m'は自然数）とおける。

これを（１）式に代入すると

$n^3=4m'^3$

となるので、同様の論法より、nは偶数であることがわかる。

よって、m，nは公約数２をもつことになり、仮定に矛盾する。

ゆえに、$\sqrt[3]{2}$は無理数である。

命題２．２．　$\sqrt[3]{2}$は定木とコンパスを有限回用いて作図できる数ではない。

［証明］$\sqrt[3]{2}$が作図できる数であると仮定すると、$\sqrt[3]{2}\not\in Q$であるので、第１章における命題１．７より次のことがいえる。

$K_0=Q$として次の性質をもつ数体の系列K_0，K_1，K_2，・・・，K_nが存在する。

$K_1=K_0(\sqrt{\beta_1})$，$0<\beta_1\in K_0$，$\sqrt{\beta_1}\not\in K_0$

$K_2=K_1(\sqrt{\beta_2})$，$0<\beta_2\in K_1$，$\sqrt{\beta_2}\not\in K_1$

$K_j=K_{j-1}(\sqrt{\beta_j})$，$0<\beta_j\in K_{j-1}$，$\sqrt{\beta_j}\not\in K_{j-1}$（j＝１，２，・・・，n）

$\sqrt[3]{2}\not\in K_{n-1}$，$\sqrt[3]{2}\in K_n$

このとき、$\sqrt[3]{2}=y+z\sqrt{\beta_n}$（$y,\ z\in K_{n-1},\ z\neq 0$）　　----------（２）

とかける。

（２）式の両辺を３乗すると

$2 = y^3 + 3y^2z\sqrt{\beta_n} + 3yz^2\beta_n + z^3\beta_n\sqrt{\beta_n}$

$= y^3 + 3yz^2\beta_n + (3y^2z + z^3\beta_n)\sqrt{\beta_n}$

となる。

ここで、$y^3 + 3yz^2\beta_n$, $3y^2z + z^3\beta_n \in K_{n-1}$なので、第１章における定義１．６の次に述べたＫ（$\sqrt{\beta}$）の元に関する表現の一意性より

$y^3 + 3yz^2\beta_n = 2$, $3y^2z + z^3\beta_n = 0$

となる。

また、これらより、

$2 = y^3 + 3yz^2\beta_n - (3y^2z + z^3\beta_n)\sqrt{\beta_n}$

$= (y - z\sqrt{\beta_n})^3$

と変形できる。

よって、実数の範囲で、２は立方根として、$y \pm z\sqrt{\beta_n}$の２つももつことになり矛盾する。

故に、$\sqrt[3]{2}$は作図できる数ではない。

第３章　円積問題

第１節　円積問題の由来

与えられた多角形と面積の等しい３角形は、容易に描くことができる。

また、図１にしたがうと

$x^2+r^2=z^2$　　---------- （１）

という関係式を得るが

$r^2=y^2+\left(\frac{1}{2}a-\frac{1}{4}h\right)^2$,

$z^2=y^2+\left(\frac{1}{2}a+\frac{1}{4}h\right)^2$

より（１）式は

$x^2=\frac{1}{2}ah$

と変形されるので、底辺ａと高さｈが与えられた、３角形と面積の等しい正方形（１辺ｘ）を描くことができるということがわかる。

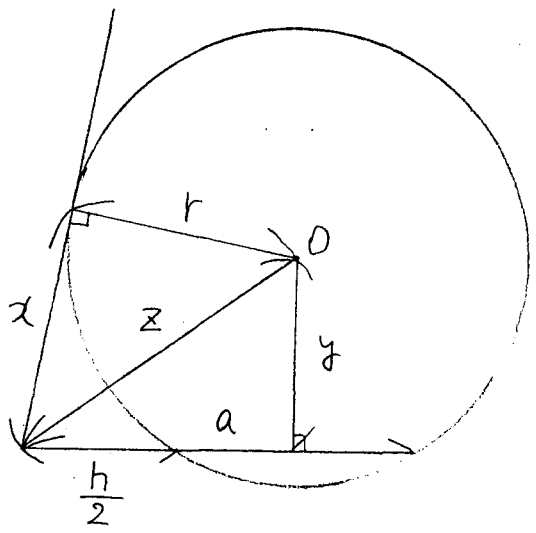

図１

したがって、辺の数が無限に大きくなった場合を考えて、”与えられた円と面積の等しい正方形が作図できるか？”という円積問題が生まれた。

ところで、第１章における命題１．７の後に述べた関係式

$F_\alpha=\alpha F_1$

より、今後、計算を簡素化するために、与えられた円の半径を１として考えていくことにする。

円の半径を１，求める正方形の１辺をｘとすれば

$x^2 = 1 \cdot 1 \cdot \pi$

より

$x = \sqrt{\pi}$

となる。

第１章における命題１．４より、πが作図可能な数であれば$\sqrt{\pi}$もまた作図可能な数である。

ここで、代数的数について触れておく。

定義３．１． 有理係数の多項式

$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$

の零解になる数を代数的数という。

命題３．２． ２個の代数的数ａ，ｂに対して、$a \pm b$，ab，a/bも代数的数である。

この命題の証明は省略させていただく。

尚、詳しい証明に関しては『ガロワと方程式』草場　公邦著、朝倉書店を参照していただきたい。

この命題より、代数的数の全体からなる集合は体をなしていることがわかる。

命題３．３． F_1の元は代数的数である。

［証明］まず、βが代数的数の時、$\sqrt{\beta}$も代数的数であることを示す。

βは代数的数なので

$\beta^n + c_1 \beta^{n-1} + \cdots + c_n = 0$

となる$c_j \in Q$（$j = 1, 2, \cdots, n$）が存在する。

よって、$\sqrt{\beta}$は

$x^{2n} + c_1 x^{2n-2} + \cdots + c_n = 0$

の解である。

したがって、$\sqrt{\beta}$は代数的数となる。

有理数は代数的数なので、$a \in F_1$，$a \in Q$とすると第１章における命題１．７より、次

のことがいえる。

$K_0=Q$として次の性質をもつ数体の系列K_0，K_1，K_2，・・・，K_nが存在する。

$K_1=K_0(\sqrt{\beta_1})$，$0<\beta_1\in K_0$，$\sqrt{\beta_1}\notin K_0$

$K_2=K_1(\sqrt{\beta_2})$，$0<\beta_2\in K_1$，$\sqrt{\beta_2}\notin K_1$

$K_j=K_{j-1}(\sqrt{\beta_j})$，$0<\beta_j\in K_{j-1}$，$\sqrt{\beta_j}\notin K_{j-1}$（$j=1$，$2$，・・・，$n$）

$a\notin K_{n-1}$，$a\in K_n$

次に、K_jの元が代数的数であるとき、K_{j+1}の元も代数的数となることを示す。

K_jの元は代数的数であるので、$\beta_{j+1}\in K_j$から$\sqrt{\beta_{j+1}}$　も代数的数であることがわかる。

また、$x\in K_j(\sqrt{\beta_{j+1}})$とすると、$x=y+z\sqrt{\beta_{j+1}}$（$y$，$z\in K_j$）と表されるが命題３．２より　xは代数的数となることがわかる。

