作図できる数，できない数

志甫　淳

1　はじめに

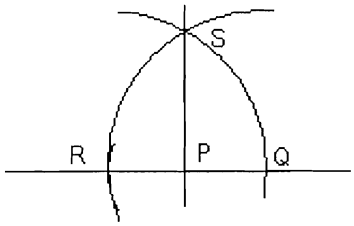
本稿では定規とコンパスによる作図問題について，特に正多角形の作図および三大作図問題についての解説を行います．作図問題についての解説は代数学関係の多くの教科書で既になされていますので私が新しいアイデアを加える余地はほとんどないのですが，なんとか私なりの解説を目指したいと思います．なお，本稿は2002年11月16日に東京大学大学院数理科学研究科において行われた公開講座「数のいろいろ　—定規とコンパスからガロアの理論まで—」での私の講演をベースにして書かれたものです．(講演では4節までの内容と5～7節の内容の一部を話しました．)

2　作図問題

(定規とコンパスによる) 作図問題とは，平面上に (例えば紙の上に) いくつかの点が最初に与えられている時に，それらから定規とコンパスのみを有限回用いることにより求めたい点あるいは図形の作図が可能であるかどうか判定せよ (あるいは可能であればその作図法を示せ) という問題である．まず肩慣らしとして (あとで用いる) 次の問題を考えてみよう．

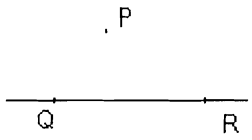
問題 2.1. 直線 PQ が与えられている時，点 P を通り直線 PQ に垂直な直線を作図せよ．

解答は例えば次の通りである：まず点 P を中心とし点 Q を通る円を描きこの円と直線 PQ との Q とは異なる交点を R とする．次に点 Q を中心とし点 R を通る円と点 R を中心とし点 Q を通る円を描き，2つの円の交点の一つを S とする．すると点 P と点 S を結んでできる直線が求めるものである (次頁の図参照)．

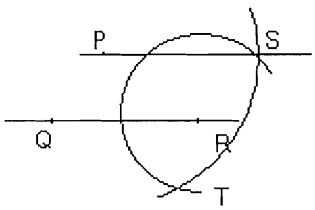


ではもう一題，あとで用いる次の作図問題を考えてみよう．

問題 2.2. 点 P と直線 QR が与えられているとする．点 P を通り直線 QR に平行な直線を作図せよ．



解答は例えば次の通りである：点 P を中心とし半径が線分 QR の長さと等しいような円と点 R を中心とし半径が線分 QP の長さと等しいような円を描き，その交点を S,T とすると，$PQRS$, $PQRT$ のいずれかは四角形をなしている．$PQRS$ が四角形をなしていれば直線 PS が求めるもので，$PQRT$ が四角形をなしていれば直線 PT が求めるものである (下図参照)．



以上は簡単な問題ではあるが，作図問題のパズル的な面白さの一端が窺えるかと思う．こういった面白さは昔の人も感じていたようで，このような作図問題は古代ギリシャの時代から考えられてきた．そして，古代ギリシャ時代以来の有名な問題に次のようなものがあった．

問題 2.3 (正多角形の作図問題). n を 3 以上の整数とするとき，正 n 角形の作図はどのような n に対して可能であるか？

問題 2.4 (三大作図問題). (1) 任意に与えられた角度を三等分する作図は常に可能であるか？

(2) ある立方体の一辺の長さが与えられている時に，その立方体の倍の体積をもつ立方体の一辺の長さを作図で求めることは可能であるか？

(3) ある円が与えられている時，その円と同じ面積をもつ正方形の作図は可能であるか？

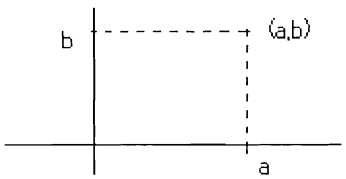
但し，上の問題文中の「作図」とは，定規とコンパスのみを有限回用いることによる作図という意味であることをここに再び書いておく．(実際，問題を述べる時にそのルールを正確に述べておくことは重要で，ルールを変えると答えが違ってくることはよくあることである．例えば将棋や囲碁でも，ルールを変更するとまるで違った遊戯になることであろう！)

これらの問題は非常に長い間数学者を悩ませてきた問題であったが，正多角形の作図問題はGaussによりある必要充分条件が与えられており，また三大作図問題に関しては19世紀末までに，どれも作図不可能であるということが証明されている．その証明の解説が本稿の目標である．

ある作図問題が与えられた時にそれが作図可能であることを示すには実際に作図する方法を与えれば充分であり，そこにはパズル的な面白さがあるであろう．しかしながら，それが作図不可能であることを示すにはどうすればよいのであろうか．作図不可能であることを示すには，(コンパスと定規による) どんな作図の方法を用いても求める作図問題の解答は得られない，ということを示さなければならない．そのために必要なことは，「コンパスと定規による作図の原理」を外側から分析する態度であり，そこにはパズル的な面白さとはまた違った面白さがあると筆者は思う．

3　作図できる数，できない数の観察

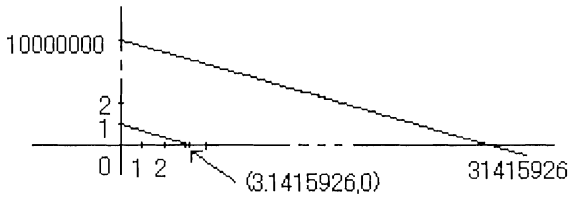
まず作図を行う平面に座標を入れてみる．すると，平面上の任意の点は実数の組 (a,b) で表されることになる (下図参照)．



これにより作図の問題を数を用いて書き表して分析することが可能となる．

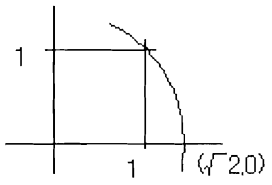
では，例として，最初に点 $(0,0),(1,0)$ のみが与えられているとして，どのような点が作図でき，どのような点が作図できないのかを観察してみよう．まず，$\pi = 3.14159265...$ を円周率とするとき，点 $(\pi,0)$ は実は作図できない点であることが今ではわかっている (９節と１０節を参照のこと)．しかし，点 $(\pi,0)$ に非常に近い点 $(3.1415926,0)$ は作図できる．その方法は例えば以下の通りである：まず最初に点 $(0,0),(1,0)$ が与えられているので x 軸 (この２点を結ぶ直線) は作図でき，また y 軸 (点 $(0,0)$ を通り x 軸に垂直な直線) を問題 2.1 の作図により作図することが出来る．次に点 $(1,0)$ を中心とする半径 $1(=(0,0)$ と $(1,0)$ を結ぶ線分の長さ) の円と x 軸の交点のひとつは点 $(2,0)$ となる．そして点 $(2,0)$ を中心とする半径１の円と x 軸の交点の一つは点 $(3,0)$

となる．これをずーっと繰り返すことにより，点 $(31415926, 0)$ を (いつかは) 作図できることになる．一方，点 $(0, 0)$ を中心とする半径 1 の円と y 軸の交点の一つとして点 $(0, 1)$ がとれる．そして点 $(0, 1)$ を中心とする半径 1 の円と y 軸の交点の一つとして点 $(0, 2)$ がとれる．これをまたずーっと繰り返すことにより点 $(0, 10000000)$ を作図することができる．そして問題 2.2 の作図により，点 $(0, 1)$ を通り，点 $(31415926, 0)$ と点 $(0, 10000000)$ を通る直線に平行な直線を作図し，その直線と x 軸との交点を考えるとそれが点 $(3.1415926, 0)$ になる (下図参照).



上の作図法では 40000000 回以上のステップが必要で (もっと少なくすることは可能ではあるが)，「これで作図できたといえるのか？」という疑問をもつ人がいるかも知れないが，「コンパスと定規を用いた有限回の作図」であることは間違いないので，(現実的な問題がどうであれ) 我々のルールから見ればこれは立派な作図である．また，「点 $(3.1415926, 0)$ は点 $(\pi, 0)$ に充分近いのだから，上の作図によって点 $(\pi, 0)$ が作図されたとみなしていいのではないか？」と思う人がいるかも知れないが，しかし我々のルールには充分近い点を同じとみなすといったルールはないのでそれは駄目だということも注意しておく．

さて，上に述べた点 $(3.1415926, 0)$ の作図と同様の方法により，a が有理数 $(=p/q\ (p, q$ は整数で $q \neq 0)$ と表される数) であれば，点 $(a, 0)$ を作図できることがわかる．では無理数 a に対して点 $(a, 0)$ は作図できないのか，と言われれば実はそうとも限らなくて，例えば $\sqrt{2}$ は有名な無理数であるが点 $(\sqrt{2}, 0)$ は作図できるということが次のようにしてわかる：x 軸および y 軸と点 $(1, 0), (0, 1)$ を作図し，次いで問題 2.1 を用いることにより $(0, 0), (1, 0), (1, 1), (0, 1)$ を頂点とする正方形を作図することができる．点 $(0, 0)$ を中心とし半径が $(0, 0)$ と $(1, 1)$ を結ぶ線分の長さ $(=\sqrt{2})$ であるような円と x 軸の交点を考えると，これが点 $(\sqrt{2}, 0)$ となる (下図参照).



