2005 年度蔵野ゼミ卒業論文
「角の三等分の作図が不可能であることを、高校生にもわかるように解説する試み」

明治大学理工学部数学科
阿部 海登
押味 優
川杉 正和
守法 孝浩
山口 絢子

平成 18 年 2 月 24 日

1　序

紀元前５世紀頃、ギリシアのデロス島で非常に恐ろしい伝染病が流行っていて、毎日何十人という人々がこの伝染病のために命を奪われていました。人間の力ではどうしてもこの伝染病を防ぐことができないと考えた島の人々は、デロス島の守護神であるアポロンの神霊にお伺いを立てたところ、

> 「祭壇の体積を立方体のままで二倍にせよ。然らば悪疫はたちどころに止むであろう」

という御神託を受けました。まず島の人々は一辺の長さが前の祭壇の２倍になるような祭壇を作ったのですが、悪疫は全く治まりませんでした。人々はこれを大いに怪しんだところ、ある学者が誤りを指摘しました。「一辺を２倍にしてしまったら、立方体の体積は８倍になってしまうではないか。神の欲せられる祭壇は８倍ではなくて２倍の体積であろう」と。人々は自分たちの間違いに気付き、今度はもとの祭壇と同じ祭壇を二つ並べて神前に置きました。しかしながら、これでも悪疫は止む様子がありません。困り果ててしまった人々は、アポロンの神の御神託をもう一度仰ぐことにしました。すると、

> 「汝等は確かに体積が２倍の祭壇を作った。しかしその形は立方体ではないではないか。余の望むものは体積が２倍であって、かつ立方体である祭壇であるぞ。」

というお告げを受けたそうです。人々はやっと御神託の意味が理解できたのです。しかし、どうしたら立方体のままで体積を２倍にできるか解りませんでした。そこで人々はこの問題を大学者プラトン[1]のところにもっていきました。プラトンは島の人々のためにと、この問題を熱心に研究しました。最初は定木とコンパスだけで解こうとしたのですが、どうしてもできません。プラトンとその弟子たちは、特殊な器械を使うことによってようやくこの問題を解くことができました。しかし、プラトンは

> 「そのような方法は、幾何学の美点を放棄し、破壊するものである。定木とコンパスだけで解くのが望ましい。」

と言ってさらに研究を続けたそうですが、ついに解くことはできませんでした。

そして定木とコンパスだけで体積が２倍の立方体を作図する問題が、未解決問題として残ったのです。この問題は、デロス問題とも呼ばれています。ギリシアの人々はこのデロス問題を含めた次の３つの問題 (ギリシアの三大作図問題) に興味を持っていたようです。

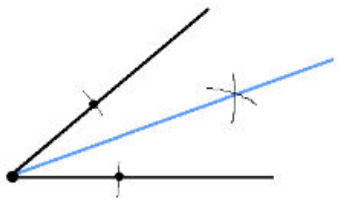
立方体倍積問題＝デロス問題 与えられた立方体の丁度２倍の体積を有する立方体を作れ。

円積問題 与えられた円と同じ面積を有する正方形を作れ。

角の三等分問題 任意に与えられた角を三等分せよ。

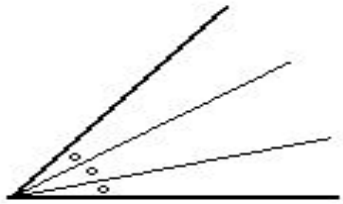
今回の卒論では、大学での専門的な数学を学んでない人を対象に、上の第３の問題である「角の三等分問題」について解説したいと思います。

定木とコンパスを使って「任意に与えられた角を二等分する」ことは容易にできます。



紀元前５，６世紀頃のギリシアの数学者達は、「任意に与えられた角を三等分せよ」、つまり、与えられた角を三等分する二本の半直線を作図せよ、

[1]プラトン：Platon, BC427–BC347, ギリシアの大哲学者



という問題を考え始めました。ところが、この問題はその外見上の簡潔さにもかかわらず、実に大きな困難を蔵していました。この問題に取り組んだ有名無名の学者は数知れないほどいたといわれています[2]。この問題に決定的な解答が与えられたのは、１９世紀に入ってからのことでした。それは、

> 「定木とコンパスを有限回用いる作図法によって、任意の角の三等分線を引くことは不可能である。」

というものでありました。つまり、「90° のように三等分線が引ける場合もあれば、60° のように三等分線が引けない場合もある」ということが、１８３７年にワンツェル[3]によって証明され、二千有余年かけてようやく完全に解決したのです。デロス問題もワンツェルによって、円積問題はリンデマン[4] によって、それぞれ不可能であることが証明されました。ギリシアの三大作図問題は否定的 (つまり、不可能である) ということは、ギリシア人たちも経験的には知っていたようです。

不可能であることが証明されているにもかかわらず、三等分線を作図する方法をいまだに考えている人々、三等分線の作図法を発見したと宣言している人々がいます。そのような人達は、三等分家 (Trisector) と呼ばれています。三等分家の特徴は、ほとんどが老人男性であり、角の三等分問題を若いときに幾何の授業で知り定年退職後に取り組んでいるそうです。しかし彼らは大体高校の範囲までしか数学を学んでいないので、何故「不可能」なのかが解っていないようで、実際その人達の論文は「不可能」を「可能」へと証明するものではなく、精度のよい「近似法」を書いているにすぎないようです[5]。

この卒論の目的は、角の三等分が何故不可能なのかを高校生にも解るように説明することにあります。

第２章では、定木とコンパスだけでは角の三等分は不可能ですが、特殊な道具を用いて、角の三等分線を引く方法があるので、その中のいくつかを紹介します。

[2] ド・モルガン (Augustus De Morgan, 1806–1871) の「角の三等分よりも、便箋を簡単に折り畳む方法を発明する方がよほど社会の役に立つ。」という言葉があるように、ギリシアの作図問題の数学的意味を疑問視する声もあったようです。

[3] ワンツェル：P.-L. Wantzel

[4] リンデマン：C. L. F. Lindemann

[5] 円積問題についても、ホッブズ (Thomas Hobbes, 政治哲学者, 1588–1679) が解を見つけたと公表し、数学者のジョン・ウォリス (John Wallis、イギリスの数学者、1616–1703) との長い泥沼の論争に発展した。彼は自分の解の誤りを認識できずに死ぬまで激しい論争を続けた。

第３章では、定木とコンパスで 60° が三等分可能な角であることを証明します。

第４章では、３章で使ったある定理の証明を解説します (ここまでは、高校生に説明することを目標とする) 。

第５章では、ガロア理論を使い「正 n 角形が作図可能である n は？」について考えます。(ここでは、大学で学んだ、群論・環論・体論を使う。)

注意 1.1 作図で使える道具とその使い方を説明します。

定木 一点とそれと異なる他の一点を結ぶ線分、半直線あるいは直線を引く[6]。

コンパス 与えられた一点を中心として、他の与えられた点を通る円を描く。

作図可能であるとは、「上記２つの操作を有限回用いてできる」を意味する。

2　特殊な道具を使った三等分

一般に、コンパスと定木を使えば任意の角度を２等分することができることは、小学校で習った。しかし、コンパスと定木だけでは、角の三等分線を作図することはできないことが、第３、４章で証明される。

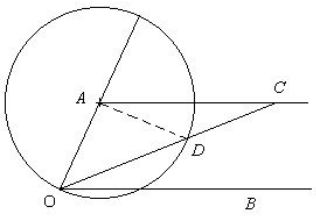
では、何かうまい道具を使って任意の角度を３等分する事ができないものか？この章では、特殊な道具を使った三等分線の作図法をいくつか紹介することにする。

2.1　２箇所に印のついた定規を使う方法

コンパスと２箇所に印のついた定規 (例えば 0, 1 というメモリ) を用いると、任意の角は容易に３等分する事ができる（アルキメデスの方法）。そのことを紹介する。

与えられた角を $\angle AOB$ とする。ここで OA は定規の印の付いた二点間の長さにとっておく。点 A を端点とし OB と平行な半直線を引く。また、A を中心として半径 OA の円を描く。

今、定規の 1 の印を点 A を端点とし OB と平行な半直線上、0 の印を円周上においたまま動かし、さらに点 O を通るような直線を引く。（ここで印のついた定規を使う）



[6]「定規」と書く場合、他に物差しとしての機能もあるため、ここでは「定木」とします。

このとき $OA = DA = DC$ であるから、$\triangle ADC$、$\triangle AOD$ は二等辺三角形であり、$\angle DCA = \angle DAC$, $\angle AOD = \angle ADO$ である。このとき、

$$\angle AOD = \angle ADO = \angle DCA + \angle DAC = 2\angle DCA$$

である。一方、錯角の関係から、

$$\angle BOC = \angle DCA$$

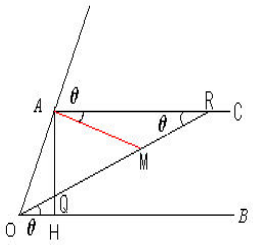
である。よって、

$$\angle AOB = \angle BOC + \angle AOD = \angle BOC + 2\angle BOC = 3\angle BOC$$