ゆえに、K_nの元は代数的数ということになり、F_1の元は代数的数であるという結論を得る。

また、有理係数の多項式

$f(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$

の零解にならない数、つまり代数的数でない数を超越数という。

結局、円積問題は「πは超越数である」ということを証明すれば解決する。

以下、第２節ではπの超越性について調べていくことにする。

尚、第２節で取り扱う諸命題の証明は、『ガロアの理論』Ｉ．スチュワート著、永尾汎監訳、新関　章三訳、共立全書を参考にさせていただいた。

第２節　πの超越性

ここでは、まず、基本対称式について少し触れておくことにする。

定義３．３．　ｆを数体Ｋ上の多項式とする。

Ｋの元αがｆの単根であるとは、ｆ（ｔ）が、（ｔ－α）で割り切れて、（ｔ－α）^{2}で割り切れないときをいう。

また、元αがｆの多重度ｍの根であるとは、ｆ（ｔ）が、（ｔ－α）^{m}で割り切れて、（ｔ－α）$^{m+1}$で割り切れないときをいう。

多重度が１より大きい根を重複根、あるいは多重根という。

（多重度も数えて）ｎ個の１次因子の積として表されるｎ次多項式を考える。

$f(t)=k(t-\alpha_1)(t-\alpha_2)\cdots(t-\alpha_n)$

ただしｋ∈Ｋで、α_i（ｉ＝１，２，・・・，ｎ）は必ずしも異なるとは限らないＣにおける根である。

$f(t)=a_0+a_1t+\cdots+a_nt^n$

と仮定し、はじめの式を展開したものと係数を比較すると

$a_n=k$

$a_{n-1}=-k(\alpha_1+\alpha_2+\cdots+\alpha_n)$

$a_{n-2}=k(\alpha_1\alpha_2+\alpha_1\alpha_3+\cdots+\alpha_{n-1}\alpha_n)$

$a_0=k(-1)^n\alpha_1\alpha_2\cdots\alpha_n$

を得る。

右辺のα_1，・・・，α_nに関する（±ｋを度外視した）式は特別な名でよばれている。

定義３．４．　不定元t_1，・・・，t_nに関するｒ次の基本対称式

$s_r(t_1,\cdots,t_n)$

とは、元t_1，・・・，t_nの中から、互いに異なるｒ個の元をとって積をつくったものすべての和である。

尚、上の等式は

$a_{n-r}=k(-1)^r s_r(\alpha_1, \cdots, \alpha_n)$

と簡単にまとめることができる。

これらの多項式は、不定元t_iの置換によって不変であるという意味で対称的である。

基本対称式以外にも対称式は存在する。

たとえば、$t_1^2+t_2^2+\cdots+t_n^2$などがそうである。

しかし、すべての対称式は基本対称式で書き表される。

ここで、πの超越性を証明するのに必要な命題を1つ紹介しておく。

命題3．5． 体K上の$t_1, \cdots, t_n$に関する任意の対称式は、次数が与えられた対称式の次数以下の、基本対称式$s_r(t_1, \cdots, t_n)$ $(r=0, \cdots, n)$に関するK係数の多項式で表される。

この命題の証明については、ここでは省略させていただく。

尚、詳しい証明に関しては *Salmon, G, Lessons introductory to the modern Higher Algebra*, 及び、*Van der Waerden, B, L, Modern Algebra (2vols)*を参照していただきたい。

最後に、1882年、*Lindemann* によって発見された「πの超越性」の証明によって、円積問題は見事、解決をむかえるわけである。

命題3．6． πは超越数である。

［証明］ πをある0でないQ上の多項式の根であると仮定する。

その時、$i=\sqrt{-1}$とするとiπも代数的数となる。

そこで、$\theta_1(x) \in Q[x]$をその根が$\alpha_1=i\pi, \alpha_2, \cdots, \alpha_n$であるような多項式とする。

Euler の有名な定理より

$e^{i\pi}+1=0$

であるから

$(e^{i\pi}+1)(e^{\alpha_2}+1)\cdots(e^{\alpha_n}+1)=0$ ---------- (1)

次に、整係数の多項式で、その根が（１）式を展開したときに現れるｅの指数$\alpha_{i_1}+\cdots+\alpha_{i_r}$（$1\leqq r\leqq n$）であるようなものを構成する。

例えば、$e^{\alpha_s}e^{\alpha_t}\cdot 1\cdots 1$となる項は指数$\alpha_s+\alpha_t$を与える。

対ｓ、ｔをすべてとって$\alpha_1+\alpha_2,\ \cdots,\ \alpha_{n-1}+\alpha_n$が得られる。

これらの基本対称式は$\alpha_1,\ \cdots,\ \alpha_n$の対称式ともなるから命題３，５よりそれらは$\alpha_1,\ \cdots,\ \alpha_n$の基本対称式の多項式として表される。

すると、これらは$\alpha_1,\ \cdots,\ \alpha_n$を根としてもつ多項式$\theta_1$の係数で表現される。　よって、対ｓ，ｔからつくられた和$\alpha_s+\alpha_t$はある方程式$\theta_2(x)=0$を満たす。
ここで、θ_2は有理数を係数とする多項式である。

同様にして、α_iのｋ個の和の全体はＱ上のある多項式$\theta_k(x)$の根となる。

そのとき、$\theta_1(x)\ \theta_2(x)\cdots\theta_n(x)$はＱ上の多項式で、その根は（１）式におけるｅの指数である。

ｘのある適当なべきで割り、ある適当な整数をかけると根が（１）式の展開式における０でない指数$\beta_1,\ \cdots,\ \beta_r$であるようなＺ上の多項式$\theta(x)$が得られる。

ところで、（１）式は次の形

$e^{\beta_1}+\cdots+e^{\beta_r}+e^{0}+\cdots+e^{0}=0$

すなわち

$e^{\beta_1}+\cdots+e^{\beta_r}+k=0\quad(k\in Z)$　　----------　（２）

の形で書かれる。

（１）式の展開式には１・１・・・・１なる項が現れるからｋ＞０である。

さて、$\theta(x)$を

$\theta(x)=c_0x^r+c_1x^{r-1}+\cdots+c_r\quad(c_0\neq 0)$

とおく。ここで、０はθの根でないから$c_r\neq 0$である。

そこで

$$f(x)=\frac{c^s x^{p-1}\{\theta(x)\}^p}{(p-1)!}$$

とおく。

ここで、ｓ＝ｒｐ－１でｐは任意の素数とする。

また

$F(x)=f(x)+f'(x)+\cdots+f^{(s+p)}(x)$

と定義する。

ここで、$f^{(s+p+1)}(x)=0$であることに注意すると

$$\frac{d}{dx}\{e^{-x}F(x)\}=-e^{-x}f(x)$$

を得る。

よって

$$e^{-x}F(x)-F(0)=-\int_0^x e^{-y}f(y)\,dy$$

ここで、$y=\lambda x$とおけば

$$F(x)-e^{x}F(0)=-x\int_0^1 e^{(1-\lambda)x}f(\lambda x)\,d\lambda$$

xをβ_1，・・・，β_r上にわたって動かしてその和をとると（2）式より

$$\sum_{j=1}^{r}F(\beta_j)+kF(0)=-\sum_{j=1}^{r}\beta_j\int_0^1 e^{(1-\lambda)\beta_j}f(\lambda\beta_j)\,d\lambda$$

---------- （3）

を得る。

ここで、十分大きいすべてのpに対して上式の左辺の値は0でない整数となることを以下に示す。

$0<t<p$ならば

$$\sum_{j=1}^{r}f^{(t)}(\beta_j)=0$$

次に0でない項を得るには$\{\theta(x)\}^p$を少なくともp回微分しなければならないから$p\leqq t\leqq s+p$なるtに対して各微分$f^{(t)}(\beta_j)$はpを因数にもつ。

そのような任意のtに対して

$$\sum_{j=1}^{r}f^{(t)}(\beta_j)$$

は次数がs次以下のβ_jの対称式である。

したがって、それは命題3．5より次数がs次以下の係数c_i/cに関する多項式である。

$f(x)$の定義における因子c^sにより上の式は整数となる。

よって、$t\geqq p$のときは適当な$k_t\in Z$に対して

$$\sum_{j=1}^{r}f^{(t)}(\beta_j)=pk_t$$

とかける。

さて、$F(0)$に注目する。

適当な$l_t\in Z$に対して

$$f^{(t)}(0)=\begin{cases}0 & (t\leqq p-2)\\ c^s c_r{}^p & (t=p-1)\\ l_t p & (t\geqq p)\end{cases}$$

したがって、（3）式の左辺はある$m\in Z$に対して

$mp+kc^{s}c_{r}^{p}$ $(p \leqq t)$

となる。

ところで、$k \neq 0$, $c \neq 0$, $c_{r} \neq 0$ であるから

$p > max(k|c||c_{r}|)$

となるように素数pを選べば、（3）式の左辺はpで割り切れない整数となるから0ではない。

最後に（3）式の右辺を評価する。

$$|f(\lambda\beta_{j})| \leqq \frac{|c|^{s}|\beta_{j}|^{p-1}|(m(j))|^{p}}{(p-1)!}$$

