2011 年度藏野研究室卒業論文
“目盛付定規で作図できるための必要十分条件”

明治大学理工学部数学科
牛込 利江
大田 康介
高瀬 友樹
武田 侑子
和田 昂之

平成 24 年 2 月 21 日

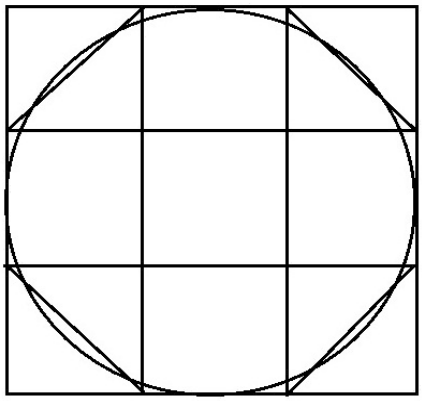
目 次

1 Introduction

紀元前5世紀のギリシャでは、円積問題、倍積問題、角の三等分の三大作図問題について研究されていた。プラトン[1]によると難しい道具を用いてこれらを作図することは出来るが、そのような方法は幾何学の美しさを壊してしまうもので、定木とコンパスだけで作図することが望ましいと言って、定木とコンパスだけでの作図が始まった。道具を定木とコンパスに限定したのは古代ギリシャだけで、プラトン以前にも他の道具を用いた作図は行われていた。

まず、「作図」とは目盛りのない定木とコンパスの2つの道具だけを有限回使用して、要求された図形を描くこととする。定木は与えられた2点を結んで線分を引くための道具で、長さを測ることはできないものとする。コンパスは与えられた点を中心にとり、与えられたもう一点を通るような円を描くための道具とする。

1. 円積問題–与えられた任意の円の面積に等しい正方形の作図問題–
古来、土地の測量や穀物倉庫などに関連して、長方形や台形、円などの平面図形の面積、四角柱や円柱などの体積を求める計算が行われていた。色々な平面図形の中でも円は身近に観察できる図形でありながら、古代エジプトや古代バビロニアでは、円の面積の近似値しか求めることができなかった。それは円が曲線図形だからである。三角形や四角形などの直線図形は面積が比較的簡単に求められたのに対して、円の求積は困難であった。古代エジプトの「リンド・パピルス」にある幾何学の問題で「直径9の円の丸い土地の面積はいくらか」というものがあり、解法は「円の面積とその円に外接する正方形の面積を比較せよ」と添えられていた。つまり、円をそれに外接する正方形の四隅を切り取って出来る八角形によって近似する方法が考えられていた。



この八角形の面積は、$9^2 - 4 \times \frac{1}{2} \cdot 3 \cdot 3 = 81 - 18 = 63$ となるが、古代エジプト人

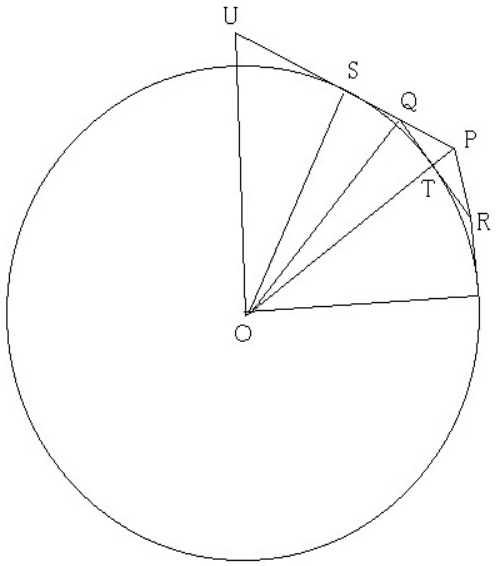
[1]Plato (紀元前 430-350) 古代ギリシャの哲学者で、ソクラテスの弟子でアリストテレスの師である。

はこれを 64 すなわち 8^2 で近似した。つまり直径 9 の円の面積を一辺 8 の正方形の面積にほぼ等しいと考えたわけである。この結果から私たちはエジプトにおける円周率の値を計算することができる。直径 9 の円の面積は $\pi(\frac{9}{2})^2$ であり、これがほぼ 8^2 に等しいというのだから、$\pi(\frac{9}{2})^2 \fallingdotseq 8^2$ より、$\pi \fallingdotseq 3.16$ と求めることができ、誤差はおおよそ 0.02 であることが分かる。

また、古代バビロニアでは、円をそれに内接・外接する正十二角形によって挟み込む方法を用いて円の求積がなされていた。

（内接正十二角形の面積）$<$（円の面積）$<$（外接正十二角形の面積）

によって近似的に求められた。



円の半径を 2 として考える。内接正十二角形の面積は 12 と求められる。$SQ = QT = TR = x$, $SP = y$ とおく (つまり、外接する正十二角形の一辺が $2x$ である)。このとき $\triangle OUP$ は正三角形なので、$OP = 2y$ となる。$\triangle OPQ = \triangle OPS - \triangle OQS$ であり、$\triangle OPQ = \frac{1}{2} \cdot 2y \cdot x$、$\triangle OPS = \frac{1}{2} \cdot 2 \cdot y$、$\triangle OQS = \frac{1}{2} \cdot 2 \cdot x$ なので、

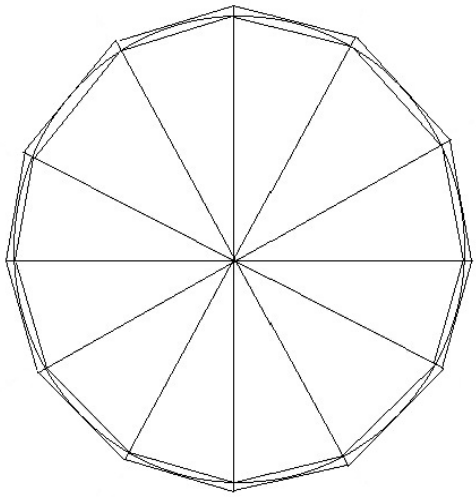
$$xy = y - x \tag{1}$$

となる。また $\triangle OPS$ は直角三角形なので三平方の定理より、$(2y)^2 = y^2 + 2^2$ なので

$$3y^2 = 4 \tag{2}$$

となる。(1) より $y = \frac{x}{1-x}$ なので、(2) に代入すると $x^2 - 8x + 4 = 0$ となり、$0 < x < 2$ なので $x = 4 - \sqrt{12}$ である。ここで $\sqrt{12} > \frac{7}{2} - \frac{1}{24}$ であることを用いて $x < 4 - (\frac{7}{2} - \frac{1}{24}) = \frac{1}{2} + \frac{1}{24}$ である。

外接正十二角形の面積は $\triangle OQT$ の 24 個分なので、$24 \cdot \frac{1}{2} \cdot 2 \cdot x = 24x < 24(\frac{1}{2} + \frac{1}{24}) = 13$ となり、$12 <$（円の面積）< 13 が分かる。このことから古代バビロニア人は円の面積を 12.5 としていた。この結果から円周率を計算してみると、$\pi(2)^2 \fallingdotseq 12.5$ より $\pi \fallingdotseq 3.125$ となる。



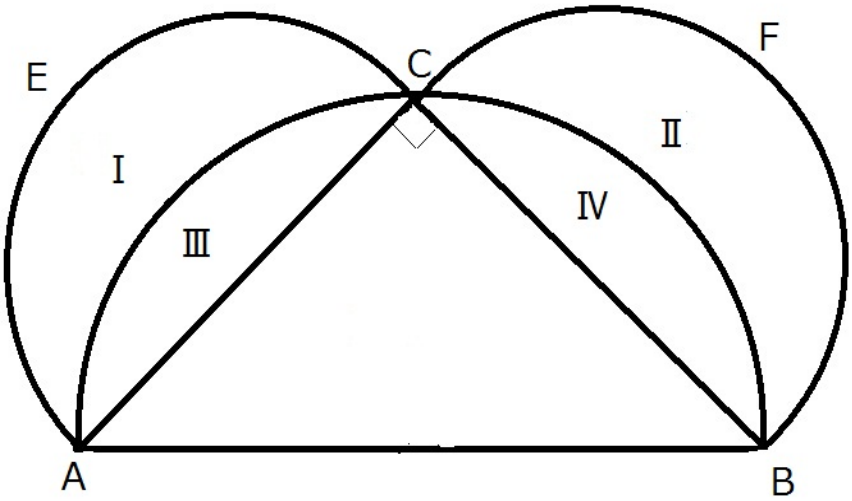
古代エジプトと古代バビロニアでは、円の求積は円を直線図形に還元するという円の面積を近似的に求めることに終わっていたが、厳密さを志向していた古代ギリシアでは、定木とコンパスのみを用いて円の面積と同等な面積をもつ正方形を作ることが探究されていた。この円の正方形化に取り組んだ最初の数学者は、アナクサゴラス[2]であったという。彼は、この問題を入獄中に研究したと伝えられている。次にこの問題を研究したキオスのヒポクラテス[3]は、いくつかの三日月型を正方形化することを通じて、円の正方形化に迫ろうとした。直角二等辺三角形において、下の図で

$$I \text{の面積} + II \text{の面積} = \text{三角形 } ABC \text{の面積} \tag{3}$$

[2]Anaxagoras (紀元前 500-428 年頃) 古代ギリシャの哲学者で、アテネに哲学を持ち込んだ最初の人である。

[3]Hippocrates (紀元前 460-380 年頃) 初め商人であったが、商用で航海中に海賊に所持品を奪われ、取り返そうとアテネにやってきて幾何学を学び、有名になった。

を示した。



式 (3) は、次のように証明される。

$$\frac{\text{半円 } AC \text{ の面積}}{\text{半円 } AB \text{ の面積}} = \frac{\pi(\frac{AC}{2})^2}{\pi(\frac{AB}{2})^2} = \frac{AC^2}{AB^2} = \frac{AC^2}{AC^2 + CB^2}$$

であるが、$AC = CB$ なので

$$\frac{\text{半円 } AC \text{ の面積}}{\text{半円 } AB \text{ の面積}} = \frac{AC^2}{2AC^2} = \frac{1}{2}$$