このように，作図できる点と作図できない点との分布は(我々の眼からすると) 非常に複雑に見える．また，おぼろげながらではあるが，ある点が作図できるかどうかはその点の座標に現れる実数の性質を反映しているようだ，ということが窺える．

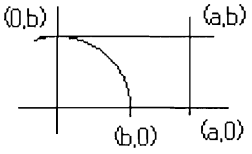
4　作図できる数の特徴づけ

ではどのような点が作図できるのかを調べていくことにしよう．作図の最初に点 $P_0, P_1, \cdots, P_n$ が与えられているとする．($n \geq 1$ とする．そうでないときは適当な点を付け加えて $n \geq 1$ の状況にもっていくことにする．) すると P_0 の座標が $(0,0)$, P_1 の座標が $(1,0)$ になるような座標がとれる．この状況で点 $P_i\,(2 \leq i \leq n)$ の座標を (a_i, b_i) とおく (a_i, b_i は実数)．問題 2.1 の作図を用いることにより座標軸は作図できることに注意しよう (前節参照)．従って座標軸を作図に利用することができる．まず最初に次の命題を示す：

命題 4.1. a, b を実数とするとき，点 (a,b) が作図できることと点 $(a,0), (b,0)$ が共に作図できることとは同値である．

証明．点 (a,b) が作図できると仮定すると，(a,b) を通り y 軸に平行な直線が問題 2.2 により作図できる．この直線と x 軸との交点が点 $(a,0)$ である．また (a,b) を通り x 軸に平行な直線が問題 2.2 により作図でき，この直線と y 軸との交点は $(0,b)$ となる．点 $(0,0)$ を通り半径 b(=点 $(0,0)$ と点 $(0,b)$ を結ぶ線分の長さ) の円と x 軸との交点が点 $(b,0)$ である．

一方，点 $(a,0), (b,0)$ が共に作図できると仮定する．この時，点 $(0,0)$ を通り半径 b(=点 $(0,0)$ と点 $(b,0)$ を結ぶ線分の長さ) の円と y 軸との交点として点 $(0,b)$ が作図できる．すると問題 2.1 を用いることにより，$(0,0), (a,0), (0,b)$ の 3 つが頂点であるような長方形が作図できる．この長方形のもう一つの頂点が点 (a,b) である．(下図参照)



□

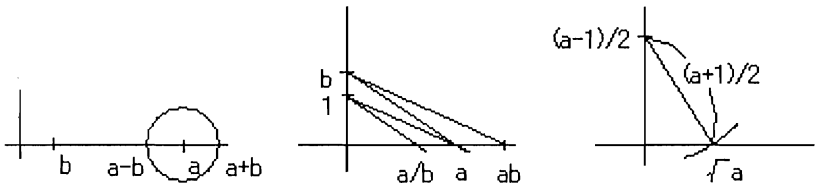
命題より，作図の問題においては $(a,0)$ という座標で表される点 (すなわち x 軸上にある点) が作図できるかどうかを議論すれば充分である．以下，実数 a に対して，「点 $(a,0)$ が作図できる」ということを単に「a は作図できる」あるいは「a は作図できる数である」と言うことにする．次の命題は，すでに作図できている数からある種の新しい数が作図できることを主張するものである：

命題 4.2. 実数a, bが作図できるとすると，$a+b, a-b, ab$も作図できる．$b \neq 0$であればa/bも作図できる．更にaが0以上の実数であるとき，$\sqrt{a}$も作図できる．

証明．まず点$(a,0)$を中心として半径b(=点$(0,0)$と点$(b,0)$を結ぶ線分の長さ)の円とx軸との交点として$(a+b,0),(a-b,0)$が作図できる．よって$a+b, a-b$は作図できる．

次に点$(0,0)$を中心として半径1(=点$(0,0)$と点$(1,0)$を結ぶ線分の長さ)の円とy軸との交点として$(0,1)$，半径bの円とy軸との交点として$(0,b)$が作図できる．この時，点$(0,b)$を通り点$(0,1)$と$(a,0)$を結んでできる直線に平行な直線を引くと，それとx軸との交点が$(ab,0)$となる．また点$(0,1)$を通り点$(0,b)$と$(a,0)$を結んでできる直線に平行な直線を引くと，それとx軸との交点が$(a/b,0)$となる．よって$ab, a/b$は作図できる．

最後に，0以上の実数aに対して$(a-1)/2, (a+1)/2$が作図できることが今までの結果からわかるので，点$(0,(a-1)/2)$を通り半径が$(a+1)/2$であるような円が作図できる．この円とx軸との交点の一つが$(\sqrt{a},0)$となることがピタゴラスの定理からわかる．従って$\sqrt{a}$も作図できる．



□

上の命題により次の定理が証明されたことになる．

定理 4.3. $0, 1, a_2, b_2, \cdots, a_n, b_n$から加減乗除および(0以上の実数の)平方根をとる操作を繰り返すことにより得られる実数は全て作図できる．

上の定理は「これこれの数は作図できる」というタイプの定理なので実際に作図法を挙げることにより証明がなされている(つまりパズル的な証明である)ということに注意しよう．

さて，実は作図できる数は上の定理で述べられている数に限ることもわかる．すなわち次が成り立つ：

定理 4.4. 作図できる数は$0, 1, a_2, b_2, \cdots, a_n, b_n$から加減乗除および(0以上の実数の)平方根をとる操作を繰り返すことにより得られる実数に限る．

この定理は「これこれ以外の数は作図できない」ということを主張しているのと同値なので，その証明には「コンパスと定規による作図の原理」を外側から分析する態度が必要であるということに注意しておく．

証明．ここでは，簡単に証明の方針のみを述べて，詳しい計算は読者に任せることにする．まず，定規とは直線を描く道具であり，直線の方程式は$ax+by+c=0$ (a,b,cは実数で$(a,b)\neq(0,0)$，定数倍で調節することによりcは0または1であるとしてよい) の形で表されていることを思い出そう．また，コンパスとは円を描く道具であり，円の方程式は$(x-p)^2+(y-q)^2=r$ (p,q,rは実数で$r\geq 0$) の形で表されていることを思い出そう．

さて，作図における操作とは次のいずれかである：

(1) すでに作図された2点$(x_1,y_1),(x_2,y_2)$を結ぶ直線を引く．

(2) すでに作図された点(x_0,y_0)を中心とし，すでに作図された2点(x_1,y_1), (x_2,y_2)の間の距離を半径とする円を描く．

(3) 描かれている直線あるいは円たちの交点を求める．

(1) で引かれる直線の方程式を$ax+by+c=0$とおくと，この直線が2点$(x_1,y_1),(x_2,y_2)$を通るという条件から，a,b,cが$0,1,x_1,y_1,x_2,y_2$から加減乗除を繰り返すことで得られる数であることがわかる．同様に，(2) で描かれる円の方程式を$(x-p)^2+(y-q)^2=r$とおくと，p,q,rはx_0,y_0,x_1,y_1,x_2,y_2から加減乗除を繰り返すことで得られる数であることがわかる．

次に (3) により新たに作図される点の座標について考える．異なる直線$ax+by+c=0$と$a'x+b'y+c'=0$が交点をもつとき交点の座標(x,y)はこの2つの一次式を連立させて解けば求められる．それは一次方程式を解くことに帰着されるので，x,yはa,b,c,a',b',c'から加減乗除を繰り返して得られる数である．次に異なる円$(x-p)^2+(y-q)^2=r$と$(x-p')^2+(y-q')^2=r'$が交点をもつとき，交点の座標(x,y)はこの2つの二次式を連立させて解けば求められ，それは二次方程式を解くことに帰着されることが計算によりわかる．二次方程式の解の公式には加減乗除と平方根を取る操作しか現れないので，結局交点の座標(x,y)はp,q,r,p',q',r'から加減乗除と平方根を取る操作の繰り返しで得られる数であることがわかる．また交点が存在する時は平方根記号の中の数は0以上であることもわかる．直線$ax+by+c=0$と円$(x-p)^2+(y-q)^2=r$が交点をもつときも同様の考察により，交点の座標(x,y)はa,b,c,p,q,rから加減乗除と(0以上の実数の)平方根を取る操作の繰り返しで得られる数であることがわかる．

以上の議論より，すでに作図されている点から (1) や (2) によって直線や円を描いて (3) により交点を求めることで新しく作図された点の座標は，既に作図されている数から加減乗除および(0以上の実数の)平方根をとる操作をくりかえすことにより得られることがわかる．従って作図される数は，作図の最初から与えられている点の座標に現れる数(つまり$0,1,a_2,b_2,\cdots,a_n,b_n$)から加減乗除および(0以上の実数の)平方根をとる操作をくりかえすことにより得られることがわかる．□

本節の２つの定理により作図できる数の特徴づけができたことになる．次節では定理 4.3 の応用として正多角形の作図の作図可能な場合についての Gauss の証明を紹介する．一方，作図不可能性の証明の為には定理 4.4 はまだ利用しやすい形になっているとはいえない．(加減乗除と平方根をとる操作の繰り返しで**書けないこと**を直接証明するのは困難である！) 定理 4.4 を利用しやすい形に書き換えるためには代数学における体 (たい) という概念を利用するのが便利である．そこで６節で体について説明し，そして７節では体を用いた定理 4.3,4.4 の言い換えを紹介する．

5　正多角形の作図 I — 作図可能な場合

この節では正多角形の作図問題について，作図可能な場合についての Gauss による証明 (を適宜書き換えたもの) を紹介する．正多角形の作図問題を座標を用いた形で改めて書くと例えば次のようになる．

問題 5.1 (正多角形の作図問題). n を 3 以上の整数とする．最初に点 $(0,0)$ と点 $(1,0)$ のみが与えられた時，点 $(0,0)$ を中心とする半径 1 の円に内接し点 $(1,0)$ を頂点の一つとする正 n 角形はどのような n について作図できるか？