ここで、$m(j) = \sup_{0 \leqq \lambda \leqq 1} |\theta(\lambda\beta_{j})|$

したがって

$$\left|-\sum_{j=1}^{r}\beta_{j}\int_{0}^{1}e^{(1-\lambda)\beta_{j}}f(\lambda\beta_{j})\,d\lambda\right| \leqq \sum_{j=1}^{r}\frac{|\beta_{j}|^{p}|c^{s}||m(j)|^{p}B}{(p-1)!}$$

ここで

$$B = \max_{j}\left|\int_{0}^{1}e^{(1-\lambda)\beta_{j}}d\lambda\right|$$

よって、上の式は$p \to \infty$のとき0に収束するため矛盾する。

ゆえに、πは超越数である。

第４章　角の３等分問題

第１節　角の３等分問題の由来

任意の大きさの角を、定木とコンパスを用いて、２等分することは簡単である。

また、その角をさらに２等分することによって、任意の大きさの角を４等分することも可能である。

では”３等分は？”と考えて生まれたのが角の３等分問題である。

つまり、角の３等分問題とは、

「与えられた任意の大きさの角を３等分せよ」

というものである。

まず、図１のように、ｘｙ平面上に、Ｏを原点、ＯＡ＝１となるように点Ａをｘ軸上にとる。

ＯＢ＝１、∠ＡＯＢ＝θとすると点Ｂの座標は、

Ｂ（ｃｏｓθ，ｓｉｎθ）と表される。

仮に、∠ＡＯＢが３等分できたとして、３等分線上に、ＯＣ＝１となるように点Ｃをとると、点Ｃの座標は、

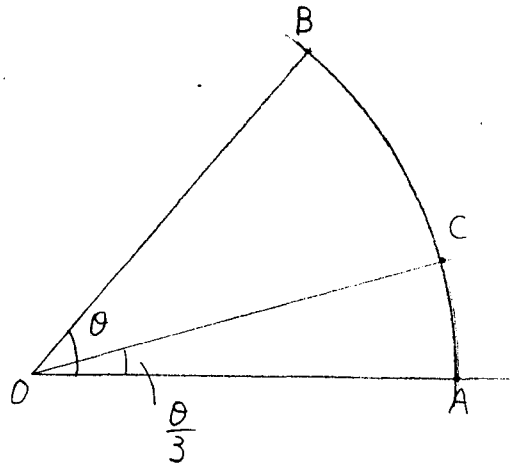

図１

$$C\left(\cos\frac{\theta}{3},\ \sin\frac{\theta}{3}\right)$$

となるので、角の３等分問題では、この点Ｃを求めることに帰着される。

ところで、加法定理を利用すると、

$$\cos\theta = 4\cos^3\left(\frac{\theta}{3}\right) - 3\cos\left(\frac{\theta}{3}\right)$$

と変形できる。ここで、$\cos\theta = \alpha$、計算の都合上、$2\cos(\theta/3) = x$とおくと角の３等分方程式

$x^3 - 3x - 2\alpha = 0$　　---------- （１）

を得る。

結局、角の３等分問題では、（１）式の解が、与えられた２点（０，０），（１，０）を出発点として、定木とコンパスを有限回用いて、作図可能かどうか調べていけばいいということになる。

ところで、角の３等分問題が、”一般には作図不可能である”ということを証明するためには、１つでも反例（作図できない例）をあげればいいので、第２節では、θが一般角の場合について考えていく一方で、３等分できない代表的な角として、$\theta = 60^\circ$の場合をとりあげて考えていこうと思う。

尚、第２節で取り扱う諸命題の証明は、『数学への誘い』，羽鳥　裕久著，培風館、及び、柳原　弘志氏による講義録「作図不能問題」を参考にさせていただいた。

第２節　一般には作図不可能である証明

第１節の角の３等分方程式

$x^3-3x-2\alpha=0$　　----------　（１）

において、θが一般角の場合について考えていくわけだが、ここでは、（１）式をもう少し一般化させた次の命題の証明から始めることにする。

命題４．１．　整係数３次方程式

$ax^3+bx^2+cx+d=0\ (a\neq 0)$　　----------　（２）

の解が、作図可能な数であるとすると、（２）式は少なくとも１つの有理数解をもつ。

［証明］（２）式の解をx_1，x_2，x_3とし、x_1が作図可能な数で有理数でないとすると第１章における命題１．７より次の事がいえる。

$K_0=Q$として次の性質をもつ数体の系列K_0，K_1，K_2，・・・　，K_nが存在する。

$K_1=K_0(\sqrt{\beta_1})$，$\beta_1=-1$

$K_2=K_1(\sqrt{\beta_2})$，$\beta_2\in K_1$，$\sqrt{\beta_2}\notin K_1$

$K_j=K_{j-1}(\sqrt{\beta_j})$，$\beta_j\in K_{j-1}$，$\sqrt{\beta_j}\notin K_{j-1}$（$j=1,2,\cdots,n$）

$x_1\notin K_{n-1}$，$x_1\in K_n$

このとき、

$x_1=y+z\sqrt{\beta_n}$（y、$z\in K_{n-1}$，$z\neq 0$）

とかける。

これを（２）式に代入すると、

$a(y+z\sqrt{\beta_n})^3+b(y+z\sqrt{\beta_n})^2+c(y+z\sqrt{\beta_n})+d=0$

$ay^3+3a\beta_n yz^2+by^2+b\beta_n z^2+cy+d$

$\quad+(3ay^2z+a\beta_n z^3+2byz+cz)\sqrt{\beta_n}=0$　　----------　（３）

となる。

ここで、

$A=ay^3+3a\beta_n yz^2+by^2+b\beta_n z^2+cy+d$，

$B=3ay^2z+a\beta_n z^3+2byz+cz$

とおくと（３）式は、

$A+B\sqrt{\beta_n}=0$

とかける。

A，B$\in K_{n-1}$なので、第１章における定義１．６の次に述べたK（$\sqrt{\beta}$）の元に関する表現の一意性より

$A=0$，$B=0$

となる。

また、これらを用いると、

$A-B\sqrt{\beta_n}=0$

となることから、A，Bをもとにもどすと、

$0=ay^3+3a\beta_n yz^2+by^2+b\beta_n z^2+cy+d$

$\quad-(3ay^2z+a\beta_n z^3+2byz+cz)\sqrt{\beta_n}$

$=a(y-z\sqrt{\beta_n})^3+b(y-z\sqrt{\beta_n})^2+c(y-z\sqrt{\beta_n})+d$

となるので、$y-z\sqrt{\beta_n}$も（２）式の解の１つということがわかる。

また、$x_2=y-z\sqrt{\beta_n}$とおくと、$x_2\notin K_{n-1}$，$x_2\in K_n$は明らかである。

ここで、解と係数の関係を用いると、$x_1+x_2+x_3=-b/a$となるので、

$(y+z\sqrt{\beta_n})+(y-z\sqrt{\beta_n})+x_3=-b/a$

つまり、

$x_3=-2y-(b/a)$

を得る。

y，a，b$\in K_{n-1}$より、$x_3\in K_{n-1}$となるが、K_{n-1}よりも手前にある数体の元である可能性も出てくる。

そこで、$x_3\notin K_0$とし、$x_3\notin K_{m-1}$，$x_3\in K_m$となる自然数mが、１，２，・・・，n－１の中に存在すると仮定すると、

$x_3=y'+z'\sqrt{\beta_m}$（y'，$z'\in K_{m-1}$，$z'\neq 0$）

とかけて、前述のx_1に対する議論と同様の論法より、x_1，x_2のいずれか一方が、$y'-z'\sqrt{\beta_m}$（$\in K_m$）と一致するはずである。