である。よって、

$$\text{半円 } AC \text{ の面積} + \text{半円 } CB \text{ の面積} = \text{半円 } AB \text{ の面積}$$

が成立する。この式の両辺から

$$III \text{ の面積} + IV \text{ の面積}$$

を引くと

$$I \text{ の面積} + II \text{ の面積} = \text{三角形 } ABC \text{ の面積}$$

となる。I と II の面積は等しいので、それぞれは三角形 ABC の半分の面積に等しい。三角形は正方形化できるので、この図での三日月形は正方形化された。

このようにしてヒポクラテスは曲線図形である月形の面積と同等な直線図形が作られるということから、円と同等な直線図形を作り得ると考えたのである。しかし、円の正方形化は解決されなかった。この問題の最終的な解決は 19 世紀になっ

てようやく得られた。1882 年にドイツの数学者であるリンデマン[4]が π が超越数であることを示し、円積問題は定木とコンパスを有限回使用して作図することは不可能であることを示した。

リンデマン

2. 倍積問題–与えられた立方体の体積の 2 倍の体積を持つ立方体の作図問題–
伝説によると、ミノス王は立方体の形をした墓を彼の息子に建てたが、彼は、その墓は 100 フィート（30 メートルくらい）しかないことを聞いたとき、これはとても小さすぎると思った。「体積を 2 倍にしなければならない」と彼は言い、一辺を 2 倍にした墓をすぐに建てるように建築者に要求した。数学者はすぐにこの方法では新しい墓の体積が元の墓の体積の 8 倍になってしまうという間違えに気づき、研究を重ねたが、難しくて解くことは出来なかった。
他に「デロス島の問題」と呼ばれる伝説がある。紀元前 430 年頃にギリシャのデロス島では大変な伝染病が流行していた。これを大いに恐れた島の人々はデロス島の守護神であるアポロンの神殿にお伺いを立てたところ、そのときの神託は「もし不運を取り除きたいなら、神殿の正面にある祭壇（立方体）の 2 倍になるような祭壇をつくって奉納しなさい。」という神託を受けた。人々は各辺を 2 倍にした祭壇を奉納したが、伝染病は一向に収まらなかった。なぜなら、体積が 8 倍になってしまうからである。困った人々は立方体を 2 個並べて置いたけれど、これも効

[4]Carl Louis Ferdinand von Lindemann (1852-1939) ミュンヘン大学の教授で、ドイツの数学者である。π が超越数であることを示し、円積問題の作図が不可能なことを示した。

果はなかった。困り果てた人々はもう一度神託を聞いてみると、各辺の長さではなくて、「体積を 2 倍にして、かつ立方体でなければならない」というお告げだった。つまり、元々の立方体の一辺の長さの $\sqrt[3]{2}$ 倍の長さを一辺に持った立方体の作図をするということだったのだ。しかし、人々はどのようにしたら元の立方体の 2 倍の体積の立方体を作れるのか分らなかった。そこで人々は賢人として名高いギリシャの哲学者であるプラトンに相談をした。すると、この難問はプラトンも解くことができなかった。しかしプラトンは「神は 2 倍の祭壇をお望みなのではなくて、ギリシャ人が幾何学を軽視しないようにするために、この課業を与えたのだ。」言った。三大作図問題の最終的な解法は (プラトンによって許された)2 つの道具だけでは作図不可能であるという証明だった。これらの証明は 19 世紀になってようやく与えられた。また、このときは代数学的な考えはまだギリシャ人には知られていなかった。

次に、定木とコンパス以外の特殊な道具を使用した倍積問題の解法を紹介する

・メナイクモス[5]の解法

メナイクモスは平面と円錐が交わって出来る、3 種類の円錐曲線の断面を考察した。後に、平面に直接曲線を作図し、それらを楕円、放物線、双曲線と名付けた。今日、これらは 2 次方程式のグラフとして扱われている。比例の関係式から 2 つの放物線 (または放物線と双曲線) の交点を見出すことによって倍積問題は解かれた。

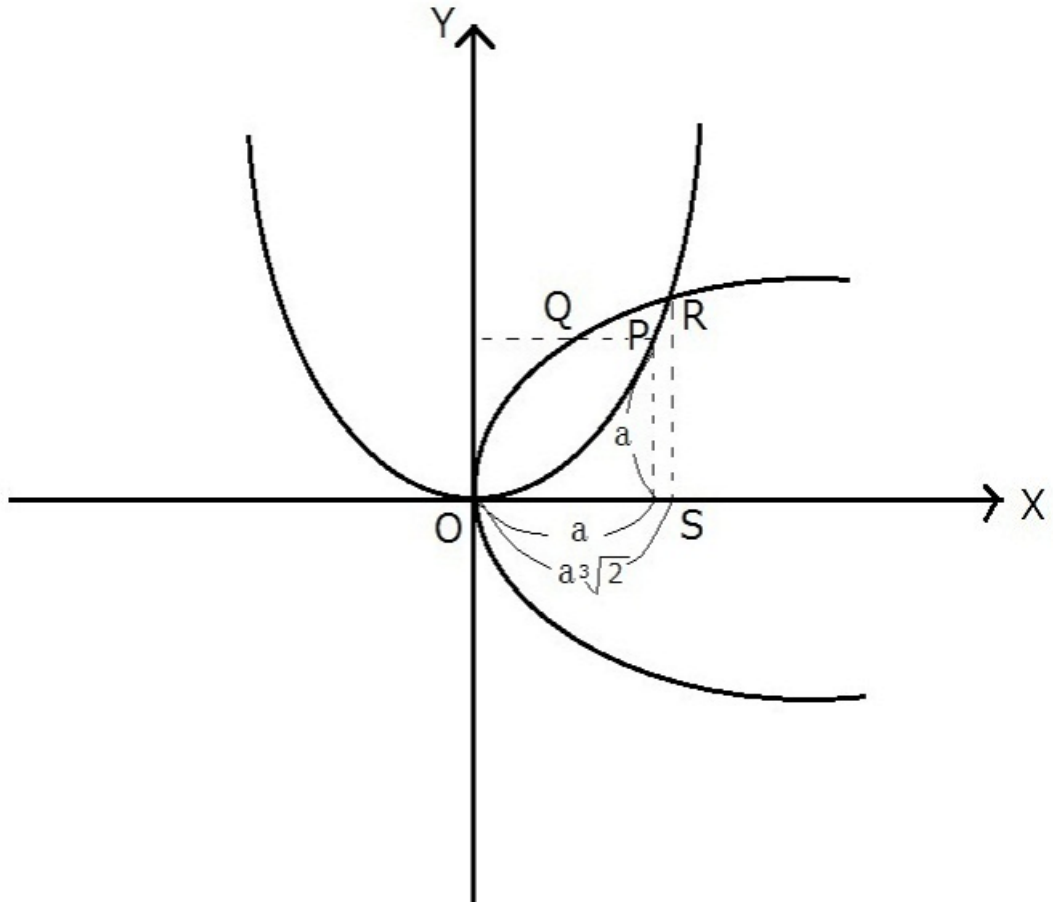
以下の二つの放物線について考える。

$$y = \frac{1}{a}x^2 \tag{4}$$

$$x = \frac{1}{2a}y^2 \tag{5}$$

式 (4) のグラフは頂点が原点の放物線で、対称となる軸は y 軸である。放物線の点の 1 つは $P(a, a)$ と書ける。式 (5) のグラフも放物線であり、頂点は原点だが、対称軸は x 軸である。点の 1 つは $Q(\frac{a}{2}, a)$ である。

[5]Menaechmus (紀元前 350 年頃) 放物線と直角の双曲線を発見したとされている。彼は倍積問題の解法でこれらを使った。



2 つの放物線の交点の x 座標は連立方程式 (4), (5) を解くことで見つけられる。(4) を (5) に代入することで $x = \frac{1}{2a}(\frac{1}{a}x^2)^2$ を得る。これは $x^4 - 2a^3x = 0$ となる。

この式の左辺を因数分解することで実数解 $0, a\sqrt[3]{2}$ を得る。原点 $(0,0)$ は明らかに交点のうちの 1 点だが、興味があるのは交点のもう 1 点である $R(a\sqrt[3]{2}, a\sqrt[3]{4})$ である。R から x 軸に垂線を引いて、その足を S とする。いま、$\overline{OS}$ の長さは $a\sqrt[3]{2}$ である。よって、$\overline{OS}$ は体積 $2a^3$ の立方体の一辺である。

メナイクモスの要求された立方体の一辺の作図は作図出来たが、放物線は定木とコンパスで作図出来ないので、その解法は定木とコンパスだけを使うことでは達成されなかった。

3. 角の 3 等分問題–与えられた任意の角を 3 等分する直線の作図問題–

ここでの角の三等分とは、任意の角の三等分線が定木とコンパスで作図可能であるかという問題である。T.L. ヒースによると、ギリシア人がこのような問題に出くわしたのは、9 の倍数の正多角形を円に内接させようと試みたときであった。正 9 角形の中心角は 40 度である。120 度の作図は可能なので、これの 3 等分が考え

られたことが始まりである。この作図問題はワンツェル[6]によって 19 世紀に解決され、それは定木とコンパスを有限回使用して作図することは不可能であるという証明だった。なお、不可能であることが証明されているにも関わらず、いまだに角の三等分は作図可能であることを示そうとする人々がおり、この人たちは trisector と呼ばれている。また、任意の角の三等分の作図という問題であるにも関わらず、少なくとも一つの角の三等分の作図と勘違いし、直角などの三等分の作図が出来ればこの問題が解けたと思う人もいる。
また、無限等比級数 $\frac{1}{3} = (\frac{1}{2})^2 + (\frac{1}{2})^4 + (\frac{1}{2})^6 + (\frac{1}{2})^8 + \cdots$ より、角の二等分を無限回繰り返すことで角の三等分が可能になるが、有限回の操作で作図しなければならないので、これも許されていない。
角の三等分と倍積問題の証明は、1837 年にフランスの数学者であるワンツェルが作図不可能であるということを示した。この証明を公表したのは、ワンツェルが 23 歳の工学部の学生の頃だった。また、ガウス[7] は正 n 角形が作図可能であるための必要十分条件は n が 2 の冪と相異なるフェルマー素数の積であり、正 17 角形の作図が出来ることも発見した。後で詳しく説明する。