注 5.2. 上の正 n 角形が作図できたならば例えば辺の長さが 1 の正 n 角形も作図できるので，本質的には上の問題を考えれば充分である．

$\alpha = 2\pi/n = 360^\circ/n$ とおく．上の問題文中の正 n 角形を作図するためには点 $(\cos\alpha, \sin\alpha)$ が作図できればよいが，$\sin\alpha = \sqrt{1-\cos^2\alpha}$ であることを用いれば $\cos\alpha$ が作図できれば充分であることがわかる．逆に文中の正 n 角形がもし作図できたならば $\cos\alpha$ は作図できる数であるから，結局正 n 角形の作図問題とは $\cos\alpha$ の作図問題である．本節の目標の定理は次の通りである．

定理 5.3. n が素数 p で $p-1$ が 2 のべきであるようなものの時，$\cos\alpha$ は作図できる数である．

この定理から，次のような結果が得られる．

系 5.4 (Gauss). n が

$$n = 2^s p_1 p_2 \cdots p_r$$

の形 (但しここで s は 0 以上の整数で，$p_1, \cdots, p_r$ は互いに異なる奇素数で $p_i - 1$ が 2 のべきであるようなもの，また $r = 0$ のときは s は 2 以上と仮定する) をしている時，正 n 角形の作図はできる．

まずは定理から系が導かれることを示そう．n が系の表示のような形をしているとして，まず $r \geq 1$ の時を考える．すると，定理から正 p_i 角形 $(1 \leq i \leq r)$ が作図できることがわかる．そして下で示す補題を用いれば正 $p_1 p_2 \cdots p_r$ 角

形が作図できることがわかる．更に与えられた角の二等分を作図することは可能であるから (これは有名な事実なので作図法は読者に任せることにする), それを繰り返すことにより正 $2^s p_1 p_2 \cdots p_r$ 角形, つまり正 n 角形が作図できることになる．$r = 0$ の時は角の二等分の作図のみを用いて正 2^s 角形すなわち正 n 角形が作図できる．これで系が示された．

上の議論で用いた補題を証明しておこう．

補題 5.5. $m_1, m_2, \cdots, m_r$ を 3 以上の整数でどの二つも互いに素であると仮定し，$m = m_1 m_2 \cdots m_r$ とおく．このとき正 m_i 角形 $(1 \leq i \leq r)$ が全て作図できるならば正 m 角形もまた作図できる．

証明．帰納法により $r = 2$ と仮定してよい．条件より $\cos(2\pi/m_i)\,(i = 1, 2)$ は作図でき，またもし $\cos x, \cos y$ が作図できるならば $\cos(x+y), \cos(x-y)$ が共に作図可能であることが (たとえば具体的作図あるいは三角関数の加法定理により) わかる．従って整数 s_1, s_2 で $s_1 m_1 + s_2 m_2 = 1$ を満たすものが存在すれば $s_2(2\pi/m_1) + s_1(2\pi/m_2) = 2\pi/m$ となるので $\cos(2\pi/m)$ が作図でき題意が言える．よって $s_1 m_1 + s_2 m_2 = 1$ を満たす整数 s_1, s_2 の存在を示せばよい．

これは有名な命題ではあるがここに証明を書いておく．$t_1 m_1 + t_2 m_2$ $(t_1, t_2$ は整数$)$ の形の数で正の整数になるようなもので最小なものを $d = t_1^* m_1 + t_2^* m_2$ とする．m_1 を d でわった商を q, 余りを $u\,(0 \leq u < d)$ とすると $u = (1 - qt_1^*)m_1 + (-qt_2^*)m_2$ であるから，もし $0 < u < d$ であるならばこの式は d の定義 (最小性) に矛盾する．よって $u = 0$ であり，つまり m_1 は d でわりきれる．同様に m_2 もまた d で割り切れることがわかるので d は m_1, m_2 の公約数となる．しかし m_1, m_2 は互いに素であったのだから $d = 1$ でなければならない．そこで $s_1 = t_1^*, s_2 = t_2^*$ とおけばよい．　□

それではいよいよ定理 5.3 の証明を紹介する．証明の方針は $\cos(l\alpha)$ の形の数 (l は整数) の適当な和を 2 次方程式を解いて求めてゆき，最後に $\cos\alpha$ を求めるに至る，というものである．p を奇素数で $p - 1 = 2^m$ であるとし，$\alpha = 2\pi/p$ とおく．この時整数 l に対して $\cos(l\alpha)$ は l を p で割った余りにしかよらない (つまり l, l' の p で割った余りが等しければ $\cos(l\alpha) = \cos(l'\alpha)$ である) ことに注意しよう．

以下，整数 a に対して a を p で割った時の余りを $\overline{a}$ とかくことにする．定理の証明のためには「p で割った余り」に関する初等整数論から少し準備することが必要である．

定義 5.6. p で割り切れない整数 a に対して $\overline{a^k} = \overline{1}$ となる最小の自然数 k を a の p を法とする位数という．

a を p で割り切れない整数，k を a の p を法とする位数とし，$p - 1$ を k で割った商を s, 余りを $t\,(0 \leq t < k)$ とする．初等整数論で有名な Fermat の小定理により $\overline{a^{p-1}} = \overline{1}$ が成り立つので $\overline{1} = \overline{a^{p-1}} = \overline{(a^k)^s a^t} = \overline{a^t}$ を得るが，

$0 < t < k$ とすればこの式は位数 k の定義 (最小性) に矛盾する．従って $t = 0$ であり，よって k は $p-1$ の約数である．以上より p で割り切れない整数 a の p を法とする位数は常に $p-1$ の約数であることがわかる．更に次の命題が成り立つ．

命題 5.7. p で割り切れない整数 r で p を法とする位数が丁度 $p-1$ になるものが存在する．

例えば $p = 5$ の時は $r = 2, 3$, $p = 17$ の時は $r = 3, 5$ などがその例である (各自確かめてみよ)．

証明．命題は任意の素数 p について正しいが，ここでは $p - 1 = 2^m$ となっている場合に限って証明する (定理 5.3 の証明のためにはこれで充分である)．まず任意の p で割り切れない整数 a の p を法とした位数は $p - 1 = 2^m$ の約数である (よって 2 のべきである) ことに注意しよう．さて p で割り切れない整数で p を法とする位数が最大であるようなもの (のひとつ) を r とし，その p を法とする位数を 2^k とする (k は m 以下の自然数)．この時，任意の p で割り切れない整数 x に対して $\overline{x} = \overline{r^i}$ となる整数 i $(0 \leq i \leq 2^k - 1)$ が存在することを x の p を法とする位数 $(2^l \ (l \leq k)$ とする) に関する帰納法で示す．$l = 0$ のときは $\overline{x} = \overline{1} = \overline{r^0}$ ゆえ明らか．また $l(\leq k)$ が一般の時は $\overline{x^{2^{l-1}}}, \overline{r^{2^{k-1}}}$ は共に $\overline{1}$ ではなくかつ 2 乗すれば $\overline{1}$ なので共に $\overline{-1}$ となることがわかり，従って $\overline{(xr^{2^{k-l}})^{2^{l-1}}} = \overline{x^{2^{l-1}} r^{2^{k-1}}} = \overline{1}$ である．従って $xr^{2^{k-l}}$ の p を法とする位数は 2^{l-1} 以下であり，よって帰納法の仮定から $\overline{xr^{2^{k-l}}} = \overline{r^j}$ なる $j\,(0 \leq j \leq 2^k - 1)$ が存在する．このとき $2^k - 2^{k-l} + j$ を 2^k で割った余りを i とおけば $\overline{x} = \overline{xr^{2^{k-l}} r^{2^k - 2^{k-l}}} = \overline{r^{2^k - 2^{k-l} + j}} = \overline{r^i}$ となる．

さて，上に示したことから集合 $\{\overline{1}, \cdots, \overline{p-1}\}$ は集合 $\{\overline{r^0}, \overline{r^1}, \cdots, \overline{r^{2^k-1}}\}$ に含まれていることになる．従って $p - 1 \leq 2^k$ がなりたつ．これと $p - 1 = 2^m, k \leq m$ であることから $k = m$ でなければならない．従って r の p を法とする位数は $2^m = p - 1$ である．　□

さて定理 5.3 の証明に戻ろう．命題 5.7 のような整数 r を一つとり固定する．そして $1 \leq k \leq m$ なる整数 k に対して $x_k = r^{2^{m-k}}$ とおく．(この時 x_k の p を法とする位数は丁度 2^k である．) そして p で割り切れない整数 a に対して実数 $S(a,k)$ を $S(a,k) = 2\sum_{i=1}^{2^{k-1}} \cos(ax_k^i \alpha)$ と定義する．$S(a,k)$ もまた a を p で割った余りにしかよっていないことに注意しよう．x_1 の p を法とする位数が丁度 2 であることから，$\overline{x_1} = \overline{-1}$ でなければならないことが容易にわかる．従って $S(1,1) = 2\cos(x_1\alpha) = 2\cos(-\alpha) = 2\cos\alpha$ である．よって $S(1,1)$ が作図できる数であることを示せばよいことになる．

$S(a,k)$ 達に関する計算を見通しよく行うために整数 l に対して $e(l) = e^{l\alpha\sqrt{-1}} = \cos(l\alpha) + \sqrt{-1}\sin(l\alpha)$ とおく．このとき $e(l)$ は l を p で割った余り