ところが、x_1，$x_2\notin K_{n-1}$より、x_1，$x_2\notin K_m$となり矛盾する。

よって、$x_3\in K_0$、つまり、x_3は有理数でなければならない。

したがって、（２）式の解が、作図可能な数であるとすると、（２）式は少なくとも１つは有理数解をもつ。

例えば、$\theta=60°$の時、（１）式は、

$x^3-3x-1=0$　　----------　（４）

となる。

命題４．１を用いると、もし、６０°が３等分可能ならば、（４）式は少なくとも１つは有理数解をもつはずである。

命題４．２． $x^3-3x-1=0$は有理数解をもたない。

［証明］（４）式が有理数解をもつと仮定し、$x=m/n$（m，nは互いに素な整数）とおき、（４）式に代入すると

$m^3-3mn^2-n^3=0$ ---------- （５）

$m^3=n(3mn+n^2)$

となる。

ここで、nが素因数pをもっているとすると、左辺も素因数pをもつことになる。

つまり、pはmの素因数となるので、m，nが互いに素であることに矛盾する。

よって、$n=\pm1$となる。

逆に、（５）式を$n^3=m(m^2-3n^2)$と変形することによって、同様の論法より、$m=\pm1$が得られる。

したがって、$x=\pm1$となるが、これは（４）式の解とはならない。

すなわち、（４）式は有理数解をもたない。

第１節でも述べたが、”任意の大きさの角は一般には３等分できない”ことの証明は$\theta=60°$の時の作図不能性を示せば十分であるが、これだけではあまりにも物足りないので、以下の判定条件を付け加えておく。

命題４．３． 整係数３次方程式

$ax^3+bx^2+cx+d=0$ $(a\neq0)$ ---------- （２）

が有理数解m／n（m，nは互いに素な整数）をもつとき、mはdの約数であり、nはaの約数である。

ただし、$d\neq0$とする。

［証明］$x=m/n$として（２）式に代入すると、

$am^3+bm^2n+cmn^2+dn^3=0$ ---------- （６）

$dn^3=-m(am^2+bmn+cn^2)$

となる。

ここで、mは右辺の因数で、しかも、m，nは互いに素ということから、mはdの約数

ということがわかる。

また、（６）式を$am^3=-n(bm^2+cmn+dn^2)$と変形することによって、同様の論法より、ｎがａの約数であることを得る。

例えば、命題４．３を用いると、$\theta=60^\circ$の時、（４）式よりｍは－１の約数、ｎは１の約数となり、ｘ＝±１を得るが、これは（４）式の解とはならないので、６０°の３等分は不可能ということが判断できる。

最後に、ここではその証明については触れないが、一般にｎ°の作図可能性について次の命題が成立する。

命題４．４．　ｎを自然数とするとき、ｎ°が作図可能となるための必要十分条件は、ｎが３の倍数となることである。

この命題より、ｎ＝３ｍ（ｍは自然数）としたとき、任意の角θが３等分可能であるための必要十分条件は、$\theta=3n$、すなわちθが９の倍数となることであるという結論を得る。

第５章　円の等分問題

第１節　分円方程式

第２章から第４章まで、３つの作図不能問題について考えてきた。

この章では、作図不能問題ではないが、定木とコンパスのみを用いての作図問題として、円の等分問題をとりあげることにする。

円の等分問題とは、原点を中心とした半径１の円周上に、$z_0=(1,\ 0)$，z_1，z_2，・・・，z_{n-1}のｎ個の点を等間隔にとることによって、円に内接する正ｎ角形を作図するものである。

まず、方程式

$z^n=1$　　----------　（１）

を複素平面上で考える。

$\theta=2\pi/n$（$n\geqq 2$）とおくと、ｎ個の点$z_0=1$，$z_1=\cos\theta+i\sin\theta$，$z_2=\cos 2\theta+i\sin 2\theta$，・・・，$z_{n-1}=\cos(n-1)\theta+i\sin(n-1)\theta$は単位円をｎ等分する。

do Moivre の定理より、

$z_k{}^n=\cos(nk\theta)+i\sin(nk\theta)=1$

となり、z_kはｎ次方程式（１）の解であることがわかる。

よって、円の等分問題では、この分円方程式$z^n=1$の解が作図できる数であるかどうかを調べればよい。

第２節以降では、z_0，z_1，z_2，・・・，z_{n-1}を解とした分円方程式を

$z^n-1=(z-1)(z^{n-1}+z^{n-2}+\cdots+z+1)$

と変形して、$z_0=1$とおき、$z_1=\cos\theta+i\sin\theta$の実部が作図できる数であるか

どうかを調べていくことにする。

z_1が作図できる数なら、z_2，z_3，・・・もコンパスを用いると作図できるというわけである。

尚、第３節における諸命題の証明は、『不可能の証明』、津田　丈夫著、共立出版社，『初等幾何学作図問題』、窪田　忠彦著、内田老鶴圃新社を参考にさせていただいた。

第２節　正５角形，正７角形の作図

［１］正５角形の作図可能性

第１節より、ｎ＝５のとき、分円方程式は

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

となりz_1は

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

の解となる。

$z\neq 0$より両辺をz^2でわると

$$z^2+z+1+\frac{1}{z}+\frac{1}{z^2}=0 \quad \cdots\cdots\cdots\cdots\cdots\cdots (2)$$

となるので、$t=z+\frac{1}{z}$とおき（２）式に代入すると

$t^2+t-1=0$

となる。よって、

$$t=\frac{-1\pm\sqrt{5}}{2}$$

となり、ｔをもとにもどすと

$$z+\frac{1}{z}=\frac{-1+\sqrt{5}}{2}$$ より

$2z^2+(1-\sqrt{5})z+2=0$

$$z=\frac{-1+\sqrt{5}\pm i\sqrt{10+2\sqrt{5}}}{4}$$

となる。

同様に

$$z+\frac{1}{z}=\frac{-1-\sqrt{5}}{2}$$ より

$$z=\frac{-1-\sqrt{5}\pm i\sqrt{10-2\sqrt{5}}}{4}$$

が得られる。

z_1は実部，虚部ともに正であるので

$$z_1=\frac{-1+\sqrt{5}+i\sqrt{10+2\sqrt{5}}}{4}$$

となる。

このｚ₁の実部が作図できる数かどうかを調べるわけだが、

$$\frac{-1+\sqrt{5}}{4} \in Q(\sqrt{5})$$

よりこれは明らかである。

ゆえに、正５角形は作図可能である。

次に、具体的な作図法を紹介しておく。

まず、図１のように、半径ｒの円に内接する正１０角形の１辺ＡＢの作図から考える。

単位円周上に点Ａをとり、ＯＱ⊥ＯＡ，ＯＱ＝ｒ／２となる点Ｑをとる。

次に、ＱＲ＝ｒ／２となる点Ｒを線分ＡＱ上にとる。

最後にＡＲ＝ＡＢとなる点Ｂを円周上にとり、長さＡＢでコンパスにより順次円周を区切ると、１つとばしで結んだ図形が円に内接する正５角形となる。

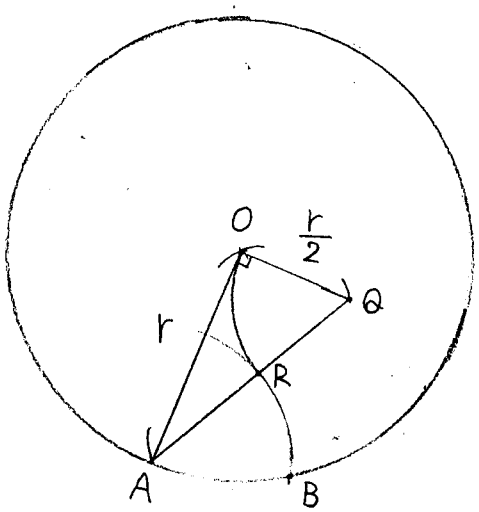

図１

［２］正７角形の作図不可能性

正５角形の作図のときと同様に考えると、ｚ₁は

$$z^6+z^5+z^4+z^3+z^2+z+1=0$$

の解となる。

両辺をz^3でわると

$$z^3+z^2+z+1+\frac{1}{z}+\frac{1}{z^2}+\frac{1}{z^3}=0 \quad \cdots\cdots\cdots\cdots\cdots\cdots (3)$$

となるので、$t=z+\frac{1}{z}$とおくと

$$z^2+\frac{1}{z^2}=\left(z+\frac{1}{z}\right)^2-2=t^2-2$$

$$z^3+\frac{1}{z^3}=\left(z+\frac{1}{z}\right)\left(z^2-1+\frac{1}{z^2}\right)=t(t^2-3)$$

より（４）式は

$$t^3+t^2-2t-1=0 \quad \cdots\cdots\cdots\cdots\cdots\cdots (4)$$

と変形できる。

第４章命題４．３より、（４）式が有理数解ｍ／ｎ（ｍ，ｎは互いに素な整数）をもてば、ｍ，ｎはそれぞれ１，－１の約数となるので、（４）式はｔ＝±１を解にもつことになる。