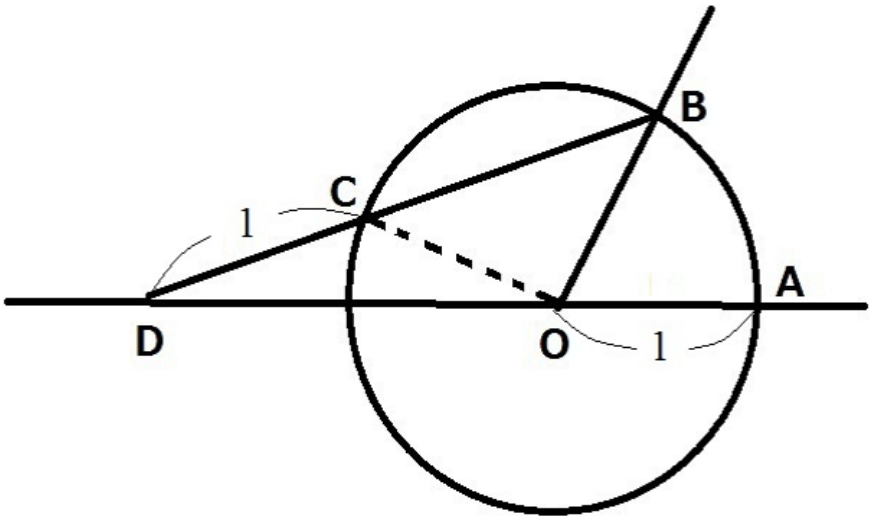
ガウス

つまり、定木とコンパスでは三大作図問題はすべて作図不可能であることが示された。

次に、定木とコンパス以外の特殊な道具を使用した解法を紹介する。

・アルキメデス[8]の解法

[6]Pierre Wantzel（1814-1848 年）パリ出身のフランス人数学者
[7]Carl Friedrich Gauss (1777-1855) ドイツの数学者、天文学者、物理学者で、最も偉大な貢献をしたのは数論の分野である。
[8]Archimedes (紀元前 287-212 年) 古代ギリシャの数学者で、円周率の近似値計算や級数を用いて放物線の面積を求める取り尽くし法を考案した。

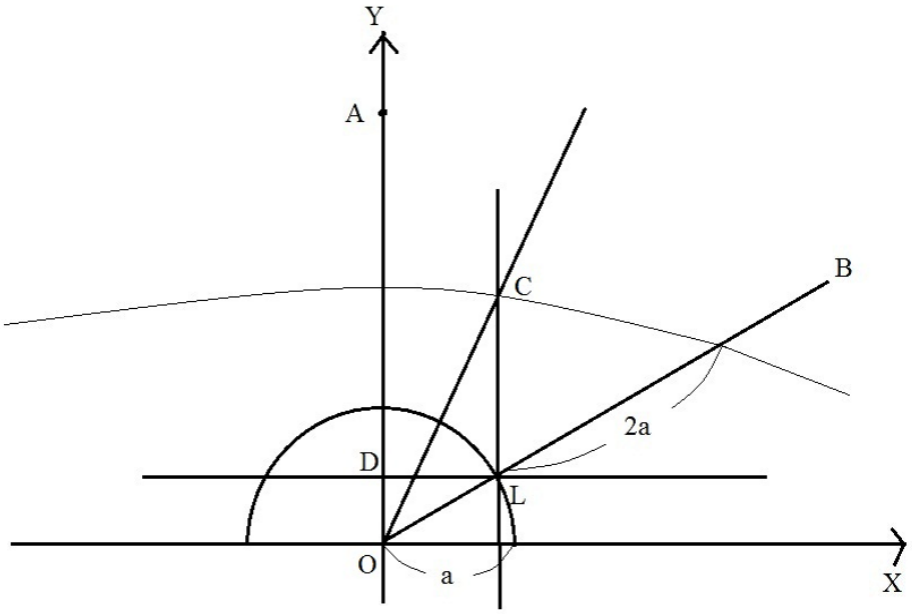


図で$\angle AOB$が与えられた角とする。中心をOで半径1の円を描く。点CとDを、Cは円周上でDは$\overline{AO}$の延長上にあり、$CD=1$であり、直線CDがBを通るように選ぶ。このとき$\angle ADB$=$\frac{1}{3}\angle AOB$である。これは以下のように示される。
$DC=CO=OB=1$なので三角形DCOと三角形COBは共に二等辺三角形である。したがって、$\angle ODC=\angle COD$と$\angle OCB=\angle CBO$である。三角形の外角の大きさは離れた2つの内角の大きさの和に等しい。つまり、

$$\begin{aligned} & \angle AOB \\ = \ & \angle ODC+\angle CBO \\ = \ & \angle ODC+\angle OCB \\ = \ & \angle ODC+\angle ODC+\angle COD \\ = \ & 3\angle ODC \\ = \ & 3\angle ADB \end{aligned}$$

よって$\angle ADB=\frac{1}{3}\angle AOB$である。
この作図を行うために、定規に距離が 1 である二点に印をつけておく。片方の点を直線OA上に、もう片方の点を円上においたまま定規をスライドさせ、定規が定める直線がBを通るようにすればよいのである。

・ニコメデスの解法



ニコメデスのコンコイドと呼ばれる曲線を使うことで$\angle AOB$の三等分線の作図が達成出来た。

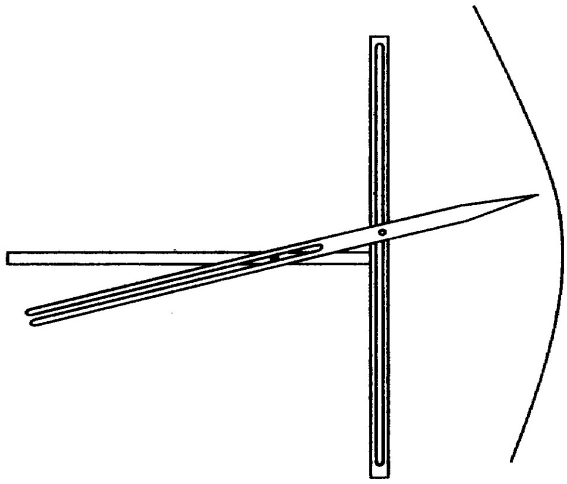
1. XY座標を描き、OY上に点Aを定める。線分OBを引き、三等分する角を$\angle AOB$とする。

2. Oを中心に半径aの円を描く。円と線分OBの交点をLとする。LからX軸に平行な線を描き、Y軸との交点をDとする。

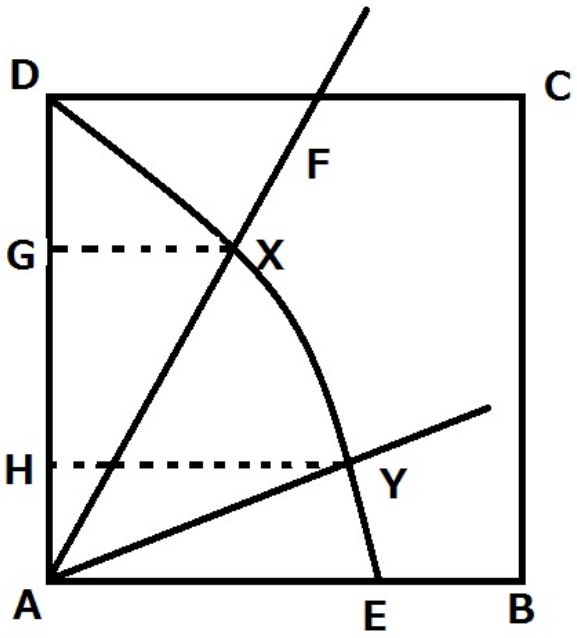
3. Oを基点としたポールを想定し、線分DLと交わる点からの長さが$2a$となるような点の軌跡がコンコイドである。

4. 点LからY軸に平行な線を引き、コンコイドとの交点をCとする。線分OCが$\angle AOB$を三等分する。

このコンコイド曲線を描くための器具が図のようなものである。



・円積曲線の解法



古代ギリシャ人は円積問題と角の三等分問題の両方を円積曲線で解いた。円積

曲線はヒッピアス[9]によってつくりだされた。これは上の図のような曲線である。正方形 ABCD があり、線分 $\overline{AD}$ を $\overline{AB}$ まで点 A を中心に等速に回転させ、また線分 $\overline{DC}$ を $\overline{AB}$ まで等速に平行に動かす。2 つの線分は同時に動かし、同時に目的地に達するものとする。この 2 つの線分の交点の集合を円積曲線という。

円積曲線の定義は

$$arcDF : arcDB = DG : DA$$

である。

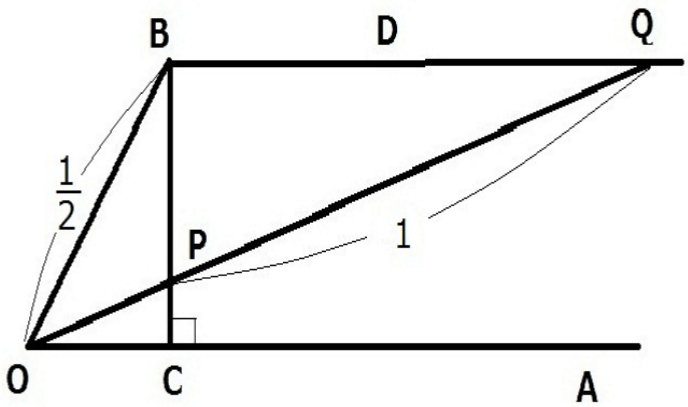
与えられた角 BAF は以下のように三等分される。

1. 正方形 $ABCD$ を作図する。
2. 円積曲線 DE を描いて、X は $\overrightarrow{\mathrm{AF}}$ との交点とする。
3. $\overline{XG}$ を $\overline{BA}$ に平行に描く。
4. $AH = \frac{1}{3}AG$ となるような点 H を $\overline{AD}$ 上に作図する。
5. $\overline{AB}$ に平行に $\overline{HY}$ を描く（Y は円積曲線上にある。）
6. $\overrightarrow{\mathrm{AY}}$ を描く。