となる事から、OD は $\angle AOB$ の３等分線の一本であることがわかった。残りの一本の三等分線は、$\angle DOA$ の二等分線であるので、簡単に作図できる。

上と類似の方法として、次のものもある。

$\angle AOB$ を３等分したい。ここで、あらかじめ OA の長さは、定規の印の二点の距離の半分になるようにとっておく。下図のように A から OB 上に引いた垂線の足を H とする。A を通り OB と平行な半直線 AC を引く。定規を使って、O を通る直線で「AH、AC との交点をそれぞれ Q, R とする時、$QR = 2OA$ となる」をみたすものを引く。(つまり、QR は、印の付いた定規の二点の距離である。)



このとき、OR は、$\angle AOB$ の三等分線の一本である。実際、今 QR の中点を M としたとき、$\triangle MAR$ は二等辺三角形であるので、

$$AM = RM = OA$$

である。よって、

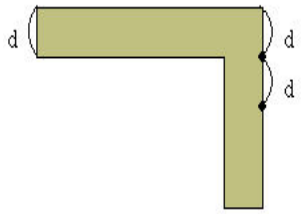
$$\angle AOM = \angle AMO = 2\angle MRA = 2\angle ROB$$

である。

2.2　L 字型定規 (カーペンター・スクエア)

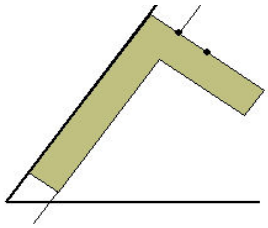
これは、上で示したアルキメデスの方法をもとにした、３等分した角を簡単に書くための方法である。手順は至って簡単であり、以下の様に作図すればよい。

1. まず下図のような L 字型定規を用意する。定規の幅を d とする。

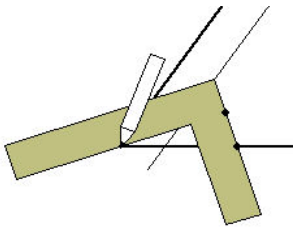


また、L 字型定規には、上の図のような二つの目盛りが付いているとする。

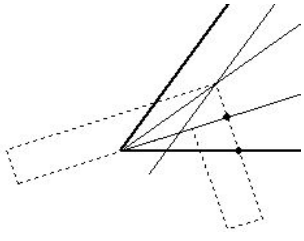
2. L 字型定規を用いて、与えられた角の一本の半直線と平行で距離が d の直線を引く。



3. 下図のように定規の外側の角が 2 で引いた平行線上に重なるように当て、さらに定規の外側の角から遠い方の印が３等分する角のもう一方の半直線上に重なるように置く。さらに、下図のように、L 字型定規の内側が角の頂点を通るように定規を置く。



4. 上図のように引いた線が角の３等分線になっている。

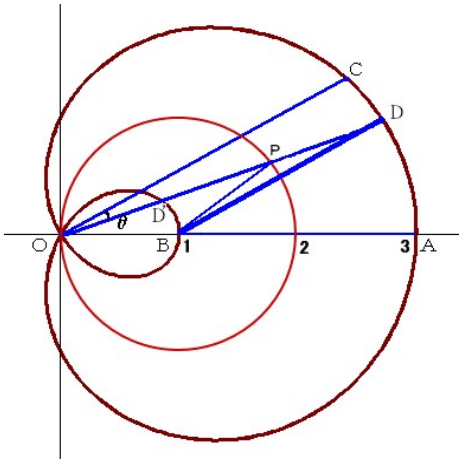


証明は、三つの合同な直角三角形を考えれば容易である。

2.3　適当な曲線を利用して角を三等分する方法

適当な曲線を用いることにより、与えられた角を三等分することが可能である。そのような方法としては、ニコメデス[7] のコンコイド (concoid)、ヒッピアス[8]の曲線、パスカル[9]のリマソン (蝸牛曲線) などが知られている。

ここでは、パスカルのリマソンを紹介しよう。



OB の長さを 1 として、B を中心にして半径 1 の円を書く (上の図の朱色の円)。次に点 O を通る直線を引き、この直線と円周のもう一つの交点を P とする。直線 OP 上にあり、点 P からの距離が 1 である点を D, D' をとる。このとき D と D' が描く軌跡がパスカルのリマソンとなる (上の図で、茶色の曲線がリマソンである)。

リマソンを用いて与えられた $\angle COB$ の 3 等分線を作図しよう。

B を通り OC と平行な直線を引く。点 D は、上の図のように、この直線とリマソンとの交点とする。このとき、線分 OD が $\angle COB$ の 3 等分線の一本となる。

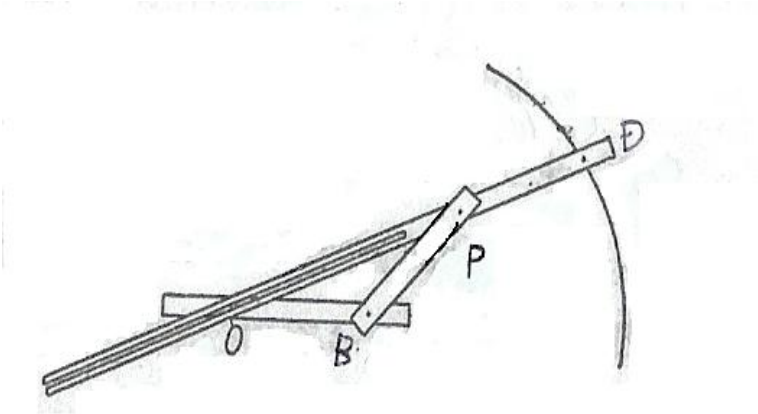
証明は容易である。今、直線 OC と直線 BD は平行であるので、$\angle POC = \angle PDB$ である。OD と最初の円との交点を P とする。リマソンの定義により、$PD = 1 = PB$ であるので、$\angle PDB = \angle PBD$ である。また、$BO = 1 = BP$ であるので、$\angle BOP = \angle BPO$ である。$\angle BPO = \angle PDB + \angle PBD$ であるので、

$$\angle BOP = 2\angle POC$$

であることがわかる。

パスカルのリマソンは、次のような単純な道具を用いて書くことができる。

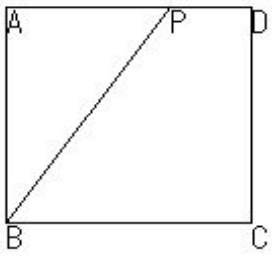
[7]Nicomedes, 西暦 180 年頃のギリシアの数学者
[8]Hippias, 紀元前 6 世紀後半–紀元前 5 世紀前半
[9]Blaise Pascal, 1623–1662, フランスの哲学者、数学者、物理学者



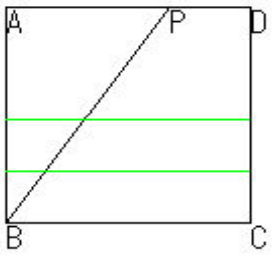
2.4　折り紙を用いて角を三等分する方法。

最後に、折り紙を使って、任意の角を 3 等分する方法を紹介する。
与えられた鋭角の 3 等分線をいかに引くかを見てみよう。

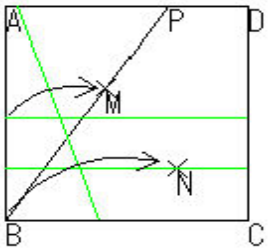
(1) 折り紙の 4 頂点を *A, B, C, D* とし、*AD* または *DC* 上に点 *P* をとる。
∠*PBC* を三等分したい。



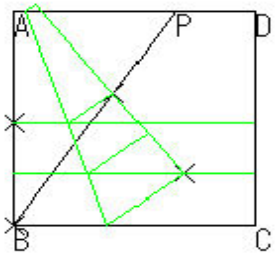
(2) 適当な幅で折り上げ *BC* に平行な 2 直線を折る。



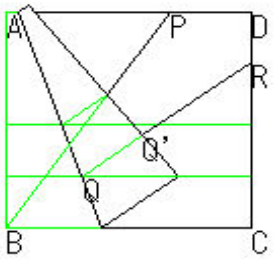
(3) 図のように 2 点を移動する。



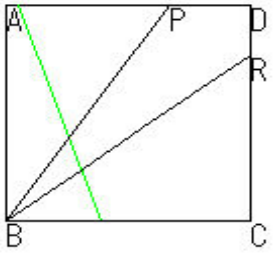
(4) 紙にたるみがないようにしてきちっと合わせる。



(5) QQ' を延長して、折り目 QR をつける。



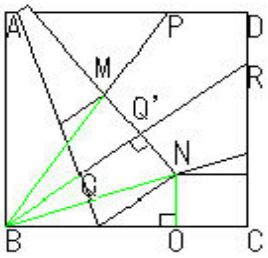
(6) (5) でつけた線 QR を延長して折り目をつけると、$\angle PBR$ が求める 3 等分線となる。



以下、簡単に理由を述べる。

まず、折り返した直線に対して、(2) で引いた 2 本の平行線のうちの下の線と、直線 QRは対称である。よって、直線 QR は B を通ることに注意。

下図において、3 つの三角形 $\triangle MBQ'$, $\triangle NBQ'$、$\triangle NBO$ が合同であることを証明すればよい。