ところが、$(\pm 1)^3+(\pm 1)^2-2\times(\pm 1)-1=\mp 1$（複合同順）

となりこれは矛盾する。

したがって、（４）式は有理数解をもたないということになり、第４章命題４．１より、（４）の解は作図可能な数でないことがわかる。

ここで、$z=\cos\theta+i\sin\theta$とおくと

$$t=z+\frac{1}{z}=\cos\theta+i\sin\theta+\frac{1}{\cos\theta+i\sin\theta}$$

$$=\cos\theta+i\sin\theta+\frac{\cos\theta-i\sin\theta}{(\cos\theta+i\sin\theta)(\cos\theta-i\sin\theta)}$$

$$=2\cos\theta$$

となりｔが作図可能な数でなければz_1の実部も作図可能な数でないということがわかる。

ゆえに、正７角形は作図不可能である。

第３節　正ｎ角形の作図

［１］合同記号

円に内接する正３角形，正４角形，正５角形，正６角形は作図可能で、正７角形は作図不可能であることがわかった。

それでは、一般にはｎがどのような数のとき作図可能となるかを、これから調べていくことにする。

まず、今後の証明に必要となってくる合同記号について、次のように定義する。

定義５．１．　ａ－ｂ＝ｎｐ（ａ，ｂ，ｎ，ｐは整数）
であるとき、すなわちａとｂの差がｐの倍数のとき
　ａ≡ｂ（ｍｏｄｐ）
と表し、これをｐを法とする合同式といい、記号”≡”を合同記号という。

合同記号は、同値性の条件を満足する。
（ｉ）ａ≡ａ（ｍｏｄｐ）
（ii）ａ≡ｂ（ｍｏｄｐ）ならば、ｂ≡ａ（ｍｏｄｐ）
（iii）ａ≡ｂ（ｍｏｄｐ），ｂ≡ｃ（ｍｏｄｐ）ならば、ａ≡ｃ（ｍｏｄｐ）

命題５．２．　ａ≡ａ′（ｍｏｄｐ），ｂ≡ｂ′（ｍｏｄｐ）ならば、
　ａ±ｂ≡ａ′±ｂ′（ｍｏｄｐ）
　ａｂ≡ａ′ｂ′（ｍｏｄｐ）
が成り立つ。

［証明］定義５．１より、ａ′＝ａ＋ｍｐ，ｂ′＝ｂ＋ｎｐ（ｍ，ｎは整数）とおくと
　ａ′±ｂ′＝ａ±ｂ＋（ｍ±ｎ）ｐ
　よって、ａ±ｂ≡ａ′±ｂ′（ｍｏｄｐ）
　ａ′ｂ′＝（ａ＋ｍｐ）（ｂ＋ｎｐ）

$= ab + anp + bmp + mnp^2$

$= ab + (an + bm + mnp)\,p$

よって、$ab \equiv a'b' \pmod{p}$

命題５．３． pが素数のとき、$ab \equiv 0 \pmod{p}$ ならば

$a \equiv 0 \pmod{p}$、または$b \equiv 0 \pmod{p}$ である。

証明は簡単なので省略する。

［２］*Eisenstein* の定理

ある方程式が既約であるかどうかを調べる手段として、*Eisenstein* の定理が使われる。

ここでは、その証明を考えていくわけだが、その前にまず、次の定理から証明することにする。

定理５．４．（*Gauss* の定理）整係数の多項式

$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n$

が有理数体で可約とする。

すなわち、２つの有理係数の多項式の積に分解されるときは、実はそれは、２つの整係数の多項式の積に分解できる。

［証明］（ｉ）$a_0, a_1, a_2, \cdots, a_n$の公約数が１以外に存在しないとき

条件より、有理数$\alpha_0, \alpha_1, \cdots, \alpha_s, \beta_0, \beta_1, \cdots, \beta_t$を適当にとると

$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n$

$= (\alpha_0x^s + \alpha_1x^{s-1} + \cdots + \alpha_s)(\beta_0x^t + \beta_1x^{t-1} + \cdots + \beta_t)$

---------- （５）

と分解される。

右辺の係数の共通分母をとって整理すると

右辺$= \dfrac{q}{p}(b_0x^s + b_1x^{s-1} + \cdots + b_s)(c_0x^t + c_1x^{t-1} + \cdots + c_t)$

（$b_0, b_1, \cdots, b_s, c_0, c_1, \cdots, c_t$は整数）と変形できる。

ただし、$b_0, b_1, \cdots, b_s$の公約数が１以外に存在せず、$c_0, c_1, \cdots, c_t$

の公約数も１以外に存在しない。また、ｐ（＞０），ｑも互いに素な整数と定めることができる。

ここで、ｐ＞１として、ｐの素因数の１つをｐ′とすると、b_0，b_1，・・・，b_sの公約数は１以外に存在しないので、ｐ′で割り切れないものが１つはあることになる。この順に見ていって、最初にｐ′で割り切れないものをb_hとする。

同様に、c_0，c_1，・・・，c_tをこの順で見て、最初にｐ′で割り切れないものをc_kとすると

（５）式の右辺におけるx^{h+k}の係数＝ $\frac{q}{p}$ $\{b_h c_k + (b_{h-1} c_{k+1} + b_{h-2} c_{k+2} + \cdots) + (b_{h+1} c_{k-1} + b_{h+2} c_{k-2} + \cdots)\}$

となるが、ｐ′が｛　｝内の約数とはならないのは明らかである。また、ｐ′とｑは互いに素であることから、ｐ＝１を得る。

（ii）a_0，a_1，a_2，・・・，a_nに最大公約数ｒ＞１が存在するとき

$a_0 = r a_0'$，$a_1 = r a_1'$，・・・，$a_n = r a_n'$とすると

$a_0' x^n + a_1' x^{n-1} + a_2' x^{n-2} + \cdots + a_n'$

は可約であるので（ｉ）より整係数多項式の積にかける。よって、

$a_0' x^n + a_1' x^{n-1} + a_2' x^{n-2} + \cdots + a_n'$

$= q (b_0 x^s + b_1 x^{s-1} + \cdots + b_s)(c_0 x^t + c_1 x^{t-1} + \cdots + c_t)$

であるので、両辺をｒ倍して

$a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n$

$= r\ q (b_0 x^s + b_1 x^{s-1} + \cdots + b_s)(c_0 x^t + c_1 x^{t-1} + \cdots + c_t)$

となる。

（ｉ），（ii）より *Gauss* の定理は証明された。

定理５．５．（*Eisenstein* の定理）整係数の多項式

$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$

がある素数ｐに対して

［ｉ］a_nはｐで割り切れない

［ii］a_0，a_1，・・・，a_{n-1}はｐで割り切れる

［iii］a_0はp^2で割り切れない

が成立するとき、ｆ（ｘ）は有理数体において既約である。

［証明］ｆ（ｘ）が有理数体において可約であると仮定すれば

$a_0+a_1x+a_2x^2+\cdots+a_nx^n$

$=(b_0+b_1x+b_2x^2+\cdots+b_sx^s)\ (c_0+c_1x+c_2x^2+\cdots+c_tx^t)$

と変形でき、定理５．４よりb_0, b_1, b_2, ・・・, b_s, c_0, c_1, c_2, ・・・, c_tを整数と定めてもよい。

まず、$a_0=b_0c_0$で、条件［ii］，［iii］より、$b_0\equiv 0\ (\mathrm{mod}\ p)$，$c_0\not\equiv (\mathrm{mod}\ p)$とすることができる。

$j=0$，・・・，k（＜s）のとき、$b_j\equiv 0\ (\mathrm{mod}\ p)$が成立すると仮定すると、$j=k+1$のとき

$a_{k+1}=b_0c_{k+1}+b_1c_k+\cdots+b_kc_1+b_{k+1}c_0$

で、仮定より、$b_{k+1}\equiv 0\ (\mathrm{mod}\ p)$を得る。

よって、$b_0\equiv b_1\equiv\cdots\equiv b_s\equiv 0\ (\mathrm{mod}\ p)$となるが、$a_n=b_sc_t\equiv 0\ (\mathrm{mod}\ p)$となり条件［ｉ］に矛盾する。