このとき $\angle BAY$ は要求された角である。もちろん私たちは円積曲線を定木とコンパスで作図出来ないので角の三等分は出来ない。

・ネウシス作図の解法

ネウシス作図とは、ある点を通る直線上に、一定の条件を満たすように、定められた長さの線分を作図する方法である。



図の $\angle AOB$ は三等分したい角である。$OB = \frac{1}{2}$、線分 $\overline{BC}$ は半直線 $\overrightarrow{\mathrm{OA}}$ に垂直で、

[9]Hippias (紀元前 420 年頃)

半直線 $\overrightarrow{\mathrm{BD}}$ は半直線 $\overrightarrow{\mathrm{OA}}$ に平行であるように描く。ネウシスの作図法も定木とコンパスのみでの作図は不可能で、定規に距離 1 の点を 2 点印をつけて、半直線 $\overrightarrow{\mathrm{OA}}$ 上に定規を置き、点 O を通りながら目盛りの片方を線分 $\overline{BC}$ 上を動かし、もう片方の目盛りが半直線 $\overrightarrow{\mathrm{BQ}}$ 上にくるまで定規をスライドさせて、定規と線分 $\overline{BC}$ との交点を P とする。$\angle AOQ = \frac{1}{3}\angle AOB$ である。

なぜなら、まず線分 PQ の中点を M とする。すると

$$MB = MP = MQ = OB = a$$

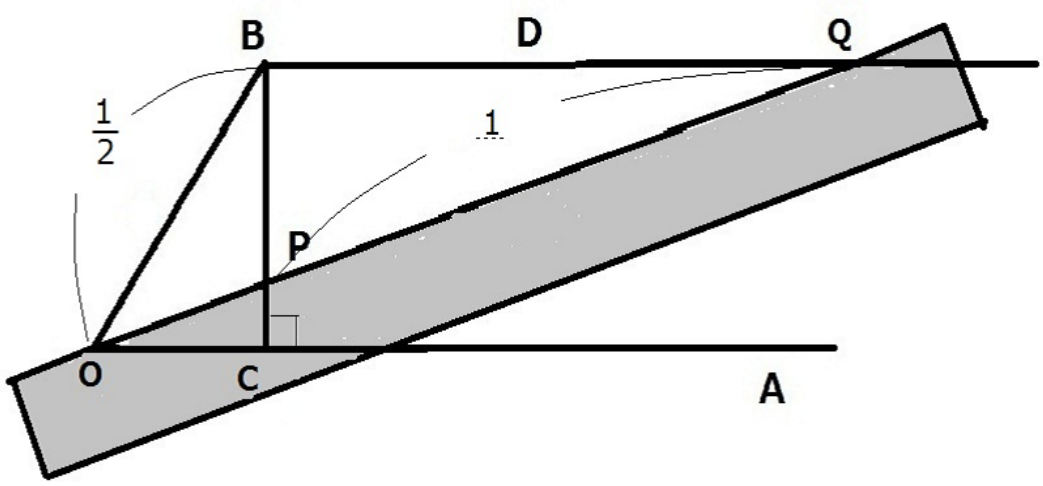
となるので、

$$\angle MQB = \angle MBQ,\ \ \angle BMO = \angle BOM$$

である。よって

$$\angle BMO = \angle MQB + \angle MBQ = 2\angle MQB$$

である。$\overrightarrow{\mathrm{BQ}}$ と $\overrightarrow{\mathrm{OA}}$ は平行なので、$\angle MQB = \angle AOQ$ である。また $\angle BOM = \angle 2AOQ$ である。よって $\angle AOQ = \frac{1}{3}\angle AOB$ である。



目盛りつき定規とは2ヶ所に印のついただけの定規とする。この定規は与えられた 2 点を通る線分を引き、線分に目盛り 1 の印をつけることができる。この目盛り付き定規を使えば、2 点を通る線分や、平行線、垂線を描くことが出来て、コンパスがないのに、あたかもコンパスがあるときと同じことが出来る。今回はこの道具を使用して、何がどこまで可能かを調べることにする。この目盛り付き定規の使用を許せば、角の三等分と倍積問題は作図可能になる。しかし、円積問題は作図不可能である。

2 RC points

この章ではコンパスと定木で作図可能な点について考える。まずはコンパスでできること、定木でできることについて述べておく。

定義 2.1 コンパスは与えられた 2 点のうち、一方を中心、もう片方を通るような円を描くことだけが可能な道具である。定木は与えられた 2 点を通る直線を引くことだけが可能な道具であり、長さを測ることはできないものとする。

定義 2.2 RC point とは $P_1 = (0, 0)$, $P_2 = (1, 0)$ か、ある $n \geq 3$ に対して、$(*)$ が成り立つ有限点列 $P_3, \ldots, P_n$ がある時の P_n のことをいう。

$(*)$ 各 $i = 3, \ldots, n$ に対して次の (1), (2), (3) のどれかが成立する。

(1) $P_1, \ldots, P_{i-1}$ のうち異なる 2 点を通る直線と、$P_1, \ldots, P_{i-1}$ のうち異なる 2 点を通る直線が唯一点で交わるとき、その交点を P_i とおく。

(2) $P_1, \ldots, P_{i-1}$ のうち異なる 2 点を通る直線と、$P_1, \ldots, P_{i-1}$ の中のある点を中心、別のある点を通るような円との交点の一つを P_i とおく。

(3) $P_1, \ldots, P_{i-1}$ の中から Q_1, Q_2, Q_3, Q_4 をとり $Q_1 \neq Q_3$ のとき Q_{1Q_2} と Q_{3Q_4} の交点の一つを P_i とおく。

ここで Q_{1Q_2} とは、中心が Q_1 で Q_2 を通る円のことである。

定義 2.3 RC line とはある 2 つの異なる RC point を通る直線のことをいう。

RC circle とは中心が RC point かつ他のある RC point を通る円のことをいう。

x が RC 数とは $(x, 0)$ が RC point であることとする。

ここで RC 数と RC point の関係について調べる。次の定理は定義から明らかであろう。

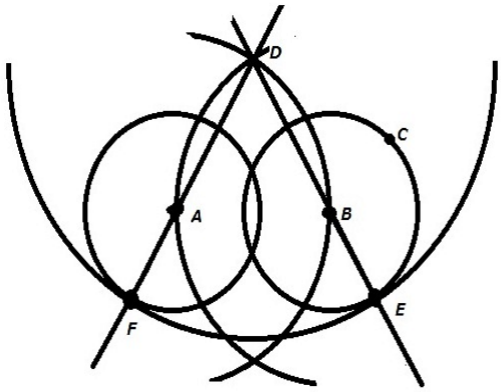
定理 2.4 (1) 2 つの異なる RC line の交点は RC point。

(2) RC line と RC circle の交点は RC point。

(3) 異なる RC circle と RC circle の交点は RC point。

定理 2.5 A, B, C は RC point とする。A_{BC} (中心 A、半径 BC の円) は RC circle である。

証明

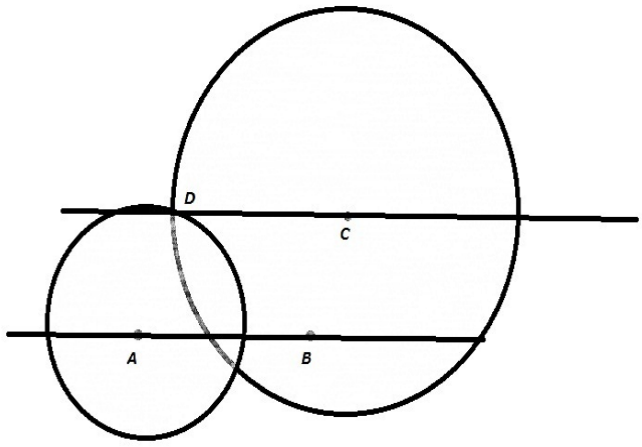


A_B, B_A を描き、その交点を D とおく。D は RC point である。直線 DB と B_C との交点を E とする。ただし E は B が D と E の間に存在するようにとる。D_E と DA の交点を F とおく。ただし F は A が D と F の間に存在するようにとる。

ここで $DE = DF$, $DB = DA$ より $BC = BE = AF$ であるので $A_F = A_{BC}$ は RC circle である。 **証明終**

補題 2.6 3 つの異なる RC point A, B, C が与えられているとき、C を通り AB に平行な RC line を引くことができる。

証明



A_{BC}, C_{AB} をそれぞれ描きその交点を D とおく。

このとき $DC = AB$, $DA = CB$ なので、2 組の対辺の長さがそれぞれ等しくなるので四角形 $ABCD$ は平行四辺形である。

A_{BC}, C_{AB} はそれぞれ RC circle なので D は RC point である。よって DC は RC line である。これが求める直線である。 **証明終**

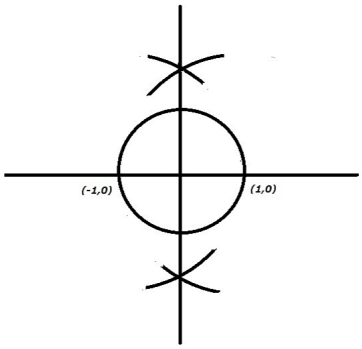
命題 2.7 (1) 座標軸は RC line である。

(2) $(p,0)$, $(-p,0)$, $(0,p)$, $(0,-p)$ のうちどれか一つでも RC point ならば、すべて RC point である。