にしかよっておらず，$e(0)=1$ で，かつ整数 l,l' に対して $e(l+l')=e(l)e(l')$ が成り立つ．そして次の命題が成り立つ：

命題 5.8. (1) 等式 $S(a,k)=\sum_{i=1}^{2^k} e(ax_k^i)=\sum_{i=0}^{2^k-1} e(ax_k^i)$ が成り立つ．

(2) 任意の 0 以上 2^k 以下の整数 j に対して $S(ax_k^j,k)=S(a,k)$ である

(3) 任意の p で割り切れない整数 a に対して $S(a,m)=-1$ である．

証明．まず $2\cos(l\alpha)=e(l)+e(-l)$ であるが，x_k の p を法とする位数が丁度 2^k であることから $\overline{x_k^{2^{k-1}}}=\overline{-1}$ がなりたつことがわかり，従って $2\cos(l\alpha)=e(l)+e(lx_k^{2^{k-1}})$ である．従って

$$\begin{aligned} S(a,k) &= 2\sum_{i=1}^{2^{k-1}} \cos(ax_k^i\alpha) \\ &= \sum_{i=1}^{2^{k-1}} (e(ax_k^i)+e(ax_k^{i+2^{k-1}})) = \sum_{i=1}^{2^k} e(ax_k^i) \end{aligned}$$

である．また $\overline{x_k^{2^k}}=\overline{1}$ であることから $e(a)=e(ax_k^{2^k})$ なので $S(a,k)=\sum_{i=0}^{2^k-1} e(ax_k^i)$ でもある．これで (1) が言えた．

次に (2) を示す．$1\le i\le j$ の時 $e(x_k^i)=e(x_k^{2^k+i})=e(x_k^j x_k^{2^k-j+i})$，$j<i\le 2^k$ の時 $e(x_k^i)=e(x_k^j x_k^{i-j})$ であることから

$$\begin{aligned} S(a,k) &= \sum_{i=1}^{j} e(x_k^j x_k^{2^k-j+i}) + \sum_{i=j+1}^{2^k} e(x_k^j x_k^{i-j}) \\ &= \sum_{i=2^k-j+1}^{2^k} e(x_k^j x_k^i) + \sum_{i=1}^{2^k-j} e(x_k^j x_k^i) = S(ax_k^j,k) \end{aligned}$$

が成り立つ．これで (2) が言えた．最後に (3) を示す．そのためにまず任意の p で割り切れない整数 a に対して $2^m(=p-1)$ 個の数 $\overline{ar},\overline{ar^2},\overline{ar^3},\cdots,\overline{ar^{2^m}}$ は全て異なることに注意する．($\overline{ar^i}=\overline{ar^j}, 1\le i<j\le 2^m$ とすれば $\overline{r^{j-i}}=1$ となり r の p を法とする位数が $2^m-1=p-2$ 以下になってしまう)．従って集合 $\{\overline{ar},\overline{ar^2},\overline{ar^3},\cdots,\overline{ar^{2^m}}\}$ は集合 $\{\overline{1},\overline{2},\overline{3},\cdots,\overline{p-1}\}$ と等しい．すると集合 $\{e(ar),e(ar^2),e(ar^3),\cdots,e(ar^{2^m})\}$ は集合 $\{e(1),e(2),e(3),\cdots,e(p-1)\}$ と等しいことになるので

$$\begin{aligned} S(a,m) &= e(ar)+e(ar^2)+\cdots+e(ar^{2^m}) \\ &= e(1)+e(2)+\cdots+e(p-1) \end{aligned}$$

$$= (1 + e(1) + e(1)^2 + \cdots + e(1)^{p-1}) - 1$$
$$= \frac{e(1)^p - 1}{e(1) - 1} - 1 = \frac{e(p) - 1}{e(1) - 1} - 1 = -1$$

と計算される．これで (3) も言えた． □

命題より $S(a, m)$ は作図できる数であり，そして我々は $S(1, 1)$ が作図できることを示せばよいのであった．従って定理は次の命題から従う．

命題 5.9. a を p で割り切れない整数，k を $1 \leq k \leq m$ なる自然数とする．この時 $S(a, k)$ は 2 次方程式

$$t^2 - S(a, k+1)t + A = 0$$

(ここで A は $S(b, k+1)$ (b は p で割り切れない整数) 達のいくつかの和) の解となる．従って $S(a, k)$ は $S(b, k+1)$ (b は p で割り切れない整数) 達から加減乗除と (0 以上の実数の) 平方根をとる操作を繰り返すことで得られる数である．

証明．まず

$$\begin{aligned} S(a, k) + S(ax_{k+1}, k) &= \sum_{i=1}^{2^k} e(ax_k^i) + \sum_{i=0}^{2^k-1} e(ax_{k+1}x_k^i) \\ &= \sum_{i=1}^{2^k} e(ax_{k+1}^{2i}) + \sum_{i=0}^{2^k-1} e(ax_{k+1}^{2i+1}) \\ &= \sum_{i=1}^{2^{k+1}} e(ax_{k+1}^i) = S(a, k+1) \end{aligned}$$

が成り立つ．次に $S(a, k)S(ax_{k+1}, k)$ を計算する．まず

$$\begin{aligned} S(a, k)S(ax_{k+1}, k) &= \sum_{j=1}^{2^k} S(a, k)e(ax_{k+1}x_k^j) = \sum_{j=1}^{2^k} S(ax_k^j, k)e(ax_{k+1}x_k^j) \\ &= \sum_{j=1}^{2^k} (\sum_{i=1}^{2^k} e(ax_k^{i+j})e(ax_{k+1}x_k^j)) \\ &= \sum_{i=1}^{2^k} (\sum_{j=1}^{2^k} e(a(x_{k+1} + x_k^i)x_k^j)) = \sum_{i=1}^{2^k} S(a(x_{k+1} + x_k^i), k) \end{aligned}$$

$$= \sum_{i=1}^{2^{k-1}} (S(a(x_{k+1}+x_k^i),k) + S(a(x_{k+1}+x_k^{2^k+1-i}),k))$$

である．そして最後の式の各項は次のように計算される．

$$\begin{aligned}
&S(a(x_{k+1}+x_k^i),k) + S(a(x_{k+1}+x_k^{2^k+1-i}),k)\\
&= S(a(x_{k+1}+x_k^i),k) + S(a(x_{k+1}+x_k^{2^k+1-i})x_k^i,k)\\
&= \sum_{j=1}^{2^k} e(a(x_{k+1}+x_k^i)x_k^j) + \sum_{j=0}^{2^k-1} e(a(x_{k+1}+x_k^{2^k+1-i})x_k^{i+j})\\
&= \sum_{j=1}^{2^k} e(a(x_{k+1}+x_k^i)x_k^j) + \sum_{j=0}^{2^k-1} e(a(x_{k+1}x_k^{i+j}+x_k^{1+j}))\\
&= \sum_{j=1}^{2^k} e(a(x_{k+1}+x_k^i)x_k^j) + \sum_{j=0}^{2^k-1} e(a(x_{k+1}+x_k^i)x_{k+1}x_k^j)\\
&= \sum_{j=1}^{2^{k+1}} e(a(x_{k+1}+x_k^i)x_{k+1}^j) = S(a(x_{k+1}+x_k^i),k+1).
\end{aligned}$$

従って $S(a,k)S(ax_{k+1},k)$ は $S(b,k+1)$ と表される数のいくつかの和である．それを A とおくと，以上の計算から $S(a,k), S(ax_{k+1},k)$ は二次方程式 $t^2 - S(a,k+1)t + A = 0$ の二つの解であることがわかる．　□

以上で命題 5.9 が示されたので定理 5.3 の証明が完結した．

例 5.10. まず $p=5, r=2$ の時にどのような計算で $S(1,1) = 2\cos\alpha$ が求まっていったのかを見てみよう．まず $x_1 = 4, x_2 = 2$ と計算される．これを命題 5.9 の証明の中の計算結果に当てはめると

$$S(1,1)+S(2,1) = S(1,2) \overset{\text{命題 5.8(3)}}{=} -1, \quad S(1,1)S(2,1) = S(2+4,2) \overset{\text{命題 5.8(3)}}{=} -1$$

を得る．従って $S(1,1)$ は $t^2+t-1=0$ の解の一つである．具体的には $S(1,1) = \frac{-1+\sqrt{5}}{2}$ である．

例 5.11. 次に $p=17, r=3$ の時にどのような計算で $S(1,1) = 2\cos\alpha$ が求まっていったのかを見てみよう．まず次の表を用意しておくと非常に便利である．

この表から $\overline{x_1} = \overline{16}, \overline{x_2} = \overline{13}, \overline{x_3} = \overline{9}, \overline{x_4} = \overline{3}$ がわかる．さて，命題 5.9 の証明 (と $S(a,k)$ が a の p で割った余りにしかよらないこと) からまず

$$S(1,1)+S(13,1) = S(1,2), \quad S(1,1)S(13,1) = S(13+16,2) = S(12,2) = S(3,2)$$

l	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\overline{3^l}$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

がわかる．但し最後の等号は $S(12,2) \overset{\text{命題}\,5.8(2)}{=} S(12\cdot 13,2) = S(3,2)$ による．従って $S(1,1)$ は $t^2 - S(1,2)t + S(3,2) = 0 \cdots$① の解の一つである．次に

$$\begin{aligned} &S(1,2) + S(9,2) = S(1,3), \\ &S(1,2)S(9,2) = S(9+13,3) + S(9+13^2,3) = S(5,3) + S(8,3) \\ &\overset{(*)}{=} S(3,3) + S(1,3) = S(1,4) = -1 \end{aligned}$$