ゆえに、ｆ（ｘ）は可約ではありえない。

命題５．６．　ｐが素数であるとき

$$f(x)=x^{p-1}+x^{p-2}+\cdots+x+1 \qquad \text{----------} \quad (6)$$

はＱ上既約である。

［証明］ｆ（ｘ）が既約であることと、ｆ（ｘ＋１）が既約であることは同値なので

$$(x-1)f(x)=x^p-1$$

において、ｘをｘ＋１におきかえると

$$xf(x+1)=(x+1)^p-1$$

となる。

よって

$$f(x+1)=\frac{1}{x}\left({}_pC_0x^p+{}_pC_1x^{p-1}+\cdots+{}_pC_kx^{p-k}+\cdots+{}_pC_{p-2}x^2+{}_pC_{p-1}x^1+{}_pC_p-1\right)$$

$$=x^{p-1}+\sum_{k=1}^{p-1}{}_pC_{k-1}x^{p-k}+p \qquad \text{----------} \quad (7)$$

となる。

ところで

$${}_pC_k=\frac{p\ (p-1)\cdots(p-k)}{k\ (k-1)\cdots 2\cdot 1}\quad (1\leqq k\leqq p-2)$$

より、${}_pC_k$はｐの倍数となることは明らかなので、（７）式に定理５．５を適用すると、

f（x）が既約であるという結論を得る。

［Ⅲ］*Fermat* 素数

命題５．７． f（x），g（x）は数体Kにおける多項式で、g（x）はKにおいて既約であるとする。Cにおける多項式とみると、f（x），g（x）が公約式（定数以外の共通因数）をもつならば、f（x）はg（x）で割り切れる。

［証明］f（x）がg（x）で割り切れないと仮定する。この時f（x）とg（x）との最大公約数r（x）はK上の多項式で、$0 < deg\, r(x) < deg\, g(x)$である。

なぜなら、$deg\, r(x) = deg\, g(x)$ならば、g（x）がf（x）の約数となり矛盾し、また、$deg\, r(x) = 0$ならば、f（x）とg（x）が公約式をもつことに矛盾するからである。

一方、r（x）はg（x）の約数であるから、g（x）＝q（x）r（x）（ただし、q（x）はK上の多項式）とかけ、g（x）の既約性に矛盾する。

命題５．８． 数体の系列

$K_0, K_1, K_2, \cdots, K_l$

ただし、$\beta_j \in K_{j-1}$，$\sqrt{\beta_j} \notin K_{j-1}$，$K_j = K_{j-1}(\sqrt{\beta_j})$（j＝１，２，・・・，k）があって、$K_0$（＝K）において既約なｎ次多項式g（x）が、$K_l$において初めて可約になる（$K_1, K_2, \cdots, K_{l-1}$において既約）とき、ｎは偶数で、g（x）は$K_l$における２つのｎ／２次既約多項式の積として表せる。

［証明］g（x）はK_lにおいて可約なので、因数分解を可能な限り続けると、K_lにおける最低次数の因数Φ（x）が存在する。このとき、Φ（x）の係数はK_lの元なので

$$\Phi(x) = (y_0 + z_0\sqrt{\beta_k})\, x^m + (y_1 + z_1\sqrt{\beta_k})\, x^{m-1} + \cdots + (y_m + z_m\sqrt{\beta_k})$$

ただし、$y_0, z_0, y_1, z_1, \cdots, y_m, z_m \in K_{l-1}$，$y_0 + z_0\sqrt{\beta_k} \neq 0$

と表すことができて、最低次数ということから、Φ（x）はK_lで既約で

$$2m \leqq n \qquad \text{----------} \quad (8)$$

となる。

また

$$\Psi(x) = (y_0 - z_0\sqrt{\beta_k})\, x^m + (y_1 - z_1\sqrt{\beta_k})\, x^{m-1} + \cdots + (y_m - z_m\sqrt{\beta_k})$$

もK$_1$における多項式である。

ここで、２つの多項式の積Φ（ｘ）Ψ（ｘ）を計算すると

$$\Phi(x)\Psi(x)=(y_0x^m+y_1x^{m-1}+\cdots+y_m)^2$$
$$-\beta_n(z_0x^m+z_1x^{m-1}+\cdots+z_m)^2$$

はK$_{1-1}$における２ｍ次多項式とわかる。

これをＣにおける多項式とみると、ｇ（ｘ）とΦ（ｘ）Ψ（ｘ）は公約数Φ（ｘ）をもつので、命題５．７において、Ｋ＝K$_{1-1}$，ｆ（ｘ）＝Φ（ｘ）Ψ（ｘ）とおくと、’２ｍ次多項式Φ（ｘ）Ψ（ｘ）がｇ（ｘ）で割り切れる’という結論が得られるので

$$2m\geqq n \quad \text{----------} \quad (9)$$

となる。

したがって、（８），（９）式より２ｍ＝ｎとなり

$$\Phi(x)\Psi(x)=hg(x)\quad(h\in K_1)$$

と表すことができる。

ゆえに

$$g(x)=h^{-1}\Phi(x)\Psi(x)$$

となり、Φ（ｘ）は最低次数であることから、$h^{-1}\Psi(x)$はK$_1$における既約多項式となる。

次に、命題５．７，命題５．８をもとに、いよいよ正ｎ角形の作図を考えていく。

まず、ｐを素数として、正ｐ角形が作図できたとすると

$$z_1=\cos\frac{2\pi}{p}+i\sin\frac{2\pi}{p}$$

の実部，虚部が作図できる数となる。

$z_1\neq1$よりz_1は（６）式のｆ（ｘ）を用いるとｐ－１次方程式ｆ（ｘ）＝０の解である。

また、$z_1\notin Q$であるので、第１章命題１．７より次のことがいえる。

K$_0$＝Ｑとして、次の性質をもつ数体の系列K$_0$，K$_1$，K$_2$，・・・，K$_n$が存在する。

$K_1=K_0(\sqrt{\beta_1})$，$\beta_1=-1$

$K_2=K_1(\sqrt{\beta_2})$，$\beta_2\in K_1$，$\sqrt{\beta_2}\notin K_1$

$K_j=K_{j-1}(\sqrt{\beta_j})$，$\beta_j\in K_{j-1}$，$\sqrt{\beta_j}\notin K_{j-1}$

$z_1\notin K_{n-1}$，$z_1\in K_n$

すると、ｆ（ｘ）はK$_n$において$x-z_1$で割り切れて、商もK$_n$における多項式となる。

すなわち、命題５．６より、ｆ（ｘ）はK$_0$では既約、K$_n$では可約となるわけである。

そこで、この数体の系列をK$_0$，K$_1$，K$_2$，・・・の順に見ていくと、ｆ（ｘ）はK$_0$，

K_1，・・・，K_{g-1}では既約、K_gでは可約となるような番号ｇ（$1 \leqq g \leqq n$）が存在するはずである。

よって、命題５．８より

$p-1=2m$（mは自然数）

と表せて、ｆ（ｘ）はK_gにおける２つのｍ次既約多項式の積として、$\Phi_1(x)\,\Psi_1(x)$と因数分解される。

$m \geqq 2$のときは、$\Phi_1(z_1)=0$、又は$\Psi_1(z_1)=0$なので、前者が成り立つとすると、$\Phi_1(x)$はK_gでは既約，K_nでは可約なので、ｆ（ｘ）の場合と同様の議論より

$m=2m'$（m'は自然数）

を得る。

以下、$m' \geqq 2$のときは、同じ論法を続けていけば

$p-1=2^h$（ｈは自然数）

と表せることがわかる。

また、ｈが

$h=(2k+1)h'$（ｋ，ｈは自然数）

のように奇数の素因数をもっていると仮定すると

$x^{2k+1}+1=(x+1)(x^{2k}-x^{2k-1}+x^{2k-2}-\cdots-x+1)$

に$x=2^{h'}$を代入すると

$2^h+1=(2^{h'}+1)n$（ｎは整数）

となり、$n=1$のときは$h=h'$となり、$n \neq 1$のときは2^h+1が素数であることに矛盾する。

ゆえに

$h=2^l$（ｌは負でない整数）

と表せる。したがって、次の結論を得た。

命題５．９．　ｐが素数のとき、正ｐ角形が作図できれば

$p=2^h+1$（$h=2^l$，ｌは負でない整数）

と表すことができる。

素数ｐがこのような形をしているとき、これをフェルマー素数という。

例えば、$l=0$のとき$p=3$，$l=1$のとき$p=5$，$l=2$のとき$p=17$，$l=3$のとき$p=257$，$l=4$のとき$p=65537$となり、これらはすべて素数となっている。