(3) (p,q) が RC point であることと、p, q はともに RC 数であることは同値である。

(4) 整数は RC 数である。

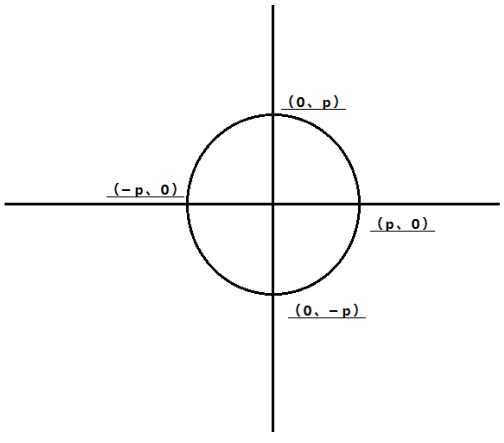
証明　まず、(1) を示す。



x 軸は $(1,0)$, $(0,0)$ を通る直線を描くことで得られる。$(-1,0)$ は、中心 $(0,0)$ で $(1,0)$ を通る円と x 軸との交点なので RC point である。

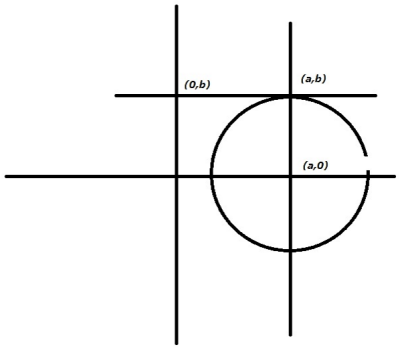
中心 $(1,0)$ で $(-1,0)$ を通る円と、中心 $(-1,0)$ で $(1,0)$ を通る円の 2 つの交点は RC point で、この 2 点を通る直線は RC line になるが、これは明らかに y 軸である。

次に、(2) を示す。



$(p,0)$ が RC point であるとする。中心 $(0,0)$ で $(p,0)$ を通る円を描けば、円と座標軸の交点はそれぞれ $(p,0)$, $(0,p)$, $(-p,0)$, $(0,-p)$ となる。

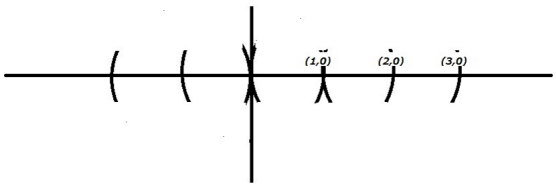
次に、(3) を示す。



(a,b) が RC point とする。(a,b) を通り x, y 軸に平行な線を引けば、それぞれの直線と座標軸との交点は $(a,0)$, $(0,b)$ である。したがって (2) より、$(a,0)$, $(b,0)$ は RC point である。したがって a, b は RC 数である。

逆のことをやれば、a, b は RC 数であるなら (a,b) が RC point であることがわかる。

(4) を示そう。



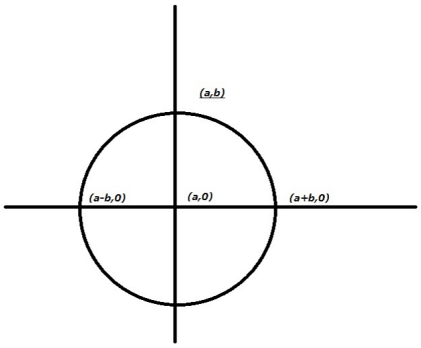
中心 $(1,0)$ で $(0,0)$ を通る円は $(2,0)$ を通る。したがって 2 が RC 数であることが分かる。中心 $(2,0)$ で $(1,0)$ を通る円は $(3,0)$ を通る。したがって 3 が RC 数であることが分かる。この作業を繰り返すことによって 0, 1, 2, 3, ... は RC 数である

ことがわかる。(2) により $-1, -2, -3, \ldots$ も RC 数 であることがわかる。従って整数は RC 数である。 **証明終**

命題 2.8 RC 数全体からなる集合は、実数体 $\mathbb{R}$ の部分体をなす

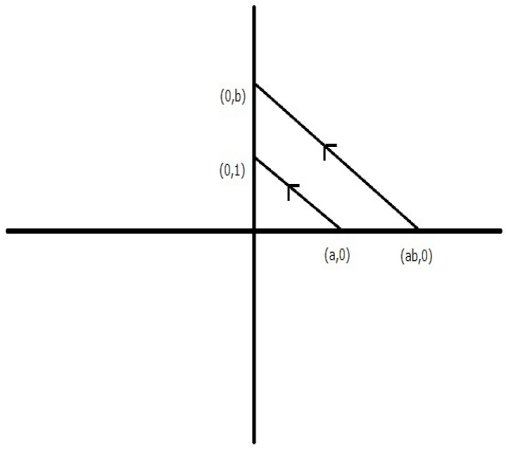
証明　和、差、積、割り算は、それぞれ次のようにして作図できる。a, b は RC 数とする。

まず、和と差を作図する。

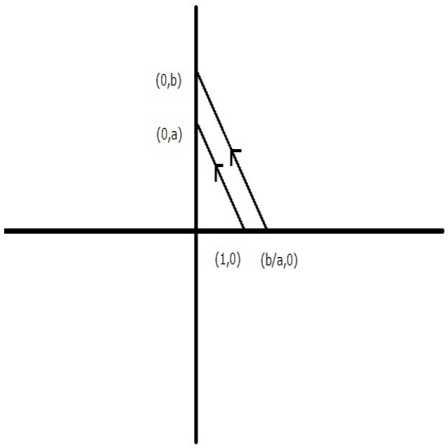


命題 2.7 (3) によって、(a, b) は RC point である。$(a, 0)$ を中心とし (a, b) を通る円を描くと、円と x 軸との交点は $(a + b, 0)$, $(a - b, 0)$ である。よって、$a + b$, $a - b$ は RC 数である。

次に、積と商を作図する。



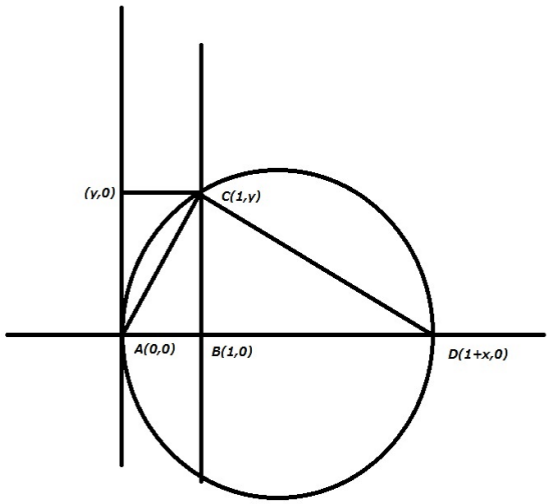
$(0,1)$, $(a,0)$ を通る直線に平行で、$(0,b)$ を通る直線を描く。直線と x 軸との交点は $(ab,0)$ である。



$(0,a)$, $(1,0)$ を通る直線に平行で、$(0,b)$ を通る直線を描く。直線と x 軸との交点は $(b/a,0)$ である。 **証明終**

命題 2.9 正の実数 x が RC 数ならば $\sqrt{x}$ は RC 数である。

証明



A は $(0,0)$, B $(1,0)$, D は $(1+x,0)$ とする。AD を直径とする円は、RC circle である。B を通り y 軸と平行な直線と円との交点を $C(1,y)$ とおく。

$AB:BC=CB:BD$ より $1:y=y:x$ なので $y=\sqrt{x}$ となる。よって $\sqrt{x}$ は RC 数である。 **証明終**

定義 2.10 $\mathbb{R}$ の部分体 F が

$$x \in F \text{ かつ } x > 0 \text{ ならば } \sqrt{x} \in F$$

を満たすとき、F は euclidean という。

命題 2.9 により、RC 数全体は euclidean である。

定義 2.11 $p + iq \in \mathbb{C}$ が RC 複素数とは (p, q) が RC point であることをいう。

定理 2.12 RC 複素数全体は $\mathbb{C}$ の部分体をなす。

証明　和、差、積で閉じていることは明らかであろう。

商のみ示す。$p_1 + iq_1$, $p_2 + iq_2$ はそれぞれ RC 複素数とする。つまり p_1, p_2, q_1, q_2 は RC 数とする。

$p_2 + iq_2 \neq 0$ とする。すると、p_2, q_2 のうち少なくとも一方は零でないので、$p_2^2 + q_2^2 \neq 0$ としてよい。すると、

$$\begin{aligned} & (p_1 + iq_1)/(p_2 + iq_2) = \{(p_1p_2 + q_1q_2) + i(-p_1q_2 + p_2q_1)\}/(p_2^2 + q_2^2) \\ = \ & (p_1p_2 + q_1q_2)/(p_2^2 + q_2^2) + i(-p_1q_2 + p_2q_1)/(p_2^2 + q_2^2) \end{aligned}$$

p_1, p_2, q_1, q_2 が RC 数であるので、$(p_1p_2+q_1q_2)/(p_2^2 + q_2^2)$ と $(-p_1q_2+p_2q_{1)})/(p_2^2 + q_2^2)$ は RC 数である。

したがって RC 複素数は体をなす。　**証明終**

定義 2.13　(1) F を $\mathbb{R}$ の部分体とする。ある自然数 n と体の列

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n \subset \mathbb{R}$$

が存在して、各 i に対して F_i が F_{i-1} の二次拡大であるとき、F_n は F 上二次拡大の繰り返しで得られる $\mathbb{R}$ の部分体であるという。$\mathbb{Q}$ 上二次拡大の繰り返しで得られる $\mathbb{R}$ の部分体すべての和集合を $\mathbb{E}$ と書く。

(2) F を $\mathbb{C}$ の部分体とする。ある自然数 n と体の列

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n \subset \mathbb{C}$$

が存在して、各 i に対して F_i が F_{i-1} の二次拡大であるとき、F_n は F 上二次拡大の繰り返しで得られる $\mathbb{C}$ の部分体であるという。$\mathbb{Q}$ 上二次拡大の繰り返しで得られる $\mathbb{C}$ の部分体すべての和集合を $\mathbb{E}'$ と書く。

$\mathbb{E}$ は $\mathbb{R}$ の部分体である。また、$\mathbb{E}'$ は $\mathbb{C}$ の部分体である。また、定義より、$\mathbb{E} \subset \mathbb{E}' \cap \mathbb{R}$ である。後に系 2.18 で、$\mathbb{E} = \mathbb{E}' \cap \mathbb{R}$ であることが証明される。