がわかる．但し等号 $(*)$ は $S(5,3) \overset{\text{命題}\,5.8(2)}{=} S(5\cdot 9^6,3) = S(3,3)$ および $S(8,3) \overset{\text{命題}\,5.8(2)}{=} S(8\cdot 9^3,3) = S(1,3)$ による．上の等式より $S(1,2)$ は $t^2 - S(1,3)t - 1 = 0 \cdots$② の解の一つである．更に

$$\begin{aligned} &S(3,2) + S(3\cdot 9,2) = S(3,3), \\ &S(3,2)S(3\cdot 9,2) = S(3(9+13),3) + S(3(9+13^2),3) = S(15,3) + S(7,3) \\ &\overset{(*)}{=} S(1,3) + S(3,3) = S(1,4) = -1 \end{aligned}$$

（等号 $(*)$ は $S(15,3) \overset{\text{命題}\,5.8(2)}{=} S(15\cdot 9^5,3) = S(1,3)$ および $S(7,3) \overset{\text{命題}\,5.8(2)}{=} S(8\cdot 9^3,3) = S(3,3)$ による）より，$S(3,2)$ は $t^2 - S(3,3)t - 1 = 0 \cdots$③ の解の一つである．最後に

$$S(1,3) + S(3,3) = S(1,4) = -1, \quad S(1,3) + S(3,3) = \sum_{i=1}^{4} S(3+9^i,4) = -4$$

より $S(1,3), S(3,3)$ は $t^2 + t - 4 = 0 \cdots$④ の二解である．従って④を解いて $S(1,3), S(3,3)$ を求め，次いで③を解いて $S(3,2)$，②を解いて $S(1,2)$ を求めて最後に①を解けば $S(1,1)$ を求めることができる．

さて，次の節へ進む前に定理に出てくるような素数（つまり $p-1$ が 2 のべきになるような素数）について補足する．もし p がこのような素数であったとすれば p は実は $2^{2^k}+1$（k はある 0 以上の整数）という形をしていなければならないことがわかる（各自証明してみよ）．そこで $F_k = 2^{2^k}+1$ とおこう．このとき $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ は全て素数になっている．（従って正 3 角形，正 5 角形，正 17 角形，正 257 角形，正 65537 角形は

作図可能である!) Fermat は F_k はどのような k についても素数となるであろうと予想したが，実はそれは正しくなかった：Euler により F_5 が

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641 \times 6700417$$

と因数分解されることが発見されたのである．そして $3, 5, 17, 257, 65537$ 以外に $2^{2^k}+1$ の形をした素数があるのかどうかは今でもわかっていない．従って正多角形の作図問題は原理的には Gauss により解決されたが，どのような正多角形が作図できるのか，という問いに対する最終的解答を我々はまだ得ていないのだ，とも言えるわけである．

6　体

この節以降はある種の作図問題が不可能であることを証明する方法について論じていきたい．この節では，そのために有用な概念である体 (たい) というものについて説明をおこなうが，紙面の都合もあり完全に証明をつけることは出来ないことをあらかじめ断っておく．

以下では，有理数全体のなす集合を $\mathbb{Q}$, 実数全体のなす集合を $\mathbb{R}$ とかく．また，複素数全体のなす集合 $\{a + b\sqrt{-1} \,|\, a, b \in \mathbb{R}\}$ を $\mathbb{C}$ とかく．このとき $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ となっている．さて，$\mathbb{C}$ においては加法，減法，乗法と 0 でない数による除法が定義されている．そして加減乗除の演算で $\mathbb{Q}$ や $\mathbb{R}$ は $\mathbb{C}$ のなかで閉じている．すなわち有理数 (実数) 同士の加法，減法，乗法，除法をした結果はやはり有理数 (実数) になる．こういった意味で $\mathbb{Q}$ や $\mathbb{R}$ は $\mathbb{C}$ という数の体系の「よい部分体系」をなしている．そこで，体という概念を次のように定義する．

定義 6.1. $0, 1$ を含む $\mathbb{C}$ の部分集合 F が体であるとは，F が加減乗除で閉じている (すなわち F に属する数同士の加法，減法，乗法，除法をした結果はやはり F に属している) こと．

注 6.2. ここで定義した体は正確には「$\mathbb{C}$ の部分体」と呼ばれるものであるが，本稿では単に体と呼ぶことにする．

定義より $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ は体である．また，集合 $\{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}$ は体になる：この集合は $0, 1$ を含む $\mathbb{C}$ の部分集合であり，また

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2},$$

$$(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2},$$

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2},$$

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}}=\frac{ac-2bd}{c^2-2d^2}+\frac{-ad+bc}{c^2-2d^2}\sqrt{2}$$

という計算によりこの集合は加減乗除で閉じていることがわかるからである．

体の存在については次の命題が基本的である．

命題 6.3. F を体として $a_1,...,a_n$ を複素数とする時，F および $\{a_1,\cdots,a_n\}$ を含む最小の体が存在する．(この体のことを以下では $F(a_1,\cdots,a_n)$ とかく．)

証明．K を「F に属する数および $a_1,\cdots,a_n$ から始めて加減乗除を繰り返すことにより得られる数全体の集合」とすると K は定義から $0,1$ を含み加減乗除で閉じているので体である．また K は F および $\{a_1,\cdots,a_n\}$ を含み，さらに F および $\{a_1,\cdots,a_n\}$ を含む体は K を含まなければならないのでこの K が求める体である．□

命題中で定義された記法を用いると，集合 $\{a+b\sqrt{2}\,|\,a,b\in\mathbb{Q}\}$ は $\mathbb{Q}(\sqrt{2})$ と書き表されることがわかる (各自確かめよ)．

F_1,F_2 を体とし，$F_1\subseteq F_2$ が成り立つとするとき，「F_2 が F_1 の何倍の大きさであるか」を表す量である拡大次数 $[F_2:F_1]$ を定義したい．そのためにまず基底という概念を定義する．

定義 6.4. F_1,F_2 を体とし，$F_1\subseteq F_2$ が成り立つとする．F_2 に属する有限個の数からなる集合 $\{a_1,a_2,\cdots,a_n\}$ が F_2 の F_1 上の基底であるとは，F_2 に属する任意の数が $c_1a_1+c_2a_2+\cdots c_na_n\quad(c_1,c_2,\cdots,c_n\in F_1)$ の形に一意的に書けること．

$\mathbb{Q}(\sqrt{2})$ に属する任意の数は $a+b\sqrt{2}\,(a,b\in\mathbb{Q})$ の形に書け，またこの形の表示が一意的であることが $\sqrt{2}$ が有理数でないことを用いてわかる．従って $\{1,\sqrt{2}\}$ は $\mathbb{Q}(\sqrt{2})$ の $\mathbb{Q}$ 上の基底である．同様の議論により，$\{1,\sqrt{-1}\}$ が $\mathbb{C}$ の $\mathbb{R}$ 上の基底であることもわかる．

さて，今みたように $\{1,\sqrt{2}\}$ は $\mathbb{Q}(\sqrt{2})$ の $\mathbb{Q}$ 上の基底であるが，例えば $\{1,1-\sqrt{2}\}$ もまた $\mathbb{Q}(\sqrt{2})$ の $\mathbb{Q}$ 上の基底であることが同様の議論でわかる．つまり基底が存在するとしても，基底のとりかたは一通りではない．しかし，どのような基底をとってきても基底に属する数の個数は一定であることを示すのが次の命題である．(証明は省略する．)

命題 6.5. F_1,F_2 を $F_1\subseteq F_2$ を満たす体とし，また $\{a_1,a_2,\cdots,a_n\},\{b_1,b_2,\cdots,b_m\}$ が共に F_2 の F_1 上の基底であるとする．このとき $n=m$ である．

基底の概念を用いて拡大次数を次のように定義する．

定義 6.6. F_1,F_2 を体とし，$F_1\subseteq F_2$ が成り立つとする．この時拡大次数 $[F_2:F_1]$ を次のように定義する：F_2 の F_1 上の基底 $\{a_1,\cdots,a_n\}$ が存在するときは $[F_2:F_1]=n$ と定義する．F_2 の F_1 上の基底が存在しないときは $[F_2:F_1]=\infty$ と定義する．

命題 6.5 により，拡大次数は，それを定義する際の基底 $\{a_1, \cdots, a_n\}$ の取り方によらないことに注意しよう．以前の議論により例えば $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $[\mathbb{C} : \mathbb{R}] = 2$ であることがわかる．また $F_1 \subseteq F_2$ を体とする時，$F_1 = F_2$ であることと拡大次数 $[F_2 : F_1]$ が 1 であることとは同値であることもわかる (各自確かめてみよ)．

次の命題は拡大次数についての基本的かつとても重要な性質である．

命題 6.7. F_1, F_2, F_3 が体で $F_1 \subseteq F_2 \subseteq F_3$ が成り立つとすると $[F_3 : F_1] = [F_3 : F_2][F_2 : F_1]$ が成り立つ．(但し 1 以上の自然数と ∞ あるいは ∞ と ∞ の積は ∞ であるとする．)