$\triangle MBQ'$ と $\triangle NBQ'$ は直角三角形であり、$MQ' = NQ'$ であるので、この二つの三角形は合同である。$\triangle NBQ'$ と $\triangle NBO$ は直角三角形であり、$NQ' = NO$ であるので、この二つの三角形は合同である。よって $\triangle MBQ'$, $\triangle NBQ'$, $\triangle NBO$ は合同であるので、BQ', BN は $\angle PBC$ の 3 等分線であることが示された。

3　角の 3 等分が一般には不可能であること

この章では、定理 3.7 (第 4 章で証明する) を用いて、60° の 3 等分線はコンパスと定木では作図不可能であることを証明する。

その前に、前提となる知識を紹介する。まず、複素数と複素数平面を導入する。

複素数　$x^2 = -1$ を満たす x を $\pm i$ で表し、i を虚数単位と言う。複素数とは $x + yi$ という形（ただし、x, y は実数とする）で表されるものを言う。$y = 0$ なら、実数である。

複素数は、実数と同じように四則演算を持つ。例えば、

$$(a+bi)(c+di) = ac - bd + (ad+bc)i$$

となる。

複素数を表すとき、$z = x + yi$ と書くことが多い。このように書いたとき、x, y は実数であるとする。

複素数平面 複素数 $z = a + bi$ を座標平面上の点 (a, b) に対応させると、複素数全体と座標平面の点全体は１対１に対応する。このように複素数と座標平面上の点を対応させた時、この平面を **複素数平面** と言う。複素数 z に対応する点 P を単に z で表し、x 軸を **実軸**、y 軸を **虚軸** と言う。

複素数 $z = a + bi$ に対して、$\bar{z} = a - bi$ を z と共役な複素数という。$z = a + bi$ の絶対値を $\sqrt{a^2 + b^2}$ と定義し、$|z|$ で表す。複素数平面上では、絶対値は原点と点 z との距離を表している。次の関係式が成り立つ。z_1 及び z_2 は複素数とする。

$$z\bar{z} = |z|^2, \quad |z| = |-z| = |\bar{z}|$$

$$|z| = 0 \Leftrightarrow z = 0, \quad |z_1 z_2| = |z_1||z_2|, \quad \left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|}$$

複素数 $z = a + bi \neq 0$ を考える。複素数平面の原点を O と表す。複素数平面上で半直線 Oz と実軸の正方向とのなす角 θ を z の **偏角**（argument) といい、$\arg(z)$ と表す。$|z| = r$, $\arg(z) = \theta$ の時、$a = r\cos\theta$, $b = r\sin\theta$ なので、

$$z = r(\cos\theta + i\sin\theta), \quad r > 0$$

と表される。これを複素数 z の **極形式** と言う。

次に、複素数の四則演算が複素数平面上でどのような形で書けるのか見てみよう。$z_1 = a + bi$, $z_2 = c + di$ は複素数、k は実数としよう。

複素数の実数倍 $z \neq 0$ の時、原点 O と z、kz は同一直線上にある。$k > 0$ の時は、kz と z は O に関して同じ側にあり、$k < 0$ の時は、逆側にある。

複素数の加法 $z = z_1 + z_2$ の時、$z = (a+c)+(b+d)i$ であるから、四角形 Oz_1zz_2 は平行四辺形になる。

複素数の減法 $z = z_1 - z_2$ の時、$z = z_1 + (-z_2)$ と考えられるので、複素数の実数倍と加法から、$Oz_1z(-z_2)$ は平行四辺形になる。

複素数の乗法 $z = z_1 z_2$ の時、$|z| = |z_1||z_2|$, $\arg(z) = \arg(z_1) + \arg(z_2)$ である (三角関数の加法定理によって証明できる)。よって、z_1 に z_2 を掛ける事は、点 z_1 を O の周りに角 $\arg(z_2)$ だけ反時計回りに回転させ、O からの距離を $|z_2|$ 倍した点に移すことに相当する。

複素数の除法 $z = \frac{z_1}{z_2}$ の時、$|z| = \frac{|z_1|}{|z_2|}$ で $\arg(z) = \arg(z_1) - \arg(z_2)$ である。乗法と同じように、複素数平面での意味づけが可能である。($\frac{z_1}{z_2}$ は、$z_2 = 0$ の場合は考えない。)

例を挙げてみよう。

例 3.1 $z_1 = 1 + \sqrt{3}i, z_2 = 1 + i$ とする。この時、積は複素数平面上でどの位置にあるか？

それぞれを極形式表示すると
$z_1 = 2(\cos 60^\circ + i \sin 60^\circ), z_2 = \sqrt{2}(\cos 45^\circ + i \sin 45^\circ)$ となる。$z_1 z_2 = 2(\cos 60^\circ + i \sin 60^\circ)\sqrt{3}(\cos 45^\circ + i \sin 45^\circ) = 2\sqrt{3}(\cos 105^\circ + i \sin 105^\circ)$ となる。つまり、長さ $2\sqrt{3}$ で偏角は 105° になる。

最後に複素数における重要な定理を紹介する。

定理 3.2 (ド・モアブルの定理) 整数 n に対して、以下の式が成り立つ。

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

証明 n に関する帰納法で証明する。
$n = 1$ の時は明らか。
$n = k$ の時に定理が成立すると仮定する。すなわち、

$$(\cos\theta + i\sin\theta)^k = \cos k\theta + i \sin k\theta$$

が成り立つとしよう。

$$\begin{aligned}
& (\cos\theta + i\sin\theta)^{k+1} \\
= \ & (\cos\theta + i\sin\theta)^k(\cos\theta + i\sin\theta) \\
= \ & (\cos k\theta + i\sin k\theta)(\cos\theta + i\sin\theta) \\
= \ & \cos k\theta\cos\theta - \sin k\theta\sin\theta + i(\cos k\theta\sin\theta + \sin k\theta\cos\theta) \\
= \ & \cos(k+1)\theta + i\sin(k+1)\theta
\end{aligned}$$

よって、$n = k + 1$ の時も成り立つ。ゆえに、全ての自然数 n に対して、定理が成り立つ事が示された。

$n < 0$ の場合は、

$$(r(\cos\theta + i\sin\theta))^{-1} = r^{-1}(\cos(-\theta) + i\sin(-\theta))$$

より明らかである。 **証明終**

この定理を用いれば、複素数の累乗根が複素数平面上のどの位置にあるのか調べる事ができる。

注意 3.3 (複素数の平方根) ド・モアブルの定理を用いて、複素数の平方根が複素数平面のどの位置にあるのか見てみよう。

$z = a + bi$ の平方根を求めよう。この複素数の偏角を θ とし、$r = \sqrt{a^2 + b^2}$ とおく。すると、$z = r(\cos\theta + i\sin\theta)$ である。

求める平方根を $z_1 = s(\sin\alpha + i\cos\alpha)$ とおくと、定理によって

$$z_1^2 = s^2(\sin 2\alpha + i\cos 2\alpha)$$

となる。$z = z_1^2$ なので、r, s 及び α, θ の関係は

$$r = \sqrt{s},\ \alpha = \frac{\theta}{2} + n\pi$$

となる。

さて、これから本題に入る。まず**作図可能な数**とは何かを定義する。

定義 3.4 複素数平面において、

- 与えられた異なる 2 点を結ぶ直線を引く。
- 与えられた 1 点を中心として、他の与えられた一点を通る円を書く。

以上の操作を有限回繰り返して、求められる複素数を作図可能な複素数という。

複素数平面上で、点 0 と点 1 は予め与えられているとして考える。

注意 3.5 複素数 $z = x + yi$ が作図可能であるための必要十分条件は、その実部の実数 x と虚部の実数 y が作図可能であることである。

このことを見てみよう。

まず最初に、与えられている点 0, 1 により実軸を引く。次に、虚軸を引くことができる。

ここで、コンパスと定木を使って、与えられた一点を通り与えられた直線と直行する直線が引けることに注意。このことを使えば、与えられた一点を通り与えられた直線に平行な直線も作図できる。

z が作図可能とする。点 z を通り、虚軸に平行な直線を引く。その直線と実軸の交点が x であるので、x は作図可能である。同様にして yi は作図可能であり、コンパスを使って y が作図可能になる。

逆に、x と y が作図可能であるとする。すると、コンパスを使って yi が作図可能であり、長方形の作図法から、$z = x + yi$ が作図できる。

作図可能な複素数同士の四則演算の結果得られた数は作図可能なのだろうか？

$z_1 = a + bi$ と $z_2 = c + di$ は作図可能な複素数としよう。

作図可能な複素数の加法・減法の作図 $Oz_1(z_1+z_2)z_2$ は、平行四辺形である。よって、z_1 と z_2 の場所がわかれば、それを用いて z_1+z_2 が作図可能である。

z_2 がわかれば、コンパスと定木で $-z_2$ が作図可能である。このことより、z_1-z_2 が作図可能である。

作図可能な複素数の乗法・除法の作図 $z_1 = r_1(\cos\theta_1 + i\sin\theta_1)$, $z_2 = r_2(\cos\theta_2 + i\sin\theta_2)$ としよう。