補題 2.14 F を $\mathbb{R}$ の部分体とする。方程式の係数が F の元である直線と円、直線と直線、円と円の交点の座標は F の元であるか、F の 2 次拡大の元である。

証明 (1) 直線と直線の場合。
二つの直線の方程式を

$$aX + bY + c = 0,$$

$$eX + fY + d = 0$$

とおく。この 2 直線が唯一点で交わる時 $af - be \neq 0$ である。交点を (x_0, y_0) とおくと

$$\begin{aligned} x_0 &= (bg - fc)/(af - be) \\ y_0 &= (ec - ag)/(af - be) \end{aligned}$$

である。したがって、交点の座標は F の元である。
(2) 直線と円の場合。
直線の方程式を

$$aX + bY + c = 0,$$

円の方程式を

$$X^2 + Y^2 + fX + gY + h = 0$$

とする。ここで、$a, b, c, f, g, h \in F$ とする。

$$d = (b^2 f + 2ac - abg)^2 - 4(a^2 + b^2)(c^2 - bcg + b^2 h)$$

とおけば、交点 (x_0, y_0) は、

$$\begin{aligned} x_0 &= \frac{-2ac + b^2 f + abg \pm \sqrt{d}}{2(a^2 + b^2)} \\ y_0 &= \frac{-2bc - abf + a^2 g \mp \sqrt{d}}{2(a^2 + b^2)} \end{aligned}$$

である。$\sqrt{d} \in F$ なら交点の座標は F の元であり、$\sqrt{d} \notin F$ なら交点の座標は F の二次拡大の元である。
(3) 円と円の場合。
二つの円の方程式を

$$X^2 + Y^2 + aX + bY + c = 0,$$

$$X^2 + Y^2 + eX + fY + g = 0$$

とおく。この連立方程式を解くことは、

$$(a - e)X + (b - f)Y + (c - g) = 0,$$

$$X^2 + Y^2 + eX + fY + g = 0$$

を解くことと同じである。これは直線と円の交点を求める場合と同じである。

よって方程式の係数が F の元である直線と円、直線と直線、円と円の交点の座標は F の元であるか、F の 2 次拡大の元である。 **証明終**

補題 2.15 $\cos x$ が RC 数なら $\cos\frac{x}{2}$, $\sin\frac{x}{2}$ も RC 数である。

証明 $\cos^2\frac{x}{2} = \frac{1+\cos x}{2}$, $\sin^2\frac{x}{2} = \frac{1-\cos x}{2}$ であり $\frac{1+\cos x}{2}$, $\frac{1-\cos x}{2}$ はそれぞれ RC 数である。

従って $\cos\frac{x}{2} = \pm\sqrt{\frac{1+\cos x}{2}}$, $\sin\frac{x}{2} = \pm\sqrt{\frac{1-\cos x}{2}}$ も RC 数である。 **証明終**

定理 2.16 RC 数全体の集合は $\mathbb{E}$ と一致する。

証明 x を RC 数とする。$x \in \mathbb{E}$ を示す。

$P = (x, 0)$ は RC point である。P_1, P_2, …,$P_n = P$ を RC point P を定めるときの点列とする。すべての i に対し P_i の座標が $\mathbb{E}$ の元であることを n に関する帰納法で示す。

$P_1 = (0, 0)$,$P_2 = (1, 0)$ である。$0, 1 \in \mathbb{Q}$ なので $i = 1, 2$ のときは正しい。

$i > 2$ に対して $i - 1$ まで正しいとする。帰納法の仮定より、P_1, P_2, …, P_{i-1} の座標は $\mathbb{R}$ の部分体 $\mathbb{E}$ の元である。よって P_i は、方程式の係数が $\mathbb{E}$ の元である直線と直線、円と直線、または円と円の交点である。前定理により P_i の座標は、$\mathbb{E}$ の元か $\mathbb{R}$ に含まれる $\mathbb{E}$ の 2 次拡大の元である。しかし、$\mathbb{E}$ は euclidian なので、$\mathbb{E}$ の 2 次拡大は無い。よって、P_i の座標は、$\mathbb{E}$ の元である。

逆に $x \in \mathbb{E}$ なら x は RC 数であることを示す。

$x \in \mathbb{E}$ をとる。このとき

$$\mathbb{Q} = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n (\subset \mathbb{R}), \quad x \in F_n$$

という 2 次拡大の列がある。F_k の元が、すべて RC 数であることを、k に関する帰納法で示す。$k = 0$ のときは、$F_0 = \mathbb{Q}$ より、明らかである。k まで正しいとする。$k + 1$ のときを考える。F_{k+1} の元は、$x = a + b\sqrt{d}$ と書ける。ただし $a, b, d \in F_k$, $\sqrt{d} \notin F_k$ である。命題 2.9 により、d は RC 数なので $\sqrt{d}$ も RC 数である。したがって x は RC 数である。 **証明終**

これにより、$x, y \in \mathbb{R}$ に対して

$$x + iy\text{: RC 複素数} \Leftrightarrow (x, y) \text{ は RC point} \Leftrightarrow x, y \text{ は RC 数} \Leftrightarrow x, y \in \mathbb{E}$$

がわかった。

定理 2.17 RC 複素数全体は $\mathbb{E}'$ と一致する。

証明　$x, y \in \mathbb{R}$ とし、$x + iy$ は RC 複素数 とする。このとき、定理 2.16 により、$x, y \in \mathbb{E} \subset \mathbb{E}'$ である。また、$i \in \mathbb{E}'$ である。したがって $x + iy \in \mathbb{E}'$ となる。

逆に $x, y \in \mathbb{R}$ として $x + iy \in \mathbb{E}'$ とする。このとき、$\mathbb{C}$ に含まれる

$$\mathbb{Q} = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n$$

2 次拡大の列で、$x + iy \in F_n$ を満たすものがある。k に関する帰納法で、F_k のすべての元は RC 複素数であることを示す。$k = 0$ のときは、$\mathbb{Q}$ の元は、明らかに RC 複素数である。k まで正しいとする。$k + 1$ のときに考える。$F_{k+1} = F_k(\alpha)$ となる $\alpha \in \mathbb{C}$ が存在する。$\alpha^2 = p + iq$ とおくと、帰納法の仮定より $p + iq$ は RC 複素数なので、(p, q) は RC point である。したがって p, q は RC 数である。ここで

$$p + iq = r(\cos x + i \sin x) \quad (r = \sqrt{p^2 + q^2})$$

とおくと r は RC 数である。また $r \cos x = p$ なので $\cos x$ は RC 数である。このとき、補題 2.15 により、$\cos \frac{x}{2}, \sin \frac{x}{2}$ も RC 数である。よって、$\alpha = \pm\sqrt{r}(\cos \frac{x}{2} + i \sin \frac{x}{2})$ は RC 複素数である。　**証明終**

系 2.18　$\mathbb{E} = \mathbb{E}' \cap \mathbb{R}$ が成立する

証明　定義より明らかに、RC 複素数が実数なら、RC 数である。このことと、定理 2.16 と定理 2.17 より証明が完了する。　**証明終**

系 2.19　α が RC 複素数ならば $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ は 2 の冪である。

証明　これは体の拡大列 $K \subset M \subset L$ が存在したとき

$$[L : K] = [L : M][M : K]$$

が成り立つことからわかる。　**証明終**

3　MR points

定義 3.1　MR (marked ruler) point とは、次の 3 つの点

$P_1 = (0, 0)$

$P_2 = (1, 0)$

$P_3 = (0, 1)$

及び以下の条件 $(*)$ を満たす点 Q のことである。

$(*)$ ある整数 $n \geq 4$ について、$P_n = Q$ かつ $i = 4, \cdots, n$ に対して、以下の (1) 又は (2) を満たす点列 $P_1, P_2, \cdots, P_n$ が存在する。

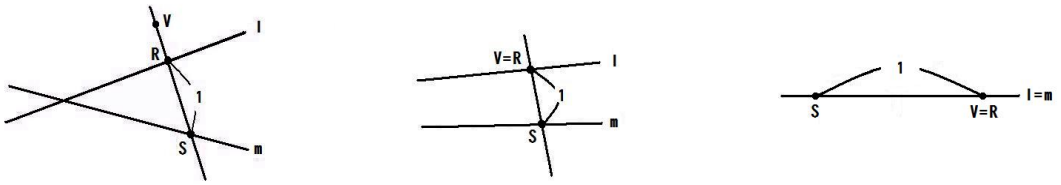
(1) $P_1, \cdots, P_{i-1}$ の中の異なる 2 点を通る異なる 2 つの直線が唯 1 つの点で交わっているとき、その点を P_i とする。

(2) 次の 3 条件をすべて満たすような異なる 2 点 R, S をとり、そのどちらかを P_i とする。

(i) 2 点 RS 間の距離は定規 1 目盛である。

(ii) $P_1, \cdots, P_{i-1}$ の中のいずれかの 1 点 V と R, S は同一直線上にある。

(iii) $P_1, P_2, \cdots, P_i$ のうち異なる 2 点を通る直線 l, m があって、$R \in l, S \in m$ である。$V \in l$ なら $V = R$ とする。$V \in m \setminus l$ となるケースは考えない。



定義 3.2 MR line とは、2 つの異なる MR point を通る直線のことをいい、MR circle とは、MR point を中心とし、他の MR point を通る円のことをいう。また、x が MR 数とは、$(x, 0)$ が MR point のことをいう。

定義 3.3 $p, q \in \mathbb{R}$ とする。$p + iq$ が MR 複素数であるとは、(p, q) が MR point であることとする。

MR line と MR line が 1 点で交わるとき、その交点が MR point であることは定義から明らかである。MR circle については次が成立する。

定理 3.4 MR circle と MR line の交点は MR point であり、MR circle と MR circle の交点もまた MR point である。