証明．ここでは $[F_2 : F_1], [F_3 : F_2]$ が共に有限な場合だけ証明することにする．$n = [F_2 : F_1], m = [F_3 : F_2]$ とすると，拡大次数の定義よりある F_2 の F_1 上の基底 $\{a_1, \cdots, a_n\}$ とある F_3 の F_2 上の基底 $\{b_1, \cdots, b_m\}$ が存在する．この時，x を任意の F_3 に属する数とすると $x = \sum_{i=1}^{m} c_i b_i$ を満たす $c_i \in F_2\,(1 \leq i \leq m)$ が存在する．そして各 c_i に対して $c_i = \sum_{j=1}^{n} d_{ij} a_j$ を満たす $d_{ij} \in F_1\,(1 \leq j \leq n)$ が存在する．この 2 式より $x = \sum_{i=1}^{m} \sum_{j=1}^{n} d_{ij} b_i a_j$ が成り立つ．そして c_i 達 $(1 \leq i \leq m)$ は x から一意的に定まり，また各 i に対して d_{ij} 達 $(1 \leq j \leq n)$ は c_i から一意的に定まる．従って d_{ij} 達 $(1 \leq i \leq m, 1 \leq j \leq n)$ は x から一意的に定まる．以上の議論より $\{b_i a_j\}_{1 \leq i \leq m, 1 \leq j \leq n}$ が F_3 の F_1 上の基底であることがわかる．従って $[F_3 : F_1] = mn$ であり，これで命題が証明された．□

F を体，α を複素数とするとき，拡大次数 $[F(\alpha) : F]$ は α と F との関係により決まる．それを説明するためにいくつかの言葉を導入しよう．まず，(一変数) 多項式とは変数 t についての

$$a_n t^n + a_{n-1} t^{n-1} + \cdots a_1 t + a_0$$

(ここで $a_0, \cdots a_n$ は複素数で $a_n \neq 0$) の形の式のことである．n のことをこの多項式の次数という．$\mathbb{C}$ の部分集合 S に対して多項式が S 係数であるとは全ての $a_i\,(0 \leq i \leq n)$ が S に属しているという意味である．F を体とする時，F 係数の次数 n の多項式 $f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots a_1 t + a_0$ が F 上可約であるとは

$$f(t) = (b_k t^k + b_{k-1} t^{k-1} + \cdots + b_0)(c_l t^l + c_{l-1} t^{l-1} + \cdots + c_0)$$

(但しここで $1 \leq k, l < n, k + l = n$ で b_i, c_i は全て F に属する) と書き表わすことができる (即ち F 係数の多項式としての因数分解ができる) ことであり，$f(t)$ が F 上既約であるとは，このような書き表し方ができないことである．$f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots a_1 t + a_0$ を多項式，α を複素数とするとき，多項式の t のところに α を代入することにより複素数 $a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots a_1 \alpha + a_0$

が得られるが，これを $f(\alpha)$ とかくことにする．F を体，α を複素数とする時，α が F 上 n 次の代数的数であるとはある次数 n の既約な多項式 $f(t)$ で $f(\alpha)=0$ となるものが存在することである．ある自然数 n に対して F 上 n 次の代数的数であるような数を F 上代数的な数といい，そうでない数を F 上超越的な数という．以上の準備のもとで，次の命題が成立する．

命題 6.8. F を体，α を複素数とする時，次は同値である．

(1) α は F 上 n 次の代数的数である．

(2) 拡大次数 $[F(\alpha):F]$ は n である．

この命題の証明も紙面の都合上省略する．上の命題の 2 条件が成り立っている時は $F(\alpha)=\{a_{n-1}\alpha^{n-1}+\cdots+a_1\alpha+a_0 \,|\, a_i\in F\}$ となっており，また $\{1,\alpha,\cdots,\alpha^{n-1}\}$ は $F(\alpha)$ の F 上の基底となっている．

例 6.9. F を体，$a\in F$ とする．このとき $f(t)=t^2-a$ とおくと $f(t)$ は F 係数の 2 次多項式で $f(\sqrt{a})=0$ である．もし $f(t)$ が F 上既約であれば上の命題により $[F(\sqrt{a}):F]=2$ である．一方，もし $f(t)$ が F 上可約であるとすれば $f(t)$ は F 係数の多項式として $f(t)=(t-\sqrt{a})(t+\sqrt{a})$ と因数分解されなければならず，従って $\sqrt{a}\in F$ となる．よって $[F(\sqrt{a}):F]=1$ である．

上の命題や例から窺えるように，体の拡大次数を計算するためにはある多項式が既約であるかどうかを判定することがしばしば重要になる．そのような判定は一般には容易ではないが，特別な形のものに対しては次のような判定条件が知られている．(この命題の証明も省略する．)

命題 6.10 (Eisenstein の既約性判定条件). p を素数とする．$f(t)=t^n+a_{n-1}t^{n-1}+\cdots+a_1t+a_0$ を整数係数の多項式とし，$a_i\,(0\le i\le n-1)$ は全て p で割り切れ，かつ a_0 は p^2 では割り切れないとする．この時 $f(t)$ は $\mathbb{Q}$ 上既約である．

7　体と作図できる数

この節では，前節で準備した体という概念を用いた作図できる数の特徴づけを与える．4 節のように，作図の最初に点 $P_0,P_1,\cdots,P_n$ が与えられているとし $(n\ge 1)$，P_0 の座標が $(0,0)$，P_1 の座標が $(1,0)$ になるような座標をとって，この状況で点 $P_i\,(2\le i\le n)$ の座標を (a_i,b_i) とおくことにする $(a_i,b_i$ は実数$)$．この節の主定理は次の通りである．(これが定理 4.3, 4.4 の体を用いた言い換えである．)

定理 7.1. $F=\mathbb{Q}(a_2,b_2,\cdots,a_n,b_n)$ とする．このとき，実数 a に対する次の二条件は同値である．

(1) a は作図できる数である．

(2) ある $\mathbb{R}$ に含まれる体の列 $F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_m$ で，$[F_i : F_{i-1}] = 2\,(1 \leq i \leq m)$ かつ $a \in F_m$ を満たすものが存在する．

証明．まず (1) を仮定して (2) を示す．a は作図できる数なので (定理 4.4 より) $0, 1, a_2, b_2, \cdots, a_n, b_n$ から加減乗除と (0 以上の実数の) 平方根をとる操作を繰り返すことにより得られる．ここで次の 3 つのことに注意する：

- $0, 1, a_2, b_2, \cdots, a_n, b_n$ は F に属する．
- K を体，x, y を K に属する数とすると $x+y, x-y, xy, x/y$ (最後の場合は $y \neq 0$ を仮定する) はやはり K に含まれる．
- K を $\mathbb{R}$ に含まれる体，x を K に属する正の実数とすると $[K(\sqrt{x}) : K]$ は 1 または 2 で，かつ $K(\sqrt{x})$ は再び $\mathbb{R}$ に含まれる．

最後のもの以外は定義から明らかである．最後の主張のうち，$[K(\sqrt{x}) : K]$ が 1 または 2 であることは例 6.9 で説明した．また K が $\mathbb{R}$ に含まれ，かつ $\sqrt{x}$ が実数であることから $K(\sqrt{x})$ もまた $\mathbb{R}$ に含まれることがわかる．さて，上に箇条書きした事柄から，a は，平方根をとる度に拡大次数 2 の拡大をしないといけないかも知れないが，しかしそうやって拡大を繰り返せばその拡大したある体に属していることがわかる．またその体は $\mathbb{R}$ に含まれているようにとれる．すなわち a は (2) の条件を満たすことになる．

次に (2) を仮定して (1) を m についての帰納法で示す．まず $m = 0$ のときは $a \in F$ である．F は $0, 1, a_2, b_2, \cdots, a_n, b_n$ から加減乗除を繰り返して得られる数全体のなす集合に他ならないので a は (1) の条件を満たすことになる．次に m が一般のときを考える．もし a が F_{m-1} に属していれば帰納法より a は作図できる数なので，a が F_{m-1} に属さない時を考えれば充分である．すると $F_{m-1} \subsetneq F_{m-1}(a)$ であるから拡大次数 $[F_{m-1}(a) : F_{m-1}]$ は 1 より大きい．一方体の列 $F_{m-1} \subseteq F_{m-1}(a) \subseteq F_m$ があることから $[F_m : F_{m-1}(a)][F_{m-1}(a) : F_{m-1}] = [F_m : F_{m-1}] = 2$ であり，従って $[F_{m-1}(a) : F_{m-1}]$ は 2 以下である．以上より $[F_{m-1}(a) : F_{m-1}] = 2$ であり，つまり a は F_{m-1} 上 2 次の代数的数である．従って a はある F_{m-1} 係数の 2 次方程式の解である．帰納法の仮定より F_{m-1} に属する数は作図できるから，それらから加減乗除および (0 以上の実数の) 平方根をとる操作により得られる数である a も (命題 4.2 より) また作図できることになる．つまり (1) の条件が成り立つ．　□

定理から次の系がいえる．これはある種の数が作図できないことを示すのに便利なものである．

系 7.2. F を上の定理の通りとする．実数 a が作図できる数であるとき，$[F(a) : F]$ は 2 のべきである．(特に a は F 上代数的である．)

証明．定理の (2) のような体の列 $F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_m$ をとる．すると $[F_m : F] = 2^m$ となる．一方 a は F_m に属するので $F \subseteq F(a) \subseteq F_m$ である．従って $[F_m : F(a)][F(a) : F] = [F_m : F] = 2^m$ であり，よって $[F(a) : F]$ は 2^m の約数である．従って $[F(a) : F]$ は 2 のべきである．　□

8　正多角形の作図 II — 作図不可能な場合

この節の目標は，5 節で述べた場合以外の n については，正 n 角形の作図が不可能であることを示すことである．再び問題 5.1 の状況に戻り，$\alpha = 2\pi/n$ とおこう．この節の主定理は次の通りである．

定理 8.1. n が $n = p^m$ (p は奇素数，m は 1 または 2) の形をしている時 $[\mathbb{Q}(\cos\alpha) : \mathbb{Q}] = p^{m-1}(p-1)/2$ である．