単位円を書けば、単位円周上で偏角が θ_1, θ_2 の点は作図可能である。すると、偏角が $\theta_1+\theta_2$ の点も作図可能である。

また、O を中心として半径 Oz_1 の円を書けば、実数 r_1 は作図可能である。同様に r_2 も作図可能である。

r_1r_2 と r_1/r_2 が作図可能であることがわかれば、z_1z_2 と z_1/z_2 が作図可能であることがわかる。

i と r_2i は作図可能である。

r_1 と i を通る直線に平行で、r_2i を通る直線を引く。このとき、その直線と実軸との交点が r_1r_2 である。

r_1 と r_2i を通る直線に平行で、i を通る直線を引く。このとき、その直線と実軸との交点が r_1/r_2 である。

作図可能な複素数の平方根の作図 $z_1 = r_1(\cos\theta_1 + i\sin\theta_1)$ としよう。このとき、z_1 の平方根は、$z_3 = \sqrt{r_1}(\cos\frac{\theta_1}{2} + i\sin\frac{\theta_1}{2})$ と $-z_3 = \sqrt{r_1}(\cos(\frac{\theta_1}{2}+\pi) + i\sin(\frac{\theta_1}{2}+\pi))$ である。

z_3 が作図可能であることを示そう。

単位円を書けば、単位円周上で偏角が θ_1 の点は作図可能である。角の二等分線を引けば、偏角が $\frac{\theta_1}{2}$ の点も作図可能である。あとは、$\sqrt{r_1}$ が作図可能であればよい。

1 から、足し算と割り算で $\frac{1}{4}$ が作図可能である。よって、$r_1+\frac{1}{4}$ と $r_1-\frac{1}{4}$ が作図可能である。次に、$(r_1-\frac{1}{4})i$ を作図する。点 $(r_1-\frac{1}{4})i$ を中心にして、半径 $r_1+\frac{1}{4}$ の円を書く。このとき、実軸との交点に $\sqrt{r_1}$ が出てくる。

以上の考察から、複素数の四則演算及び平方根は作図可能で、それらを有限回行った複素数も作図可能である事が分かった。特に、全ての有理数は作図可能である。(0, 1 は、最初から与えられていることに注意。)

以下の定理を証明しよう。

定理 3.6 複素数 α が作図可能であるための必要十分条件は、α は有理数から有限回の四則演算とルートを使って表すことができることである。

証明 有理数から有限回の四則演算とルートを使って表すことができる複素数は作図可能であることは、すでに確かめた。

作図可能な数は、定義 3.4 のようにして書いた直線あるいは円によって、「直線と直線」、「直線と円」または「円と円」の交点として表れるはずである。0, 1 からスタートして、作図可能な複素数を連続的に見つけ出し、有限回の操作で複素数 α が見つかったとしよう。すると、作図可能な複素数の列

$$\alpha_0 = 0,\ \alpha_1 = 1,\ \alpha_2,\ \alpha_3,\ \alpha_4,\ \ldots,\ \alpha_n = \alpha$$

で、α_k は、$\alpha_1, \ldots, \alpha_{k-1}$ を用いて定義 3.4 のようにして書いた直線あるいは円によって、「直線と直線」、「直線と円」または「円と円」の交点として表れるはずである。

ここで、

T = 有理数から有限回の四則演算とルートを使って表すことができる複素数全体の集合

とする。$\alpha_0, \ldots, \alpha_{k-1}$ は T の元であると仮定して、$\alpha_k \in T$ を示すことができれば、数学的帰納法を用いて $\alpha_n = \alpha \in T$ が証明できることになる。

$\beta_1, \beta_2, \gamma_1, \gamma_2$ は T の元であると仮定し、

> C_i は、「β_i と γ_i を結ぶ直線」または「β_i を中心として、γ_i を通る円」とする。$(i = 1, 2)$

α は、C_1 と C_2 の交点とする。(ただし、$C_1 \neq C_2$ と仮定する。)

$\beta_1 \in T$ であるので、複素共役 $\overline{\beta_1}$ もそうである。よって、$\beta_1 = b_{11} + b_{12}i$ としたとき、b_{11}, b_{12} は T に入っている実数である。同様に $\beta_2 = b_{21} + b_{22}i$, $\gamma_1 = c_{11} + c_{12}i$, $\gamma_2 = c_{21} + c_{22}i$ とおくと、$b_{21}, b_{22}, c_{11}, c_{12}, c_{21}, c_{22}$ も T に入っている実数である。

ここで、$\alpha = a_1 + a_2 i$ とおく。点 (a_1, a_2) は、円や直線の交点であるので、a_1, a_2 は $b_{11}, b_{12}, b_{21}, b_{22}, c_{11}, c_{12}, c_{21}, c_{22}$ から有限回の四則演算とルートを使って表すことができる実数である。よって、$\alpha \in T$ である。 **証明終**

本論に入る。

全ての角の三等分線が、作図不可能であるわけではない。例えば、45° の 3 等分線は作図可能である。45° の 3 等分は 15° である。15° は 30° の 2 等分、つまり、60° を 4 等分した角となる。ところで、60° は正三角形の一つの角なので作図可能である。2 等分線はコンパスと定木があれば作図出来るので、よって、45° 度は 3 等分可能である。

今与えられた $\angle XOY = 3\theta$ が 3 等分出来たとしよう。(点 X は実軸の正の方向に取り、Y は上半平面にとる。) 中心 O で半径 c の円を描く。OY とこの円が交わる点を D とする。また、D から OX に垂線を下ろし、垂線の足を G とする。また、扇形の弧を 3 等分し、下から順に B、C とする。B から OX に垂線を下ろし、垂線

の足を H とする。$OH = x$、$OG = a$ とする。すると

$$\cos 3\theta = \frac{a}{c}, \quad \cos\theta = \frac{x}{c}$$
$$\cos 3\theta = 4(\cos\theta)^3 - 3\cos\theta$$

が得られ、これから

$$x^3 - \frac{3c^2}{4}x - \frac{ac^2}{4} = 0 \tag{3.1}$$

がわかる。

ここで、次の定理を使う。

定理 3.7 $x^3 + ax^2 + bx + c = 0$ (ただし a, b, c は有理数) が、もし、有理数から出発して定木とコンパスを有限回使用する事によって作図可能な解を持てば、この方程式は少なくとも 1 つの有理数の解を持つ。

この定理を第 4 章で証明することにして、ここでは単に使うことにする。

上の定理の対偶は、

> $x^3 + ax^2 + bx + c = 0$ (ただし a, b, c は有理数) が有理数の解を持たなければ、この方程式は定木とコンパスを有限回用いて作図可能な解は持たない。

である。

それでは、60° が 3 等分出来ない事を証明しよう。背理法で証明する。つまり、60° の 3 等分線が作図できると仮定する。ここで、$3\theta = 60^\circ$ とおく。すると、式 (3.1) において、

$$\frac{a}{c} = \cos 60^\circ = \frac{1}{2}, \quad \frac{x}{c} = \cos 20^\circ$$

である。ここで、$a = 1, c = 2$ とおく。点 B が作図可能であれば、注意 3.5 により、その実部である $\frac{x}{2} = \cos 20^\circ$ は作図可能である。よって、x も作図可能である。すると、$x^3 - 3x - 1 = 0$ には作図可能な解があることになる。すると、定理 3.7 により、$x^3 - 3x - 1 = 0$ は有理数解を持つことになる。

次の補題が証明できれば矛盾が起こり、60° が 3 等分出来ない事が証明されたことになる。

補題 3.8 $x^3 - 3x - 1 = 0$ は有理数解を持たない。

証明 背理法によって証明する。すなわち、$x^3 - 3x - 1 = 0$ が有理数の解を持っていると仮定する。その有理数解を $\frac{u}{v}$ とする。ここで、u, v は ± 1 以外に公約数を持たない整数とする。

$\frac{u}{v}$ はこの 3 次方程式の解となるので、

$$\left(\frac{u}{v}\right)^3 - 3\frac{u}{v} - 1 = 0$$

となる。この方程式の両辺に v^3 をかけると、

$$u^3 = 3uv^2 + v^3$$

が得られる。ところで、この式は以下の 2 通りの方程式で書き表す事が出来る。すなわち、

$$u^3 = v(3uv + v^2) \tag{3.2}$$
$$v^3 = u(u^2 - 3v^2) \tag{3.3}$$

になる。

(3.2) 式より、$v = \pm 1$ でなければならない事が分かる。なぜなら、もし v が ± 1 以外の整数ならば、v はある素数 p で割り切れるはずである。すなわち、$v = v'p$ を満たす整数 v' が存在するはずである。従って (3.2) 式は、

$$u^3 = v'p(3uv + v^2)$$

となり、u^3 が p で割り切れる事を示している。従って、u が p で割り切れなければならない。これは、u, v が ± 1 以外の公約数を持たない整数であることに反する。

よって、$v = \pm 1$ である。同様に、(3.3) によって、$u = \pm 1$ でなければならない。従って $\frac{u}{v} = \pm 1$ でなければならない。