証明　次の (1) から (6) を順に示す。

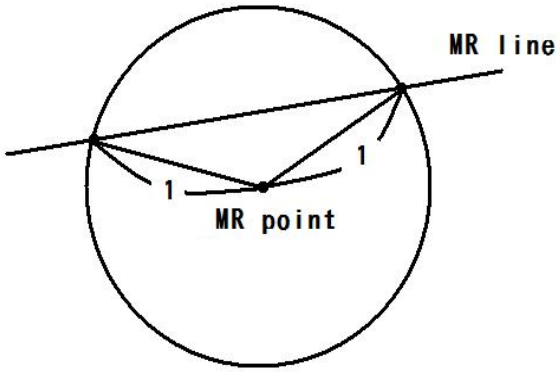
(1) MR point が中心の半径 1 の円と MR line との交点は MR point である。

(2) ある MR line l と l 上にない MR point P があるとする。このとき、P を通り、l と平行な直線は MR line である。

(3) ある MR point を通り、ある MR line と直交する直線は MR line である。

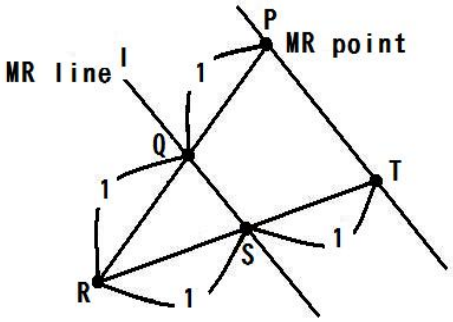
(4) MR 数は加減乗除で閉じている。
(5) MR circle と MR line との交点は MR point である（相似拡大と (1) を使う）。
(6) MR circle と MR circle の交点は MR point である。

(1) 下図の円と MR line の交点は、円の半径が 1 なので、定義 3.1 の (ii) より MR point である。



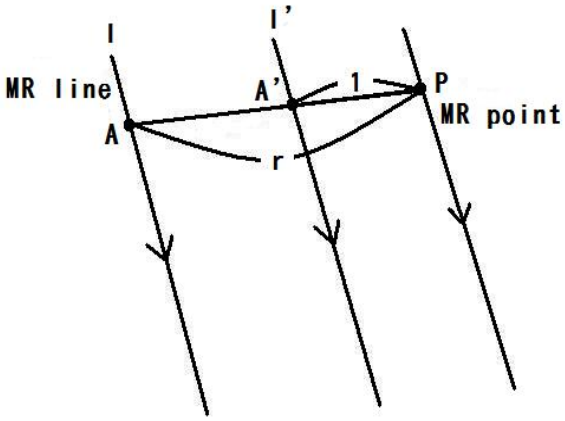
(2) を示す。まず、MR point P と MR line l の距離が 1 未満の場合を考える。

MR point P から MR line l まで長さ 1 の点 Q は MR point である。直線 PQ 上で Q からの距離が 1 になり、P の逆側にある点 R は MR point であって、さらにこの MR point R から MR line l まで長さ 1 の点 $S(S \neq Q$ にとる) は MR point である。同様に直線 RS 上にあって S からの距離が 1 で R と逆側にある点 T も MR point であり、MR point P と MR point T を通る直線を考えると、それはもとの MR line l に平行な直線であり、かつ MR line となる。



次に、MR point P と MR line l の距離が 1 以上の場合を考える。

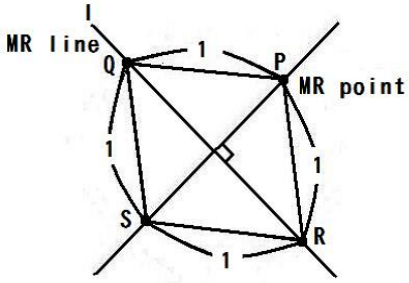
与えられた MR line l 上に MR point A をとる。点 A と与えられた MR point P を結ぶ。直線 PA の長さを r とする。この点 P から直線 PA 上に長さ 1 となる点 A' をとるとこれは MR point である。直線 AA' の長さは $r-1$ であり、$r-1<1$ ならば上の＜距離が 1 未満の場合＞を使って、点 A' を通り直線 l に平行な直線を引くことができ、その直線を l' とすると l' も MR line である。$r-1\geq 1$ ならば、点 A' から直線 AA' 上に長さ 1 となる点 A'' をとり、上の操作を繰り返す。直線 PA' の長さが 1 より、同様に＜距離が 1 未満の場合＞を使って、点 P を通り直線 l に平行な直線を引くことができ、この直線は MR line である。



(3) 与えられた MR point P と MR line l との距離を r とすると、(2) を用いることにより、$0\leq r<1$ としてよい。

- $0<r<1$ のとき

  MR point P から MR line l までの長さが 1 の点 Q,R を見つける。点 Q を通り、PR との平行線を作図し、点 R を通り PQ との平行線を作図して、交点を S とおくと PS が垂線であり、この垂線は MR line である。



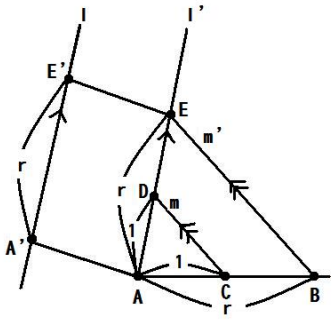
- $r=0$ のとき

  MR line l 上にない MR point Q をとる。すると MR line l と MR point Q の距離は 0 でないので、(2) より MR point Q を通り、MR line l と平行である

MR line l' が書ける。MR line l' 上には、少なくとも 2 点以上の MR point がある。よって、Q は、P から MR line l' へ引いた垂線の足ではないとする。

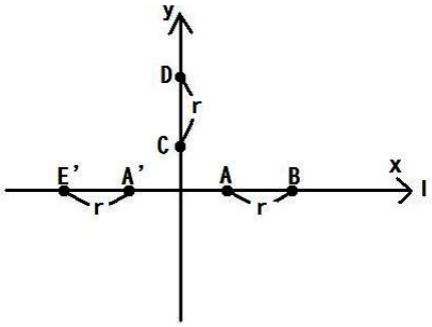
すると、線分 PQ 上に、MR line l との距離 s が $0 < s < 1$ を満たす点 R が取れる。R を通り、MR line l と平行な MR line l'' を作図する。P から MR line l'' に垂線を引けばよい。

(4) MR 数が加法と減法について閉じていることを示すための “準備” をする。まず、MR line l と l 上の MR point A' をとり、2 つの MR point A、B の 2 点間の長さを r とする。このとき、$A'E'$ の距離が r である l 上の点 E' は MR point であることを示したい。まず、直線 l と AB が一致しない場合を考える。線分 AB 上、または点 B を通る線分を延ばし、点 A から長さが 1 となる AB 上の点を C とすると、C は MR point である。次に MR line l に対して、A を通るような平行線 l' を引き、A から l' 上に長さ 1 の点 D をとると D も MR point である。C と D を結び、その線分 m に対して、B を通るような平行線 m' を引く。m' と l' の交点を E とすると、A と E の距離は r である。A と A' を通る直線を引き、E を通り直線 AA' と平行な直線を引く。l とその直線の交点を E' とすると A' と E' の距離は r である。つまり、A' との距離が r である l 上の点は MR point である。(下の図は $r > 1$ の場合の図であるが、$r < 1$ でも同様である。また、l と AB が平行であれば、$D = C$, $E = B$ となるが、この場合も同じようにできる。)



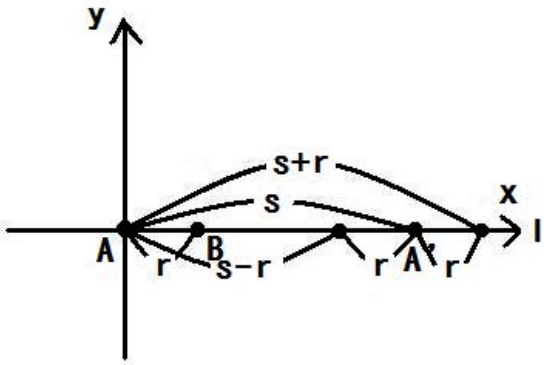
次に直線 l と AB が一致する場合を考える。このときは l を x 軸あるいは y 軸に変えて上の議論を行う。(x 軸と y 軸は共に MR line であり、どちらかは l と一致しない。) すると距離が r になる MR point C,D が l の外にとれる。次に、MR point C、D を用いて l 上に $A'E'$ の距離が r になるように E' をとる。下の図は、y 軸を

直線 l の代わりに用いた図である。



この議論により、2 つの MR point の距離は MR 数になることに注意する。

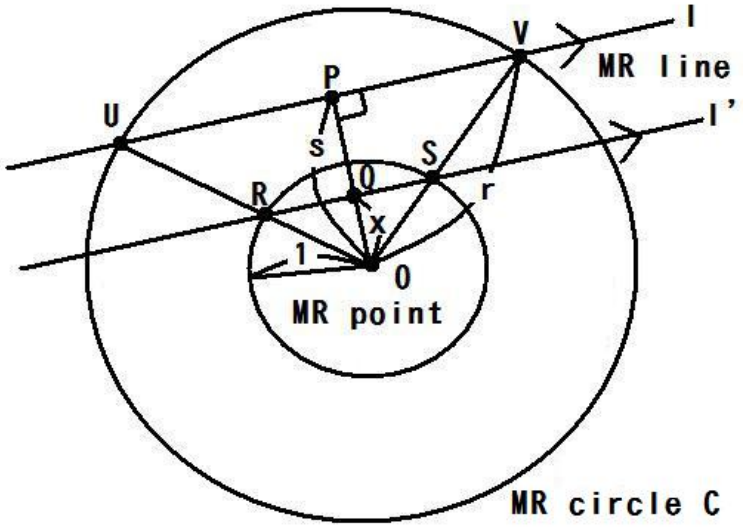
さて、s, r を MR 数とする。上の議論より、l を x 軸、A' は $(s,0)$、A は $(0,0)$、B は $(r,0)$ とすれば、$(s+r,0)$、$(s-r,0)$ は共に MR point であることがわかり、$s+r$、$s-r$ は MR 数であることがわかる。



次に、乗法、除法について考える。a, b を MR 数とする。a, b は正の数としよう。(a あるいは b が負でも同様にできる。) すると、“準備”の議論により $(0,1)$, $(0,a)$, $(0,b)$ は MR point であることに注意する。平行線の作図が可能であるので、RC のケースと同様に ab, a/b が MR 数であることが証明できる。