この定理から目標とする次の結果が得られる：

系 8.2 (Gauss). n が

$$n = 2^s p_1 p_2 \cdots p_r$$

の形 (但しここで s は 0 以上の整数で，$p_1, \cdots, p_r$ は互いに異なる奇素数で $p_i - 1$ が 2 のべきであるようなもの，$r = 0$ の時は $s \geq 2$ とする) をしていなければ正 n 角形は作図できない．

まず定理から系が導かれることを示そう．正 n 角形が作図できると仮定して，n が $n = 2^s p_1 p_2 \cdots p_r$ の形 (但しここで s は 0 以上の整数で，$p_1, \cdots, p_r$ は互いに異なる奇素数で $p_i - 1$ が 2 のべきであるようなもの，$r = 0$ の時は $s \geq 2$) をしていなければならないことを示せばよい．$n = 2^s p_1^{e_1} \cdots p_r^{e_r}$ を n の因数分解 (s は 0 以上，$e_1, \cdots, e_r$ は 1 以上の整数で $p_1, \cdots, p_r$ は互いに異なる奇素数,$r \geq 0$) とする．まず $r = 0$ の時は $s \geq 2$ でなければならない：そうでなければ n は 2 以下であり，作図問題が意味を持たないからである．従って $r = 0$ の時は題意が言えたので，以下では $r \geq 1$ と仮定する．さて正 n 角形が作図できるとすれば n の任意の 3 以上の約数 m に対して正 m 角形も作図できることに注意しよう．なぜなら正 n 角形の頂点を n/m 個ごとにつなげば正 m 角形になるからである．上の n の因数分解において，もしある $i (1 \leq i \leq r)$ に対して e_i が 2 以上であるならば正 p_i^2 角形が作図できなければならない．しかし定理より $[\mathbb{Q}(\cos(2\pi/p_i^2)) : \mathbb{Q}] = p_i(p_i - 1)/2$ でありこれは 2 のべきでない (p_i は奇数だから) ので矛盾．よって全ての i に対して $e_i = 1$ であり，更にこのとき正 p_i 角形が作図できることと $[\mathbb{Q}(\cos(2\pi/p_i)) : \mathbb{Q}] = (p_i - 1)/2$ であることから $p_i - 1$ は 2 のべきでなければならない．以上の議論から n は最初に述べた形をしていなければならないことになり，従って系が証明された．

では，定理 8.1 を証明しよう．整数 l に対して $e(l) := e^{l\alpha\sqrt{-1}} = \cos(l\alpha) + \sqrt{-1}\sin(l\alpha)$ とおく．まず次の命題に注意しよう．

命題 8.3. $e(1)$ は $\mathbb{Q}(\cos\alpha)$ 上 2 次の代数的数である．

証明．$2\cos\alpha = e(1)+e(-1)$ の両辺に $e(1)$ をかけて整理すれば $e(1)^2 - 2\cos\alpha\, e(1) + 1 = 0$ を得る．つまり $f(t) = t^2 - (2\cos\alpha)t + 1$ とおくと $f(e(1)) = 0$ である．また $f(t)$ は実数でない数 $e(1)$ を解にもつ 2 次式なので ($\mathbb{R}$ に含まれている)$\mathbb{Q}(\cos\alpha)$ 係数として因数分解されることはないことがわかる．従って $f(t)$ は既約であり，従って題意が言える． □

命題により $[\mathbb{Q}(e(1)) : \mathbb{Q}] = 2[\mathbb{Q}(\cos\alpha) : \mathbb{Q}]$ である．従って定理の (1) を証明するには $n = p^m$ (p は奇素数で m は 1 または 2) の時に $[\mathbb{Q}(e(1)) : \mathbb{Q}] = p^{m-1}(p-1)$ であることを証明すればよい．

まず $m = 1$ の時，$e(1) = e^{2\pi/p}$ は p 乗すれば 1 でかつそれ自身は 1 ではないので

$$f(t) = \frac{t^p - 1}{t - 1} = t^{p-1} + t^{p-2} + \cdots + 1$$

とおけば $f(e(1)) = 0$ である．よって $f(t)$ が $\mathbb{Q}$ 上既約であることを示せば $e(1)$ は $\mathbb{Q}$ 上 $(p-1)$ 次の代数的数となり $[\mathbb{Q}(e(1)) : \mathbb{Q}] = p-1$ が成り立つので定理 8.1(の $m = 1$ の場合) の証明が終わる．今 $g(s) = f(s+1)$ とおく．すると $g(s)$ が変数 s の多項式として $\mathbb{Q}$ 上既約であれば $f(t)$ も $\mathbb{Q}$ 上既約である．($f(t)$ が可約であればその因数分解に応じて $g(s)$ の因数分解がとれる．) ここで

$$g(s) = \frac{(s+1)^p - 1}{s} = \sum_{i=1}^{p} \binom{p}{i} s^{i-1}$$

であり (但し $\binom{p}{i}$ は二項係数)，これは二項係数の性質より Eisenstein の既約性判定条件の仮定を満たすので $\mathbb{Q}$ 上既約である．よって $m = 1$ の場合に定理 8.1 が証明できた．$m = 2$ の時は上の $f(t)$ の代わりに

$$f(t) = \frac{t^{p^2} - 1}{(t-1)(t^p - 1)} = t^{(p-1)p} + t^{(p-2)p} + \cdots + t^p + 1$$

とおくと同様の手法で $f(e(1)) = 0$ でありかつ $f(t)$ が $\mathbb{Q}$ 上既約であることが証明できる．従って $[\mathbb{Q}(e(1)) : \mathbb{Q}] = p(p-1)$ となり，定理 8.1 はこの場合にも証明された．

9　三大作図問題

この節では三大作図問題の不可能性の証明を紹介する．まずは問題を座標を用いた形で改めて書きなおしておこう．

問題 9.1 (三大作図問題). (1) 点 $(1,0),(0,0),(\cos\alpha,\sin\alpha)$ が与えられた時 (この三点のなす角が α となる)，点 $(\cos(\alpha/3),\sin(\alpha/3))$ をどのような実数 α に対しても作図することは可能であるか？

(2) 点 $(0,0),(1,0)$ が与えられている時，体積 2 の立方体の一辺の長さを作図すること，つまり 2 の 3 乗根を作図することは可能であるか？

(3) 点 $(0,0)$ を中心とし点 $(1,0)$ を通る円が与えられている時，その円と同じ面積をもつ正方形の一辺の作図，つまり $\sqrt{\pi}$ の作図は可能であるか？

この節では次の定理を証明する．

定理 9.2. 三大作図問題の作図は全て不可能である．

まず問題 (1) の不可能性を示そう．$\cos(\alpha/3)$ が作図できない数であるような実数 α が存在することを証明すればよい．それには $[\mathbb{Q}(\sin\alpha,\cos\alpha,\cos(\alpha/3)) : \mathbb{Q}(\sin\alpha,\cos\alpha)]$ が 2 のべきでないことを証明すればよい．まず 3 倍角の公式より $\cos\alpha$ は $\cos(\alpha/3)$ の多項式で書けるので $\mathbb{Q}(\sin\alpha,\cos\alpha,\cos(\alpha/3)) = \mathbb{Q}(\sin\alpha,\cos(\alpha/3))$ である．また $\sin\alpha=\sqrt{1-\cos^2\alpha}$ から $[\mathbb{Q}(\sin\alpha,\cos(\alpha/3)) : \mathbb{Q}(\cos(\alpha/3))]$, $[\mathbb{Q}(\sin\alpha,\cos\alpha) : \mathbb{Q}(\cos\alpha)]$ は共に 1 または 2 である．このことからある整数 a に対して

$$2^a[\mathbb{Q}(\sin\alpha,\cos(\alpha/3)) : \mathbb{Q}(\sin\alpha,\cos\alpha)] = [\mathbb{Q}(\cos(\alpha/3)) : \mathbb{Q}(\cos\alpha)]$$

がなりたつことがわかる．従って $[\mathbb{Q}(\cos(\alpha/3)) : \mathbb{Q}(\cos\alpha)]$ が 2 のべきでないような α が存在することを示せばよい．さて 3 倍角の公式 $\cos\alpha = 4\cos^3(\alpha/3) - 3\cos(\alpha/3)$ より，$f(t) = 4t^3 - 3t - \cos\alpha$ とおけばこれは $\mathbb{Q}(\cos\alpha)$ 係数の多項式で $f(\cos(\alpha/3)) = 0$ である．従ってある α に対して $f(t)$ が $\mathbb{Q}(\cos\alpha)$ 上既約であることが言えれば $[\mathbb{Q}(\cos(\alpha/3)) : \mathbb{Q}(\cos\alpha)] = 3$ となり，問題 (1) については定理が証明される．ここでは $\alpha = \pi/3$ の時 (この時 $\cos\alpha = 1/2$ である) に $f(t)$ が $\mathbb{Q}(\cos\alpha) = \mathbb{Q}$ 上既約であることを証明する．$g(s) = 2f(\frac{s+1}{2})$ とおくと ($\cos\alpha = 1/2$ を用いて) $g(s) = s^3 + 3s^2 - 3$ と計算され，これは Eisenstein の既約性判定条件 ($p = 3$ として用いる) より $\mathbb{Q}$ 上既約である．もし $f(t)$ が $\mathbb{Q}$ 上可約であるとすると $f(t)$ の因数分解に応じた $g(s)$ の因数分解がとれて矛盾なので $f(t)$ もまた $\mathbb{Q}$ 上既約となる．これで問題 (1) については定理が証明された．(なお $f(t)$ が $\mathbb{Q}(\cos\alpha)$ 上既約になるような $\alpha\,(0 < \alpha < 2\pi)$ は無限個存在することもわかる．その証明は各自に任せる．)