しかし、$l=5$のとき

$p = 4294967297 = 641 \times 6700417$

となりフェルマー素数でないことがオイラーによって発見された。

現在、pが4万桁以下では、フェルマー素数は上記の5個しか見つかっていない。

定理5．10． pがフェルマー素数のとき、正p角形が作図できる

このことについては、ガウスによって証明されているが、ここでは省略させていただく。

尚、くわしい証明については、『初等幾何学作図問題』、窪田　忠彦著、内田老鶴圃新社を参照していただきたい。

［4］円の等分問題の解決

命題5．11． 自然数a，bの最大公約数をdとするとき

$xa - yb = d$ ---------- （10）

となる自然数x，yが存在する。

［証明］ $a \geqq b$として、a，bの最大公約数を互除法によって求めると次のようになる。

$a = q_1 b + r_1$ （q_1，r_1は自然数で、$0 \leqq r_1 < b$）

$b = q_2 r_1 + r_2$ （q_2，r_2は自然数で、$0 \leqq r_2 < r_1$）

$r_1 = q_3 r_2 + r_3$ （q_3，r_3は自然数で、$0 \leqq r_3 < r_2$）

$r_{k-2} = q_k r_{k-1} + r_k$ （q_k，r_kは自然数で、$0 \leqq r_k \leqq r_k$）

$r_{k-1} = q_{k+1} r_k$ （q_{k+1}は自然数）

このr_kがa，bの最大公約数となるので、$d = r_k$である。このとき

$r_1 = a - q_1 b$ ＝自然数×a－自然数×b

$r_2 = b - q_2 r_1$

＝b－q_2（自然数×a－自然数×b）

＝自然数×b－自然数×a

$r_3 = r_1 - q_3 r_2$

＝自然数×a－自然数×b－q_3（自然数×b－自然数×a）

＝自然数×a－自然数×b

のように続き、ｋが奇数のときは

ｄ＝自然数×ａ－自然数×ｂ

となり（１０）式が導かれる。

また、ｋが偶数のときは

ｄ＝自然数×ｂ－自然数×ａ

となるが、この式の右辺を変形して

ｄ＝（ｂｍ－自然数）×ａ－（ａｍ－自然数）×ｂ（ｍは自然数）

とすると、ｍを十分大きくとることによって、２つの（　）の中は正にすることができるので、やはり（１０）式が導かれる。

この命題において、ｄ＝１のとき、ａ，ｂは互いに素というわけである。

命題５．１２．　ａ，ｂが互いに素な自然数で、正ａ角形と正ｂ角形が作図できるとき、正ａｂ角形も作図できる。

［証明］ａ，ｂは互いに素なので、命題５．１１より

ｘａ－ｙｂ＝１　　----------（１１）

となる自然数ｘ，ｙが存在する。

ここで、正ａ角形が作図できるとき、２π／ａの角も作図できることに注目すれば、命題５．１２は、’２π／ａの角と２π／ｂの角が作図できるとき、２π／ａｂの角も作図できる’といいかえることができる。

（１１）式の両辺に２π／ａｂをかけると

$$\frac{2\pi}{b}x-\frac{2\pi}{a}y=\frac{2\pi}{ab}$$

となる。

２π／ａの角と２π／ｂの角が作図できるとき、２π／ｂのｘ倍の角，２π／ａのｙ倍の角が作図でき、その差も作図できる。（ただし、２πを超える角が出てきた場合は、２π未満の角に直して考える）

ゆえに、命題５．１２は証明された。

最後に、次の命題を考えていく。

命題５．１３．　ｐが素数のとき、正p^2角形は作図できない

第１節より、ｎ＝ｐ^{2}のとき、分円方程式は

$z^{p^2}-1=(z^p)^p-1=(z^p-1)\{(z^p)^{p-1}+(z^p)^{p-2}+\cdots+1\}=0$

と変形できるので、z_1は

$z^{p(p-1)}+z^{p(p-2)}+\cdots+z^p+1=0$ ---------- （１２）

の解となる。

ここで、少し原始ｎ乗根について触れておく。

定義５．１４． １のｎ乗根のうち

$$z_k=e^{\frac{2\pi k}{n}i} \quad (1\leqq k\leqq n-1)$$

と定めたとき、ｋとｎが互いに素となるものを１の原始ｎ乗根という。

特に、ｎが素数のとき、１以外の（ｐ－１）個の１のｐ乗根は、１の原始ｐ乗根である。

命題５．１５． $G(z)=z^{p(p-1)}+z^{p(p-2)}+\cdots+z^p+1$（ｐは素数）

はＱ上既約である。

［証明］ｆ（ｚ）を整係数の多項式で、ｆ（１）≡１（ｍｏｄｐ）であるとし、

$F_1(z)=f(z)\,f(z^2)\cdots f(z^p)$

$F_2(z)=f(z)\,f(z^2)\cdots f(z^p)\,f(z^{p+1})\cdots f(z^{p^2})$

$=A_0+A_1z+A_2z^2+\cdots$（A_0, A_1, A_2, ・・・は整数）

---------- （１３）

とし、１の原始ｐ乗根をα_1, α_2, ・・・, α_{p-1}, １の原始ｐ^{2}乗根をβ_1, β_2, ・・・, β_{p^2-p}とおく。

ところで、ｆ（ｚ）を整係数の多項式で、ｆ（１）≡１（ｍｏｄｐ）とし、

$\omega=\cos\frac{2\pi}{p}+i\sin\frac{2\pi}{p}$ とおき、次のように考える。

$F(z)=f(z)\,f(z^2)\cdots f(z^{p-1})$

$=A_0+A_1z+\cdots$（A_0, A_1, ・・・は整数） ---------- （１４）

とおき、ｚの代わりに１，ω，ω^2，・・・，ω^{p-1}を代入して辺々加えると$(\omega^1)^k$，$(\omega^2)^k$，・・・，$(\omega^{p-1})^k$は、$k\neq np$のとき、全体としてω，ω^2，・・・，ω^{p-1}に等しくなり、$k=np$のときは、すべて１となる。

また、$1+(\omega^1)^k+(\omega^2)^k+\cdots+(\omega^{p-1})^k=\begin{cases}0 & (k\neq np)\\ p & (k=np)\end{cases}$

であるから、（１４）式は

$f(1)^{p-1}+(p-1)\,f(\omega)\,f(\omega^2)\cdots f(\omega^{p-1})$

$=p(A_0+A_p+A_{2p}+\cdots)$

$\equiv 0 \pmod p$

と変形でき、

$(p-1)\,f(\omega)\,f(\omega^2)\cdots f(\omega^{p-1})\equiv -1 \pmod p$ --------（１５）

という関係式を得る。

１のp^2乗根をすべて（１３）式のｚに代入して、辺々加えると次のようになる。

$$\sum_{k=1}^{p^2-p} F_2(\beta_k)=\sum_{k=1}^{p^2-p} f(\beta_k)\,f(\beta_k^2)\cdots f(\beta_k^{p^2})$$

$$=(p^2-p)\,F_2(\beta_1)$$

$$\sum_{k=1}^{p-1} F_2(\alpha_k)=\sum_{k=1}^{p-1} f(\alpha_k)\,f(\alpha_k^2)\cdots f(\alpha_k^{p^2})$$

$$=(p-1)\,F_1(\alpha_1)^p$$

より

（１３）式の左辺$=(p^2-p)\,F_2(\beta_1)+(p-1)\,F_1(\alpha_1)^p+f(1)^{p^2}$

また、

（１３）式の右辺$=\sum A_k z^k \quad (k=0,\ 1,\ \cdots)$

$$=\sum A_k\left(1+\beta_1^k+\beta_1^{2k}+\cdots+\beta_1^{(p^2-1)k}\right)$$

で、$1+\beta_1^k+\beta_1^{2k}+\cdots+\beta_1^{(p^2-1)k}=\begin{cases}0 & (k\neq np^2)\\ p^2 & (k=np^2)\end{cases}$