しかし、± 1 は方程式 $x^3 - 3x - 1 = 0$ の解ではない。

よって、 $x^3 - 3x - 1 = 0$ は有理数解を持たない事が証明された。 **証明終**

4 定理 3.7 の証明

ここでは、定理 3.7 を証明することを目標とする。

定理 3.7 の証明には、**体**という概念が必要となる。体とは、複素数全体の集合 **C** の部分集合で、**Q** を含み、四則演算（加減乗除）で閉じている集合のことである[10]。(複素数の部分集合 S が、「$\alpha, \beta \in S$ なら $\alpha \pm \beta$, $\alpha\beta$, $\alpha/\beta \in S$」を満たすとき、S は四則演算で閉じているという。ただし、$\beta = 0$ のときは、α/β は考えない。)

例えば、自然数全体の集合 **N** や整数全体の集合 **Z** は体にはならない。

有理数の集合 **Q**、実数全体の集合 **R**、複素数全体の集合 **C** は体になる。（**Q** を有理数体、**R** を実数体、**C** を複素数体ともいう。）

なお、体と呼ぶことができる集合は他にもたくさん考えることができる。

[10]大学では **C** の部分集合ではない体についても学ぶが、ここではそれを使わないので、**C** の部分集合のみを扱うことにする。

例 4.1　(1) $\mathbf{Q}(i) = \{a + bi \mid a, b \in \mathbf{Q}\}$ とおく。$\mathbf{Q}(i) \subset \mathbf{C}$ であることは明らかである。また、以下で見るように、$\mathbf{Q}(i)$ は四則演算で閉じている集合である。

加法について　$a+bi, c+di \in \mathbf{Q}(i)$ について。$(a+bi)+(c+di) = (a+c)+(b+d)i$ であり、$a + c, b + d \in \mathbf{Q}$ であるので、$(a + bi) + (c + di) \in \mathbf{Q}(i)$ が成り立つ。

減法について　$a+bi, c+di \in \mathbf{Q}(i)$ について。$(a+bi)-(c+di) = (a-c)+(b-d)i$ であり、$a - c, b - d \in \mathbf{Q}$ であるので、$(a + bi) - (c + di) \in \mathbf{Q}(i)$ が成り立つ。

乗法について　$a+bi, c+di \in \mathbf{Q}(i)$ について。$(a+bi)(c+di) = (ac-bd)+(ad+bc)i$ であり、$ac - bd, ad + bc \in \mathbf{Q}$ であるので、$(a + bi)(c + di) \in \mathbf{Q}(i)$ が成り立つ。

除法について　$a + bi, c + di \in \mathbf{Q}(i)$ について (ただし、$c + di \neq 0$ とする)。

$$\frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2} i$$

であり、$(ac + bd)/(c^2 + d^2), (bc - ad)/(c^2 + d^2) \in \mathbf{Q}$ であるので、$(a + bi)/(c + di) \in \mathbf{Q}(i)$ が成り立つ。ここで、$c + di = 0$ と $c = d = 0$ と同値であることに注意。よって、$c + di \neq 0$ は $c^2 + d^2 \neq 0$ と同値である。

したがって、$\mathbf{Q}(i)$ は四則演算で閉じている集合であるから、体である。

(2) $\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$ とおく。$\mathbf{Q}(\sqrt{2}) \subset \mathbf{C}$ であることは明らかである。また、$(\sqrt{2})^2 = 2$ に注意すれば、(1) と同様にして $\mathbf{Q}(\sqrt{2})$ が四則演算で閉じている集合であることがわかる。

(3) $\beta = \sqrt[3]{3}$ とおき、$\mathbf{Q}(\beta) = \{a + b\beta + c\beta^2 \mid a, b, c \in \mathbf{Q}\}$ とおく。$\mathbf{Q}(\beta) \subset \mathbf{C}$ であることは明らかである。さらに、$\beta^3 - 3 = 0$ が成立することに注意すると、$\mathbf{Q}(\beta)$ が四則演算で閉じている集合であることが示される。(定理 4.8 の証明の中で、このような集合が四則演算で閉じていることが示されている。)

定義 4.2　体 k が大きな体 K に含まれるとき、体 K を体 k の**拡大体**、k を K の**部分体**という。また、「体の拡大 K/k において」といういい方もする。

体の拡大 K/k を考えるとき、「K の k 上の基底」、「K の k 上の次元」という概念が重要となる。これらについて言及しておこう。

任意の $x \in K$ は、ある $k_1, k_2, \ldots, k_n \in k$ によって、

$$x = k_1 a_1 + k_2 a_2 + \cdots + k_n a_n$$

と一意的に表すことができる

とき、このような K の元の組 $\{a_1, a_2, \ldots, a_n\}$ を、K の k 上の**基底**とよぶ。この n を K の k 上の次元という。

例 4.4 (1) で見るように、K の k 上の基底は、いろいろなとり方がある。しかし、どのような基底をとっても、それがいくつの元からなる集合かは基底のとり方に寄らないことが知られている。

以上のことを踏まえて、次の定義を与えることにする。

定義 4.3 (1) 体の拡大 K/k において、有限個の元からなる基底を持つとき、K は k 上**有限次拡大**という。

(2) 体の拡大 K/k において、K の k 上の次元を K/k の拡大次数といい、$[K : k]$ で表す。$[K : k] = n$ のとき K/k は n 次拡大という。

例 4.4 (1) 複素数体 $\mathbf{C}$、実数体 $\mathbf{R}$ について。$\mathbf{C}$ は $\mathbf{R}$ の拡大体であり、$\mathbf{C}$ の元は、$a, b \in \mathbf{R}$ を用いて、$a + bi$ と一意的に書けるので、$\{1, i\}$ は $\mathbf{C}$ の $\mathbf{R}$ 上の基底である。ゆえに、$\mathbf{C}$ は $\mathbf{R}$ 上 2 次元となるから、$\mathbf{C}/\mathbf{R}$ は 2 次拡大である。（つまり、$[\mathbf{C} : \mathbf{R}] = 2$ である。）

基底の取り方はいろいろある。例えば、$\{1 + i, 1 - i\}$, $\{2, 3 + i\}$ なども $\mathbf{C}$ の $\mathbf{R}$ 上の基底である。

(2) $\mathbf{Q}(i) = \{a + bi \mid a, b \in \mathbf{Q}\}$ について。$\mathbf{Q}(i)$ は $\mathbf{Q}$ の拡大体であり、$\mathbf{Q}(i)$ の元は、$a, b \in \mathbf{Q}$ を用いて、$a + bi$ と一意的に書けるので、$\{1, i\}$ は $\mathbf{Q}(i)$ の $\mathbf{Q}$ 上の基底である。ゆえに、$\mathbf{Q}(i)$ は $\mathbf{Q}$ 上 2 次元となるから、$\mathbf{Q}(i)/\mathbf{Q}$ は 2 次拡大である。(つまり、$[\mathbf{Q}(i) : \mathbf{Q}] = 2$ である。)

(3) $\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$ について。$\mathbf{Q} \subset \mathbf{Q}(\sqrt{2})$ かつ $\mathbf{Q}(\sqrt{2})$ は体であるから、$\mathbf{Q}(\sqrt{2})$ は $\mathbf{Q}$ の拡大体である。また、$\mathbf{Q}(\sqrt{2})$ の元は、$a, b \in \mathbf{Q}$ を用いて、$a + b\sqrt{2}$ と一意的に書けるので、$\{1, \sqrt{2}\}$ は $\mathbf{Q}(\sqrt{2})$ の $\mathbf{Q}$ 上の基底である。ゆえに、$\mathbf{Q}(\sqrt{2})$ は $\mathbf{Q}$ 上 2 次元となるから、$\mathbf{Q}(\sqrt{2})/\mathbf{Q}$ は 2 次拡大である。（つまり、$[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$ である。）

(4) $\beta = \sqrt[3]{3}$ とおき、$\mathbf{Q}(\beta) = \{a + b\beta + c\beta^2 \mid a, b, c \in \mathbf{Q}\}$ とおく。$\mathbf{Q} \subset \mathbf{Q}(\beta)$ であり $\mathbf{Q}(\beta)$ は $\mathbf{Q}$ の拡大体である。また、$\mathbf{Q}(\beta)$ の元は、$a, b, c \in \mathbf{Q}$ を用いて、$a + b\beta + c\beta^2$ と一意的に書けるので、$\{1, \beta, \beta^2\}$ は $\mathbf{Q}(\beta)$ の $\mathbf{Q}$ 上の基底である。ゆえに、$\mathbf{Q}(\beta)$ は $\mathbf{Q}$ 上 3 次元となるから、$\mathbf{Q}(\beta)/\mathbf{Q}$ は 3 次拡大である。（つまり、$[\mathbf{Q}(\beta) : \mathbf{Q}] = 3$ である。）

定義 4.5 k は体とする。$\alpha \in \mathbf{C}$ に対し、k と α を含む最小の体を $k(\alpha)$ と書く。また、$k(\alpha)$ の形の体を k の**単項拡大**という。