次に問題 (2) の不可能性を示す．α を 2 の 3 乗根とする．作図不可能性を示すには $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ が 2 のべきでないことを示せば充分であるが，$f(t) = t^3 - 2$ とおくと $f(\alpha) = 0$ であり，また Eisenstein の既約性判定条件 ($p = 2$ として用いる) から $f(t)$ は $\mathbb{Q}$ 上既約である．従って $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ である．よって問題 (2) について定理が証明された．

最後に問題 (3) の不可能性を示す．もし $\sqrt{\pi}$ が作図されたならば π も作図できることになるので，π が作図できないことを証明すれば充分である．さて，π が作図できるとすれば π は $\mathbb{Q}$ 上代数的な数でないといけないが，次節で紹介する Lindemann の定理により π は $\mathbb{Q}$ 上超越的な数である．従って π は作図できないので，問題 (3) についても定理が証明された．

10　π の超越性

この節では次の興味深い定理の証明の概略を紹介する．

定理 10.1 (Lindemann). π は $\mathbb{Q}$ 上超越的な数である．

証明のためには対称多項式についての結果が必要なのでまずはそれを簡単に紹介する．n 変数 $t_1, \cdots, t_n$ についての整数係数対称多項式とは $at_1^{d_1}t_2^{d_2}\cdots t_n^{d_n}$ (a は整数,d_i 達は 0 以上の整数) の形の式の有限和で書ける式 $f(t_1, t_2, \cdots, t_n)$ で，変数 $t_1, \cdots t_n$ のどのような並べ替え $(t_{i_1}, t_{i_2}, \cdots, t_{i_n})$ に対しても $(t_1, t_2, \cdots, t_n)$ の所に $(t_{i_1}, \cdots, t_{i_n})$ を代入した式 $f(t_{i_1}, t_{i_2}, \cdots, t_{i_n})$ が $f(t_1, \cdots, t_n)$ と一致するようなもののことである．その例として次に挙げる基本対称多項式がある：n 変数 $t_1, \cdots, t_n$ についての基本対称多項式とは

$$s_{n,1}(t_1, \cdots, t_n) = t_1 + \cdots + t_n,$$

$$s_{n,2}(t_1, \cdots, t_n) = \sum_{1 \le i_1 < i_2 \le n} t_{i_1}t_{i_2},$$

$$s_{n,3}(t_1, \cdots, t_n) = \sum_{1 \le i_1 < i_2 < i_3 \le n} t_{i_1}t_{i_2}t_{i_3},$$

$$\cdots$$

$$s_{n,n}(t_1, \cdots, t_n) = t_1 t_2 \cdots t_n,$$

の n 個の対称多項式のこと．この時次の定理が成り立つ (証明は省略する)．

定理 10.2 (対称多項式の基本定理). 任意の整数係数の対称多項式は基本対称多項式達から和差積を繰り返すことにより得られる式である．

それでは定理 10.1 の証明を始めよう．今 π が $\mathbb{Q}$ 上代数的な数であると仮定すると $\sqrt{-1}\pi$ もまた $\mathbb{Q}$ 上代数的な数になる．そこで $g(t)$ を $\mathbb{Q}$ 係数の多項式で $g(\sqrt{-1}\pi) = 0$ を満たすものとし，$g(t)$ の次数を d とする．また $g(t) = 0$ の解を $\theta_1 = \sqrt{-1}\pi, \theta_2, \cdots, \theta_d$ とおく．すると $e^{\sqrt{-1}\pi} + 1 = 0$ より $\prod_{i=1}^{d}(1 + e^{\theta_i}) = 0$ であり，これを展開して

$$\sum_{\delta_1, \cdots, \delta_d = 0}^{1} e^{\delta_1\theta_1 + \cdots + \delta_d\theta_d} = 0$$

を得る．2^d 個の数

$$\delta_1\theta_1 + \cdots \delta_d\theta_d \quad (\delta_1, \cdots, \delta_d \in \{0, 1\})$$

のうち 0 でないものを $\alpha_1, \alpha_2, \cdots, \alpha_n\,(n < 2^d)$ とし，また $q = 2^d - n$ とおく．この時次の補題が成り立つ：

補題 10.3. ある 0 でない整数 l で次を満たすものが存在する：「任意の n 変数整数係数対称多項式 $h(t_1, \cdots, t_n)$ に対して $h(l\alpha_1, \cdots, l\alpha_n)$ は整数となる.」

証明．ここでは証明の概略のみを述べる．まず任意の n 変数整数係数対称多項式 h に対してある d 変数整数係数対称多項式 k で任意の整数 l に対して $h(l\alpha_1, \cdots, l\alpha_n) = k(l\theta_1, \cdots, l\theta_d)$ を満たすものが存在することが α_i の定義からわかる．k は d 変数の基本対称多項式 $s_{d,1}, \cdots, s_{d,d}$ から和差積を繰り返して得られるが，$s_{d,i}(\theta_1, \cdots, \theta_d)$ は $g(t)$ の t^{d-i} の係数の $(-1)^i$ 倍に等しく $(g(t) = \prod_{i=1}^{d}(t - \theta_i)$ の右辺を展開すればわかる)，それは有理数である．従ってある整数 l で，任意の $i\,(1 \leq i \leq d)$ に対して $s_{d,i}(l\theta_1, \cdots, l\theta_d) = l^i s_{d,i}(\theta_1, \cdots, \theta_d)$ が整数になるようなものが存在する．すると $k(l\theta_1, \cdots, l\theta_d)$ はこれらの和差積で得られるので整数であり，従って $h(l\alpha_1, \cdots, l\alpha_n)$ も整数となる．これで題意が証明された．　□

定理 10.1 の証明に戻る．補題の条件を満たす l を一つとって固定し，多項式 $f(x)$ を

$$f(x) = l^{np}x^{p-1}(x - \alpha_1)^p \cdots (x - \alpha_n)^p$$

とおく．但し p は充分大きい素数である．$f(x)$ は次数 $m = np + p - 1$ の多項式である．さて $t \in \mathbb{C}$ に対して積分

$$I(t) = te^t \int_0^1 e^{-st} f(st) ds$$

を考える．部分積分を繰り返すことにより

$$I(t) = e^t \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(t)$$

と計算される．但し $f^{(j)}$ は f の j 階導関数である．$J = -(I(\alpha_1) + I(\alpha_2) + \cdots + I(\alpha_n))$ とおくと上の式から

$$J = q\sum_{j=0}^{m} f^{(j)}(0) + \sum_{j=0}^{m}(\sum_{i=1}^{n} f^{(j)}(\alpha_i))$$

と計算される．この式の右辺の各項の値を調べてみよう．

まず f の定義から $j \leq p-2$ の時 $f^{(j)}(0)=0$ であり，また $j \leq p-1$ の時 $\sum_{i=1}^{n} f^{(j)}(\alpha_i)=0$ であることがわかる．また $\xi(y)=\frac{y^{p-1}}{l^{p-1}}(y-l\alpha_1)^p\cdots(y-l\alpha_n)^p$ とおけば $l^{p-1}\xi(y)$ の係数は $l\alpha_1,\cdots,l\alpha_n$ の整数係数対称多項式なので整数である．このことから $l^{p-1}\xi^{(j)}(y)$ の係数は $j!$ で割り切れる整数であることがわかる．従って $j \geq p$ の時 $f^{(j)}(0)=l^j\xi^{(j)}(0)$ は $p!$ で割り切れる整数である．また $j \geq p$ の時は $\sum_{i=1}^{n} f^{(j)}(\alpha_i)=\sum_{i=1}^{n} l^j\xi^{(j)}(l\alpha_i)$ は係数が $p!$ の倍数であるような $l\alpha_1,\cdots,l\alpha_n$ に関する対称多項式なのでその値は $p!$ で割り切れる整数である．最後に残ったのは $f^{(p-1)}(0)=(p-1)!(l\alpha_1\cdots l\alpha_n)^p$ であるがこれは整数で $(p-1)!$ の倍数である．しかし p を充分大きくとっておけばこれは p では割り切れない．

以上の考察により，p が充分に大きければ J は 0 でない (p で割り切れないので!) 整数であり，かつ $(p-1)!$ の倍数であることがわかる．従って $|J| \geq (p-1)!\cdots$①である．一方積分の定義から $|I(t)| \leq |t|e^{2|t|}\max_{s\in[0,1]}|f(st)|$ であり，これを用いて $|J|<c^p\cdots$② (但し c は $l,\alpha_1,\cdots,\alpha_n$ のみによる定数) という形の不等式を得ることができる (計算は省略する)．p が充分大きい時不等式①, ②は同時には成立しないので矛盾を得る．従って π が $\mathbb{Q}$ 上超越的であることが言え，定理が証明される．

11　さいごに

５節の内容は文献 [1] を参考にしました．但し文献 [1] では Gauss はもっと一般的に理論を展開させた結果として証明を書いています．本稿では一般論を展開するのをなるべく避けるように証明をかなり書き換えました．また１０節の内容は文献 [2] を参考にしました．

References

[1] C.F.Gauss, Disquisitiones Arithmeticae (English Version, Translated by Arthur A. Clarke), Yale University Press, 1966.

[2] 塩川宇賢, 無理数と超越数, 森北出版, 1999.

（しほ　あつし，東京大学大学院数理科学研究科）