より

（１３）式の右辺$=p^2(A_0+A_{p^2}+A_{2p^2}+\cdots)$

となる。

よって、

$(p^2-p)\,F_2(\beta_1)+(p-1)\,F_1(\alpha_1)^p+f(1)^{p^2}$

$=p^2(A_0+A_{p^2}+A_{2p^2}+\cdots)$

$\equiv 0 \pmod{p^2}$

となり

$(p^2-p)\,F_2(\beta_1)+(p-1)\,F_1(\alpha_1)^p+1\equiv 0 \pmod{p^2}$

---------- （１６）

という関係式を得る。

さて、G（x）が既約でなく、2つの整係数の多項式f（x），g（x）の積に分解されたとすると、G（x）＝0の根はすべて1の原始p^2乗根であって、f（x）＝0の根はその一部となるから

$f(\beta_1)\ f(\beta_2)\ f(\beta_3)\cdots f(\beta_{p^2-p})=0$

となる。

よって、（13）式より

$F_2(\beta_1)=0$

となり、これを（16）式に代入すると

$(p-1)F_1(\alpha_1)^p\equiv -1 \pmod{p^2}$ ---------- （17）

という関係式を得る。

（17）式の両辺に$(p-1)^{p-1}$をかけると

$(p-1)^pF_1(\alpha_1)^p\equiv(p-1)^{p-1}\equiv-(1+p) \pmod{p^2}$

となるので、$(p-1)F_1(\alpha_1)\equiv-1 \pmod{p}$を用いて上式の左辺を変形すると

$$\begin{aligned}(p-1)^pF_1(\alpha_1)^p&=\{(p-1)F_1(\alpha_1)\}^p\\&=\{-1+np\}^p\\&\equiv-1 \pmod{p^2}\end{aligned}$$

となる。よって

$-1\equiv-(1+p) \pmod{p^2}$

より

$p\equiv0 \pmod{p^2}$

となり矛盾する。

ゆえに、G（x）はQ上既約である。

命題5．16． K上既約多項式f（x）の零点が作図可能であるならば、f（x）の次数は2^m（mは自然数）である。

［証明］$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$（$a_0, a_1, \cdots, a_n\in K$）

とおき、f（x）は数体Kでは既約で、数体$K(\sqrt{\alpha})$（$\alpha\in K$）では可約であるとする。

この時、f（x）は

$f(x)=\{p(x)+q(x)\sqrt{\alpha}\}\{s(x)+t(x)\sqrt{\alpha}\}$（p（x），q（x），s（x），t（x）はKにおける多項式） ---------- （18）

と分解される。よって

$f(x)=\{p(x)s(x)+\alpha q(x)t(x)\}+\{p(x)t(x)+q(x)$

s（x）}$\sqrt{\alpha}$

となるが、f（x）はKにおける多項式なので

p（x）t（x）＋q（x）s（x）＝0　----------（19）

とならなければならない。

ここで、p（x），q（x）に共通因子があるとして

p（x）＝r（x）p'（x），q（x）＝r（x）q'（x）

とすれば

f（x）＝r（x）{p'（x）s（x）＋αq'（x）t（x）}

となりKにおける既約性に矛盾する。

したがって、p（x），q（x）は共通因子をもたない。

同様にして、s（x），t（x）も共通因子をもたないことがいえる。

そこで、（19）式を変形して

$$\frac{p(x)}{s(x)} = \frac{-q(x)}{t(x)} = c(x)$$

とおくと、c（x）はK（$\sqrt{\alpha}$）における多項式で

p（x）＝c（x）s（x），q（x）＝－c（x）t（x）

となる。

ところが、p（x）とq（x）は共通因子をもたないので、c（x）は一定数cでなければならない。

よって

p（x）＝cs（x），q（x）＝－ct（x）

となる。

そこで（18）式は

f（x）＝c{s（x）－t（x）$\sqrt{\alpha}$}{s（x）＋t（x）$\sqrt{\alpha}$}

----------（20）

と変形できるが、s（x）－t（x）$\sqrt{\alpha}$とs（x）＋t（x）$\sqrt{\alpha}$は次数が同じである。

したがって、f（x）の次数はその2倍である。

ところで

g（x）＝s（x）－t（x）$\sqrt{\alpha}$，h（x）＝s（x）＋t（x）$\sqrt{\alpha}$

はいずれも数体K（$\sqrt{\alpha}$）で既約である。

なぜなら、例えばh（x）が

s（x）＋t（x）$\sqrt{\alpha}$＝{u（x）＋v（x）$\sqrt{\alpha}$}{w（x）＋z（x）$\sqrt{\alpha}$}

（u（x），v（x），w（x），z（x）はKにおける多項式）

と分解されたとすると

s（x）＝u（x）w（x）＋αv（x）z（x），

$t(x)=u(x)z(x)+v(x)w(x)$

となる。

ここで

$\{u(x)-v(x)\sqrt{\alpha}\}\{w(x)-z(x)\sqrt{\alpha}\}$

$=\{u(x)w(x)+\alpha v(x)z(x)\}-\{u(x)z(x)+v(x)w(x)\}$

$=s(x)-t(x)\sqrt{\alpha}$

より（２０）式は

$f(x)=c\{s(x)-t(x)\sqrt{\alpha}\}\{s(x)+t(x)\sqrt{\alpha}\}$

$=c\{u(x)-v(x)\sqrt{\alpha}\}\{w(x)-z(x)\sqrt{\alpha}\}\{u(x)+v(x)\sqrt{\alpha}\}\{w(x)+z(x)\sqrt{\alpha}\}$

$=c\{u^2(x)-v^2(x)\alpha\}\{w^2(x)-z^2(x)\alpha\}$

と変形できる。

ところが、これはｆ（ｘ）が数体Ｋで既約であることに矛盾する。

したがって、ｇ（ｘ），ｈ（ｘ）はいずれも数体Ｋ（α）において既約となる。

ところで、ａをｆ（ｘ）の零点とすれば

ｇ（ａ）＝０、又はｈ（ａ）＝０

となる。

それが前者としてｇ（ｘ）に今の論法を適用すると、ｇ（ｘ）は数体Ｋ（$\sqrt{\alpha}$）に$\beta\in K(\sqrt{\alpha})$，$\sqrt{\beta}\notin K(\sqrt{\alpha})$であるような正の平方根$\sqrt{\beta}$を付加した数体において次数の等しい２つの多項式に分解される。

以下同様の議論を進めていくと、最後には１次の式に分解されるが、各々等しい次数の多項式に分解されることより、ｆ（ｘ）の次数は2^m（ｍは自然数）となることがわかる。

命題５．１５，命題５．１６を用いると、（１２）式は既約で、次数が２のべき乗ではないので、命題５．１３に取り上げた正p^2角形の作図不能性が証明された。

今までの議論をまとめると、正多角形の作図について次のような結論を得る。

定理５．１７　p_1，p_2，・・・，p_jが互いに異なるフェルマー素数ならば

$n=2^m p_1 p_2 \cdots p_j$（ｍは自然数）

として正ｎ角形が作図できる。

作図可能な正ｎ角形のｎの値の例をあげておくと次の通りである。

正３角形，４，５，６，８，１０，１２，１５，１６，１７，２０，２４，３０
３２，３４，・・・・・

参考文献

[１] *Salmon, G. (1885), Lessons introductory to the modern Higher Algebra, Hodges, Figgis, and Co. , Dublin.*

[２] *Van der Waerden, B. L. (1953), Modern Algebra (2vols.), Ungar, New York.*

[３] 羽鳥　裕久,「数学への誘い」, 培風館, *1995*

[４] 津田　丈夫,「不可能の証明」, 共立出版社, *1985*

[５] 草場　公邦,「ガロワと方程式」, 朝倉書店,*1989*

[６] Ｉ.スチュワート(永尾　汎監役, 新関　章三訳),「ガロアの理論」, 共立全書, *1979*

[７] 窪田　忠彦,「初等幾何学作図問題」, 内田老鶴圃新社, *1952*