$\mathbf{Q}(\alpha)$ の $\mathbf{Q}$ 上の次元は、どのように決まるのであろうか？

定義 4.6 k を体とする。

(1) $\alpha \in \mathbf{C}$ に対して、$f(\alpha) = 0$ をみたす k 係数の x の多項式 $f(x) \neq 0$ があるとき、α は k **上代数的である**という。

(2) k 係数の多項式 $f(x)$ が、k 係数の 2 つ以上の次数の低い多項式の積に因数分解できるとき、この多項式を k **上の可約多項式**であるという。逆に、因数分解できないときは k **上の既約多項式**であるという。

(3) $f(x)$ は k 係数の多項式で、x に関する最高次の係数は 1 であり、$\alpha \in \mathbf{C}$ が $f(x) = 0$ の解であるとする。この性質をもつ次数が最小の多項式 $f(x)$ を α **の** k **上の最小多項式**という。

注意 4.7 $f(x)$ を α の k 上の最小多項式とする。定義から明らかに $f(x)$ は k 上の既約多項式である。

$h(x)$ は、$h(\alpha) = 0$ をみたす k 係数の多項式としよう。ユークリッド除法により

$$h(x) = q(x)f(x) + r(x)$$

を得たとする。すると、$r(\alpha) = 0$ となる。$f(x)$ の次数の最小性から $r(x) = 0$ となり、$h(x)$ は $f(x)$ で割り切れることがわかる。

このことから、$f(x) \neq 0$ が $f(\alpha) = 0$ をみたす k 係数の既約多項式であるとき、$f(x)$ は α の k 上の最小多項式となる。

すべての複素数に対して、最小多項式 $f(x)$ が存在するわけではない。例えば、自然対数の底 e, 円周率 π は、$\mathbf{Q}$ 上代数的ではないことが証明されている。

ここで、次の定理が得られる。

定理 4.8 $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ を α の体 k 上の最小多項式とする。このとき、単項拡大 $k(\alpha)$ を考えると、$[k(\alpha) : k] = n$ が成り立つ。

証明

$$S = \{b_1\alpha^{n-1} + b_2\alpha^{n-2} + \cdots + b_n \mid b_1,\ b_2,\ \ldots,\ b_n \in k\} \subset \mathbf{C}$$

とおく。

まず、$S = k(\alpha)$ を証明したい。

$S \subseteq k(\alpha)$ は明らかである。

$h(x)$ は、x の k 係数の多項式であるとする。ユークリッド除法により、

$$h(x) = f(x)q(x) + r(x)$$

とできる。ただし、$q(x)$, $r(x)$ は k 係数の多項式で、$r(x) = 0$ または $r(x)$ は n 次未満の式としてよい。このとき、

$$h(\alpha) = f(\alpha)q(\alpha) + r(\alpha) = r(\alpha) \in S$$

である。このことから、S は加減乗の三演算で閉じていることがわかった。

また、$h(x) \neq 0$ が n 次未満の多項式のとき、

$$p(x)h(x) + q(x)f(x) = 1$$

をみたす多項式 $p(x)$, $q(x)$ が存在することが知られている (ベズーの定理)。このとき、

$$p(\alpha)h(\alpha) = 1$$

が成立する。よって、$h(\alpha)^{-1} = p(\alpha)$ となり、S は除法で閉じている。よって、S は体であることがわかった。$k(\alpha)$ は、k と α を含む最小の体であるので、$S \supseteq k(\alpha)$ である。

よって、$S = k(\alpha)$ がわかった。

次に、$\beta \in k(\alpha)$ が

$$\begin{aligned} \beta &= k_1\alpha^{n-1} + k_2\alpha^{n-2} + \cdots + k_{n-1}\alpha + k_n \cdot 1 \\ &= k'_1\alpha^{n-1} + k'_2\alpha^{n-2} + \cdots + k'_{n-1}\alpha + k'_n \cdot 1 \end{aligned}$$

と二通りに書けたとしよう ($k_1, k_2, \ldots, k_n, k'_1, k'_2, \ldots, k'_n \in k$ とする)。このとき、

$$(k_1 - k'_1)\alpha^{n-1} + (k_2 - k'_2)\alpha^{n-2} + \cdots + (k_{n-1} - k'_{n-1})\alpha + (k_n - k'_n) \cdot 1 = 0$$

を得る。ここで、

$$h(x) = (k_1 - k'_1)x^{n-1} + (k_2 - k'_2)x^{n-2} + \cdots + (k_{n-1} - k'_{n-1})x + (k_n - k'_n)$$

とおく。$k_l \neq k'_l$ をみたす l があれば、$h(x) \neq 0$ である。すると、$h(\alpha) = 0$ であるので、$f(x)$ の次数の最小性に反する。よって、全ての l に対して $k_l = k'_l$ がわかり、$\{\alpha^{n-1}, \alpha^{n-2}, \ldots, \alpha, 1\}$ は、$k(\alpha)$ の k 上の基底となり、$[k(\alpha) : k] = n$ となることがわかった。 **証明終**

さて、次の定理を証明することにしよう。

定理 4.9 (拡大次数の連鎖律) $k \subset K \subset L$ が体の有限次拡大のとき、

$$[L : k] = [L : K][K : k]$$

が成り立つ。

証明 $[L : K] = m, [K : k] = n$ とする。$\{e_1, \ldots, e_m\}$ を L の K 上の基底、$\{d_1, \ldots, d_n\}$ を K の k 上の基底とする。示したいことは、mn 個の元の集合 $\{\, e_i d_j \mid i = 1, \ldots, m;\ j = 1, \ldots, n \,\}$ が L の k 上の基底になることである。これが言えれば、$[L : k] = mn = [L : K][K : k]$ が結論される。

まず、$e_1, \ldots, e_m$ は L の K 上の基底であるから、L の任意の元 α は、

$$\alpha = \sum_{i=1}^{m} k_i e_i \quad (k_1, \ldots, k_m \in K)$$

と表すことができる。さらに、$\{d_1, \ldots, d_n\}$ は K の k 上の基底だから、K の元である k_i $(i = 1, \ldots, m)$ は、

$$k_i = \sum_{j=1}^{n} f_{ij} d_j \quad (f_{i1}, \ldots, f_{in} \in k)$$

と表すことができ、これを代入すると、

$$\alpha = \sum_{i=1}^{m} \left\{ \sum_{j=1}^{n} f_{ij} d_j \right\} e_i = \sum_{i=1}^{m} \sum_{j=1}^{n} f_{ij} d_j e_i$$

となるから、L に属する mn 個の元の集合 $\{ d_j e_i \mid i = 1, \ldots, m;\ j = 1, \ldots, n\}$ と、k に属する mn 個の元 f_{ij} $(i = 1, \ldots, m;\ j = 1, \ldots, n)$ を用いて、L の任意の元 α を表すことができる。

L の元 α が二通りに表すことができたとすると、その差をとってやると、

$$\sum_{i=1}^{m} \sum_{j=1}^{n} f_{ij} d_j e_i = 0 \ \ (f_{ij} \in k)$$

の形の関係式が得られる。$\sum_{j=1}^{n} f_{ij} d_j \in K$ で、$\{e_1, \ldots, e_m\}$ は L の K 上の基底だから、任意の $i = 1, \ldots, m$ に対して

$$\sum_{j=1}^{n} f_{ij} d_j = 0$$

が得られる。$\{d_1, \ldots, d_n\}$ は K の k 上の基底で $f_{ij} \in k$ だから、任意の $j = 1, \ldots, n$ に対して $f_{ij} = 0$ となる。よって、α の表し方は一意的であることがわかった。

以上で、$\{ d_j e_i \mid i = 1, \ldots, m;\ j = 1, \ldots, n\}$ は L の k 上の基底になることが結論される。 **証明終**

ところで定理 3.6 により、複素数 α が作図可能であるための必要十分条件は、α は有理数から有限回の四則演算とルートを使って表すことができることであった。

例えば、

$$\alpha = \frac{\sqrt{3 + 2\sqrt{-1}} - \sqrt{8}}{5}$$

としよう。$K_0 = \mathbf{Q}$, $K_1 = K_0(\sqrt{-1})$, $K_2 = K_1(\sqrt{3 + 2\sqrt{-1}})$, $K_3 = K_2(\sqrt{8})$ とおく。このとき、

$$\mathbf{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq K_3, \ \ \alpha \in K_3$$

となる。つまり、$i = 1, 2, 3$ に対して、$K_i = K_{i-1}(\beta_i)$ であって $\beta^2 \in K_{i-1}$ を満たす β_i が存在する。β_i は K_{i-1} 上の多項式 $x^2 - \beta_i^2 = 0$ の解である。よって、β_i の K_{i-1} 上の最小多項式の次数は 2 以下であるので、定理 4.8 によって $[K_i : K_{i-1}] \leq 2$ である。$[K_i : K_{i-1}] = 1$ のときは $K_i = K_{i-1}$ であり、そのときは、上の体の列から同じものを除けば、次の定理を得る。

定理 4.10 α は複素数とする。次は同値である。

(a) α は有理数からコンパスと定規で作図可能な複素数である。

(b) ある整数 $n \geq 0$ と体の拡大 $\mathbf{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n = K$ で、任意の $i = 1, 2, \ldots, n$ に対して $[K_i : K_{i-1}] = 2$ かつ $\alpha \in K_n$ を満たすものがある。

すると、次のことがわかる。

系 4.11 複素数 α が有理数からコンパスと定規で作図可能な複素数であるならば、$[\mathbf{Q}(\alpha) : \mathbf{Q}]$ は 2 の冪である。

証明 定理 4.10 の条件 (b) を満たす体の列 $K_0 = \mathbf{Q}, K_1, \ldots, K_{n-1}, K_n = K$ を取る。このとき、拡大次数の連鎖律 (定理 4.9) を繰り返し使えば、$[K : \mathbf{Q}] = 2^n$ であることがわかる。

さらに、

$$\mathbf{Q} \subseteq \mathbf{Q}(\alpha) \subseteq K_n$$

であるので、再び拡大次数の連鎖律を使うと、$[\mathbf{Q}(\alpha) : \mathbf{Q}]$ は 2 の冪であることがわかる。 **証明終**

注意 4.12 系 4.11 の逆は成立しない。すなわち、$[\mathbf{Q}(\alpha) : \mathbf{Q}]$ が 2 のベキであっても、定理 4.10 の条件 (b) を満たす体の列 $K_0 = \mathbf{Q} \subseteq K_1 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n$ が存在するとは限らない。

例えば、$f(x) = x^4 - x - 1$ は $\mathbf{Q}$ 上の既約多項式であり（これは、アイゼンシュタインの判定法と呼ばれる方法で確かめることができる）、$\alpha \in \mathbf{C}$ を $f(x) = 0$ の解とすれば、定理 4.8 より、$[\mathbf{Q}(\alpha) : \mathbf{Q}] = 4 = 2^2$ であることがわかる。しかし、定理 4.10 の条件 (b) を満たす体の列 $K_0 = \mathbf{Q} \subseteq K_1 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n$ は存在しない。（これを説明するには「体のガロワ理論」と群論が必要となる。定理 5.2 参照。）

さらに、次のことを示そう。

命題 4.13 $f(x) = x^3 + ax^2 + bx + c$ (a, b, c は有理数）とおく。$f(x) = 0$ が有理数の解をもたないならば、$f(x)$ は $\mathbf{Q}$ 上の既約多項式である。

証明 $f(x)$ が $\mathbf{Q}$ 上の可約多項式であると仮定する。このとき、ある有理数 p, q, r が存在して $x^3 + ax^2 + bx + c = (x + p)(x^2 + qx + r)$ と因数分解することが可能となり、3 次方程式 $f(x) = 0$ は有理数の解 $x = -p$ をもつことになるが、これは仮定に矛盾する。したがって、題意成立。 **証明終**

以上の準備のもとに、定理 3.7 を証明することにしよう。

証明 $f(x) = x^3 + ax^2 + bx + c$ とおき、$f(x) = 0$ の解のうち、作図可能なものを $\alpha \in \mathbf{C}$ とおく。このとき、定理 3.7 を背理法により証明する。すなわち、$f(x) = 0$ が有理数の解をもたないと仮定し矛盾を導く。

$f(x) = 0$ が有理数の解をもたないとすると、命題 4.13 より、$f(x)$ は $\mathbf{Q}$ 上の既約多項式となる。さらに、α は $f(x) = 0$ の解であるから、定理 4.8 より、

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

となる。ところで $\alpha \in \mathbf{C}$ は作図可能であるから、系 4.11 より、$[\mathbf{Q}(\alpha) : \mathbf{Q}]$ は 2 の冪にならなければならないが、これは矛盾である。こうして、定理 3.7 が結論される。 **証明終**

5　正 n 角形はいつ作図可能か？

ここからはガロア理論を用いて正 n 角形が定木とコンパスで作図できるのは、n がどのような数のときなのか？ということを考える。

定理 5.1 正 n 角形が作図できる必要十分条件は、$\epsilon_n = e^{\frac{2\pi i}{n}}$ が作図可能であることである。

証明 正 n 角形が作図できるとする。すると、半径 1 の円に内接し、1 と頂点として持つ正 n 角形が作図できる。

明らかに、半径 1 の円に内接し、1 を頂点として持つ正 n 角形が作図できる必要十分条件は、$e^{\frac{2\pi i}{n}}$ が作図可能であることである。 **証明終**

次に複素数 α が作図できる必要十分条件を考える。

定理 5.2 α は複素数とする。次は同値である。

(a) α は有理数からコンパスと定規で作図可能な複素数である。

(b) ある整数 $n \geq 0$ と体の拡大 $\mathbf{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n = K$ で、任意の $i = 1, 2, \ldots, n$ に対して $[K_i : K_{i-1}] = 2$ かつ $\alpha \in K_n$ を満たすものがある。

(c) $\mathbf{Q}$ 上のガロワ拡大 L で、$L \ni \alpha$ かつ $[L : \mathbf{Q}]$ が 2 の冪であるものが存在する。

(d) L_0 を α の $\mathbf{Q}$ 上の分解体としたとき $[L_0 : \mathbf{Q}]$ が 2 の冪である。

(e) $[K_i : K_{i-1}] = 2$ $(i = 1, \ldots, n)$ を満たす体の列

$$\mathbf{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = \mathbf{Q}(\alpha)$$

が存在する。

証明 (a) と (b) が同値であることは、すでに定理 4.10 で示した。

(b)⇒(c) を証明しよう。$K_i = K_{i-1}(\alpha_i)$ とする。今 α_i の K_{i-1} 上の最小多項式の次数は 2 になっている $(i = 1, \ldots, n)$。ここで、$\alpha_i^2 \in K_{i-1}$ と仮定してよい。$\sigma : K_n \to \mathbf{C}$ を体の中への同型で、$\sigma|_{K_0} = \mathrm{id}_{K_0}$ を満たすものとする。このとき、

$$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$$

であるから

$$K_0 = \sigma(K_0) \subseteq \sigma(K_1) \subseteq \cdots \subseteq \sigma(K_n)$$

となる。$\sigma(K_i) = \sigma(K_{i-1})(\sigma(\alpha_i))$ であり $\sigma(\alpha_i)$ の $\sigma(K_{i-1})$ 上の最小多項式の次数は 2 である。このとき、体の拡大

$$K_n \subseteq K_n(\sigma(\alpha_1)) \subseteq K_n(\sigma(\alpha_1), \sigma(\alpha_2)) \subseteq \cdots \subseteq K_n(\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n))$$

を考える。

$$\sigma(\alpha_1)^2 \in \sigma(K_{i-1}) = K_0(\sigma(\alpha_1), \ldots, \sigma(\alpha_{i-1})) \subseteq K_n(\sigma(\alpha_1), \ldots, \sigma(\alpha_{i-1}))$$

であるので、$\sigma(\alpha_i)$ の $K_n(\sigma(\alpha_1), \ldots, \sigma(\alpha_{i-1}))$ 上の最小多項式の次数は 1 または 2 であって、従って

$$[K_n(\sigma(\alpha_1), \ldots, \sigma(\alpha_i)) : K_n(\sigma(\alpha_1), \ldots, \sigma(\alpha_{i-1}))] = 1 \text{ または } 2$$

である。これにより $K_n(\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n))$ は K_n から 2 次拡大を有限回とって得られることがわかる。ここで、

$$\{\sigma \colon K_n \to \mathbf{C} \mid \text{中への同型で} \sigma|_{K_0} = \mathrm{id}_{K_0}\} = \{\sigma_1 = \mathrm{id}_{K_n}, \sigma_2, \ldots, \sigma_t\}$$

とおく。(これは、有限集合になる。)

上と同様な議論で、

$$\mathbf{Q}(\{\sigma_i(\alpha_j) \mid i = 1, \ldots, t;\ j = 1, \ldots, n\})$$

は $\mathbf{Q}$ から 2 次拡大を有限回とって得られることがわかる。この体を L とおく。構成法から、L は $\mathbf{Q}$ 上正規拡大なので、$L/\mathbf{Q}$ はガロワ拡大。また、連鎖律 (定理 4.9) により $[L : \mathbf{Q}]$ は 2 の冪であることがわかる。

(c)⇒(d) を証明しよう。$L/\mathbf{Q}$ はガロワ拡大で、$[L : \mathbf{Q}]$ は 2 の冪としよう。L_0 を α の $\mathbf{Q}$ 上の分解体としたとき

$$L \supseteq L_0 \supseteq \mathbf{Q}$$

であるので、連鎖律より $[L_0 : \mathbf{Q}]$ は 2 の冪となる。

(e)⇒(b) は明らか。

最後に (d)⇒(e) を示そう。

$G = \mathrm{Gal}(L_0/\mathbf{Q})$ とおく。H は、L_0 の部分体 $\mathbf{Q}(\alpha)$ に対応する G の部分群とする。$^{\#}G = [L_0 : \mathbf{Q}] = 2^l$ としよう。

このとき、次の補題 5.3 により

$$H = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G$$

で $[H_i : H_{i-1}] = 2$ $(i = 1, \ldots, n)$ をみたす部分群の列が存在する。これに対応する中間体の列

$$\mathbf{Q}(\alpha) = L_0^{H_0} \supseteq L_0^{H_1} \supseteq \cdots \supseteq L_0^{G} = \mathbf{Q}$$

をとれば、ガロワ理論を用いて $[L_0^{H_i} : L_0^{H_{i+1}}] = 2$ $(i = 0, 1, \ldots, n)$ となっていることがわかる。 **証明終**

補題 5.3 G は群で、$^{\#}G = p^l$ とする。ただし、p は素数で、l は自然数とする。H は G の部分群であるとする。$[G : H] = p^n$ としよう。

このとき、G の部分群の列

$$H = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G$$

で $[H_i : H_{i-1}] = p$ $(i = 1, \ldots, n)$ をみたすものが存在する。

証明 l に関する帰納法で証明する。

$l = 1$ のときは、明らかである。

$l \geq 2$ としよう。

H が G の正規部分群 $N \neq \{e\}$ を含むとしよう。すると、全射準同型 $\pi : G \to G/N$ を考えると、$H/N \subseteq G/N$ に関しては、補題を満たす部分群の列が存在する。その群の列の π による逆像を取ればよい。

$Z(G)$ を群 G の中心としよう。このとき、G の位数が素数の冪であるので、$Z(G) \neq \{e\}$ であることはよく知られている。

$Z(G) \cap H \neq \{e\}$ のときは、これは H に含まれる $\{e\}$ 以外の正規部分群であるので、上の議論より、部分群の列の存在がわかる。

$Z(G) \cap H = \{e\}$ と仮定する。$a \in Z(G) \setminus H$ をとる。a を適当なべきで取り替えることにより、$a^p = e$ としてよい。H_1 は、H と a で生成された G の部分群であるとする。このとき、$[H_1 : H] = p$ である。a で生成された部分群 C は G の正規部分群であり、$C \subseteq H_1$ であるので、H_1 から始まる部分群の列はとれる。それと、$H \subseteq H_1$ をつなげば、必要な列が得られる。 **証明終**

次の定理により、$[\mathbf{Q}(\epsilon_n) : \mathbf{Q}]$ の計算が可能になる。

定理 5.4 $\Phi_n(x) = \prod_{1 \leq k \leq n,\ (k,n)=1} (x - \epsilon_n^k)$ とおく。このとき、

(a) $\Phi_n(x)$ は $\mathbf{Q}$ 係数の多項式である。

(b) $\Phi_n(x)$ は $\mathbf{Q}$ 上既約である。

証明 (a) を示す。$\mathbf{Q}(\epsilon_n)$ は、$x^n - 1$ の分解体であるので、$\mathbf{Q}(\epsilon_n)/\mathbf{Q}$ はガロワ拡大である。$\sigma \in \mathrm{Gal}(\mathbf{Q}(\epsilon_n)/\mathbf{Q})$ は、$\{1, \epsilon_n, \epsilon_n^2, \ldots, \epsilon_n^{n-1}\}$ の置換を引き起こす。σ は、巡回群 $\{1, \epsilon_n, \epsilon_n^2, \ldots, \epsilon_n^{n-1}\}$ の同型を誘導するので、生成元の集合 $\{\epsilon_n^k \mid 1 \leq k \leq n,\ (k, n) = 1\}$ の置換を引き起こす。$\Phi_n(x)$ の係数は、$\{\epsilon_n^k \mid 1 \leq k \leq n,\ (k, n) = 1\}$ の対称式であるので、$\Phi_n(x)$ の係数は σ の作用で不変である。よって、$\Phi_n(x)$ の係数は有理数である。

次に、(b) を示す。$\Phi_n(x)$ が $\mathbf{Q}$ 上で可約だとする。ϵ の $\mathbf{Q}$ 上の最小多項式を $h(x)$ とする。すると、$\Phi_n(x) = h(x)k(x)$ と書ける。

$\Phi_n(x)$ は $x^n - 1$ を割り切るモニック多項式なので、$\Phi_n(x)$ の係数は $\mathbf{Z}$ に入る。同様の理由で、$h(x), k(x)$ も $\mathbf{Z}$ 係数の多項式である。

$\Phi_n(x)$ は重根を持たないので $h(x)$ と $k(x)$ は共通根をもたない。$k(x)$ の根 ϵ_n^a $(1 \leq a \leq n-1)$ で a が最小になるように選ぶ。$a \neq 1$ であるので、a を割り切る素数の一つを p とする。$a = pb$ としよう。このとき、ϵ_n^b は $h(x)$ の根であり、ϵ_n^a は $k(x)$ の根である。すると、ϵ_n^b は $k(x^p)$ の根である。ϵ_n^b の最小多項式は $h(x)$ であるので、$k(x^p)$ は $h(x)$ で割り切れる。$k(x^p) = h(x)g(x)$ としよう。$g(x) \in \mathbf{Z}(x)$ であることに注意する。

$\mathbf{F}_p$ は標数 p の素体とする。$\pi : \mathbf{Z}[x] \to \mathbf{F}_p[x]$ を自然な環準同型とする。多項式 $f(x) \in \mathbf{Z}[x]$ の π による像を $\overline{f}(x) \in \mathbf{F}_p[x]$ で表すことにする。すると、

$$(\overline{k}(x))^p = \overline{k}(x^p) = \overline{h}(x)\overline{g}(x)$$

となる。従って $\overline{h}(x)$ と $\overline{k}(x)$ は共通因子があることになる。すると $\overline{\Phi_n}(x) = \overline{h}(x)\overline{k}(x)$ が重根を持たなくてはならない。ここで $\overline{\Phi_n}(x)$ は $\overline{x^n - 1}$ を割り切ることに注意する。しかし、p のとり方から、n と p は互いに素であるので、$\overline{x^n - 1}$ は、$\mathbf{F}_p$ で重根は持たない。これは、矛盾である。これで、$\Phi_n(x)$ が $\mathbf{Q}$ 上で既約であることがわかった。 **証明終**

$\varphi(n) = {}^{\#}\{k \in \mathbf{N} \mid 1 \leq k \leq n,\ (k, n) = 1\}$ と定義する。$\varphi(n)$ はしばしはオイラー関数と呼ばれる。

前定理から直ちに次のことがわかる。

系 5.5 $[\mathbf{Q}(\epsilon_n) : \mathbf{Q}] = \varphi(n)$ である。

証明 定理 5.4 により、$\Phi_n(x)$ は ϵ_n の $\mathbf{Q}$ 上の最小多項式である。

よって、定理 4.8 により、$[\mathbf{Q}(\epsilon_n) : \mathbf{Q}]$ は、$\Phi_n(x)$ の次数と一致する。それは、明らかに $\varphi(n)$ である。 **証明終**

正 n 角形がいつコンパスと定木で作図可能か考えよう。

定理 5.1 ですでに見たように、正 n 角形がいつコンパスと定木で作図可能である必要十分条件は、ϵ_n がコンパスと定木で作図可能な複素数であることである。

ϵ_n の $\mathbf{Q}$ 上の分解体は、$\mathbf{Q}(\epsilon_n)$ である。よって、定理 5.2 により、ϵ_n がコンパスと定木で作図可能な複素数であるための必要十分条件は、$[\mathbf{Q}(\epsilon_n) : \mathbf{Q}]$ が 2 の冪であることである。

よって、次のことがわかった。

定理 5.6 正 n 角形がコンパスと定木で作図可能であるための必要十分条件は、$\varphi(n)$ が 2 の冪であることである。

ここで $\varphi(n)$ について考えてみることにする。

p を素数とすると、$\varphi(p) = p - 1, \varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$ である。

一般の自然数 n を素因数分解して考える。

$$n = p_1^{l_1} \cdots p_t^{l_t}$$

ただし、p_i は素数で、$p_1 < p_2 < \cdots < p_t$ を満たすものとする。このとき、

$$\varphi(n) = \varphi(p_1^{l_1}) \cdots \varphi(p_t^{l_t}) = p_1^{l_1-1}(p_1-1) \cdots p_t^{l_t-1}(p_t-1)$$

となることが知られている。

これが、2 の冪になるための必要十分条件は、

$$n = 2^l p_1 \cdots p_s$$

ただし $3 \leq p_1 < p_2 < \cdots < p_s$（$p_j$ は素数）かつ $p_j - 1$ は 2 の冪のときである。

参考文献

「天才数学者はこう解いた、生きた」木村俊一 (講談社)

「可換体論」永田雅宣 (裳華房)

「代数系入門」松坂和夫 (岩波書店)

「角の三等分」矢野健太郎 (創元社)

「環と体」渡辺敬一 (朝倉書店)

http://ja.wikipedia.org/wiki/Wi

http://www.geocities.jp/ja1tmc/derosumonndai.htm

http://www.nikonet.or.jp/spring/origami/origami_2.htm

http://www.shirakami.or.jp/ eichan/oms/omsxx/oms.18html

http://www004.upp.so-net.ne.jp/s_honma/

http://yosshy.sansu.org/santobun.htm