(5) 与えられた MR circle C の中心 O を中心とした半径 1 の円を書く。MR line l と MR circle C の交点を U, V とし、交点 U, V と MR circle の中心 O をそれぞれ結ぶ。このとき、単位円との 2 つの交点を R, S とし、R と S を通る直線 l' はもとの MR line l と平行になる。次に、中心 O から MR line l に垂線を下ろすと (3) よりこの垂線は MR line となる。MR line と MR line の交点は MR point なので、この垂線の足 P は MR point である。よって、中心 O とこの交点の長さ s は MR 数となる。(ここで (4) の中の “準備”を使っている) MR circle C の半径 r も MR 数なので (4) より、s/r も MR 数となる。これは相似拡大を考えたとき、円の中心 O と平行線 l' との距離 x となることがわかる。従って、平行線 l' と垂線の交点 Q は MR point である。l' は直線 OP の点 Q から引いた OP の垂線なので、(3) よ

り l' は MR line となり、(1) より単位円と平行線の交点 R, S は MR point となる。よって、OS と OR を結ぶ直線は MR line となる。MR circle C と MR line l の交点は直線 OS あるいは OR 上にある。MR line と MR line の交点は MR point より、MR circle C と MR line l との交点 V、U は MR point である。

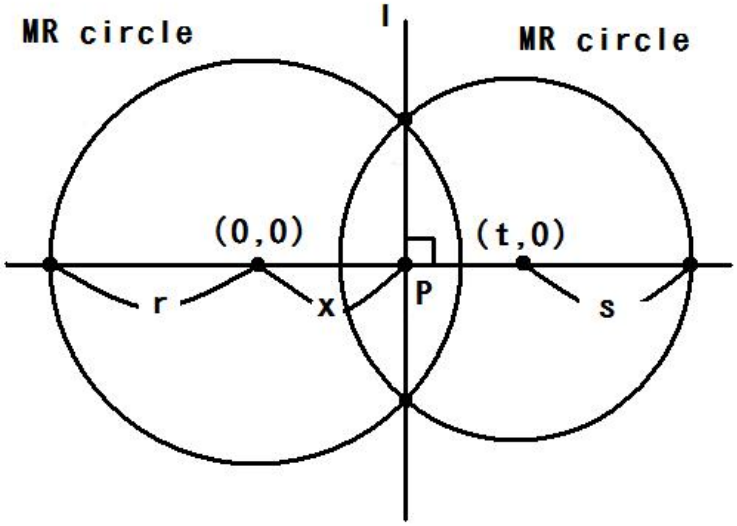


(6) 2 つの MR circle を与える。一方を $(0,0)$ 中心の半径 r の円、もう一方を $(t,0)$ 中心の半径 s の円としよう。(一般の場合も証明は同じであるので、この場合のみ証明する。)

2 つの円の中心間の距離は t となる。円の方程式 $x^2+y^2=r^2$、$(x-t)^2+y^2=s^2$ から $(x-t)^2-x^2=s^2-r^2$ が得られ、$2tx=s^2-r^2-t^2$ となる。

従って、$x=(s^2-r^2-t^2)/2t$ を得る。(4) より $(s^2-r^2-t^2)/2t$ は MR 数である。$((s^2-r^2-t^2)/2t,0)$ を点 P をとおく。すると、点 P は MR point である。y 軸と平行な直線で P を通る MR line l を引く。最初にとった 2 つの MR circle の交点は、この MR line l 上にある。よって、2 つの MR circle の交点を求めるには、片方の MR circle と MR line l との交点を求めればよい。(5) の議論により、交点は

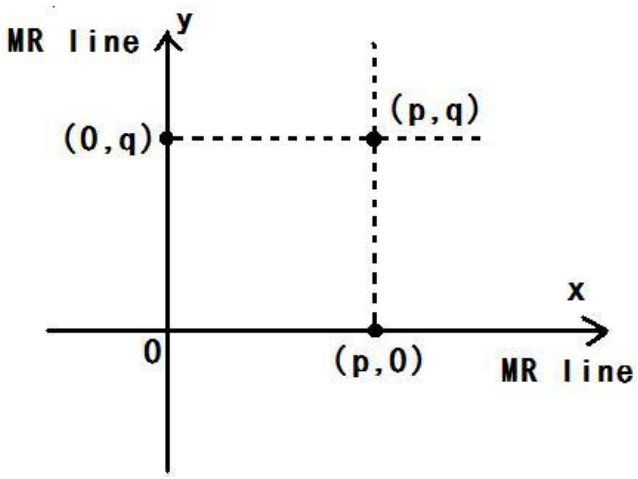
MR point である。



以上より、MR circle と MR line の交点は MR point であり、MR circle と MR circle の交点もまた MR point である。 **証明終**

定理 3.5 (p,q) が MR point であることと、p,q が MR 数であることは同値である。

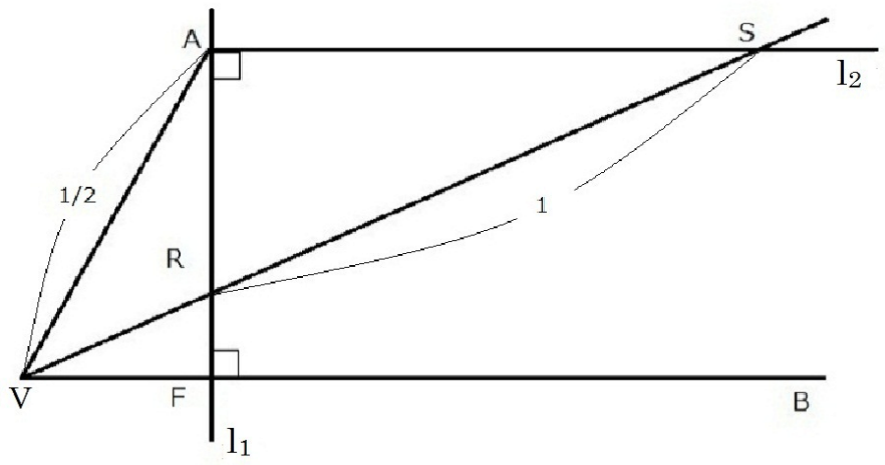
証明 $(\Rightarrow)$ (p,q) は MR point であり、y 軸と x 軸は共に MR line であるので、(2) を使うことができる。(p,q) を通り y 軸と平行な直線は MR line となり、この直線と x 軸との交点 $(p,0)$ は MR point になる。同様に (p,q) を通り x 軸と平行な直線は MR line となり、この直線と y 軸との交点 $(0,q)$ は MR point になる。(4) の議論により、$(q,0)$ も MR point になることに注意する。よって p,q は MR 数になる。



($\Leftarrow$) p, q が MR 数であるので、$(p,0)$、$(q,0)$ は MR point である。原点が中心で半径 q の円は MR circle であり、それと y 軸との交点である $(0,q)$ は MR point である。さらに定理 3.4 の (2) より、$(p,0)$ を通り y 軸に平行な直線と $(0,q)$ を通り x 軸に平行な直線をそれぞれ引くことができ、その交点である (p,q) は MR point である。 **証明終**

Marked Ruler だけで、定木とコンパスによりできることはできるので、コンパスはあると考えてもよい。よって、MR 数の集合は加減乗除で閉じているから体である。さらに、RC 数と同様の方法で、MR 数の集合はルートで閉じていることもわかる。すなわち MR 数の集合は、euclidean である。

定理 3.6 $AV = \dfrac{1}{2}$、$\angle AVB$ は鋭角とする。A から直線 VB におろした垂線の足を F とし、直線 FA を l_1 とおく。また、点 A での l_1 の垂線を l_2 とおく。R は線分 AF 上の点、S は直線 VR と l_2 の交点とし、$RS = 1$ と仮定する。このとき、直線 VR は、$\angle AVB$ の三等分線の一本である。



証明　$\angle BVS = t$ とする。このとき、$\angle VSA = t$ である。M を線分 RS の中点とすると、$\angle RAS$ は直角より、点 A は線 RS を直径とする円周上の点である。よって、$MA = MR = MS = VA = \dfrac{1}{2}$ であるから、$\triangle AMS$ と $\triangle MAV$ は二等辺三角形となる。したがって $\angle MAS = t$、$\angle VMA = \angle AVM = 2t$ となる。よって、直線 VR は $\angle AVB$ の三等分線の一本である。 **証明終**

系 3.7 $\cos x$ は MR 数とする。このとき、$\cos\dfrac{x}{3}$ は MR 数となる。

証明　$\cos x$ を MR 数とする。

x を鋭角とする。ここで、$\dfrac{1}{2}$, $\cos x$ は MR 数であるから $\dfrac{1}{2}\cos x$ も MR 数であり、$\left(\dfrac{1}{2}\cos x, 0\right)$ は MR point となる。上の図において、点 V を $(0,0)$、点 F を

$\left(\frac{1}{2}\cos x, 0\right)$ とする。このとき図における各点は MR point、各直線は MR line としてとれる。$\angle AVF = x$ であり、定理より直線 RS は x を三等分し、$\angle BVS = \frac{x}{3}$ となる。線分 VS 上に、点 V からの距離が 1 となる点 T をとる。T も MR point である。T を通り、直線 VB に直交する直線を引く。これは MR line であるから、交点 $\left(\cos\frac{x}{3}, 0\right)$ は MR point となる。よって $\cos\frac{x}{3}$ は MR 数である。

x が鋭角でないとする。$\frac{\pi}{2} \leq x < \pi$ と仮定する。このとき、$x = x' + \frac{\pi}{2}$ としよう。ただし $0 \leq x' < \frac{\pi}{2}$ である。したがって、$\cos x = \cos\left(x' + \frac{\pi}{2}\right) = -\sin x'$ である。よって、$-\sin x'$ は MR 数であり、MR 数は euclidean より、$\sin x'$, $\cos x' = \sqrt{1 - \sin^2 x'}$ も MR 数である。さらに x' は鋭角だから、$\cos\frac{x'}{3}$、$\sin\frac{x'}{3} = \sqrt{1 - \cos^2\frac{x'}{3}}$ も MR 数となる。

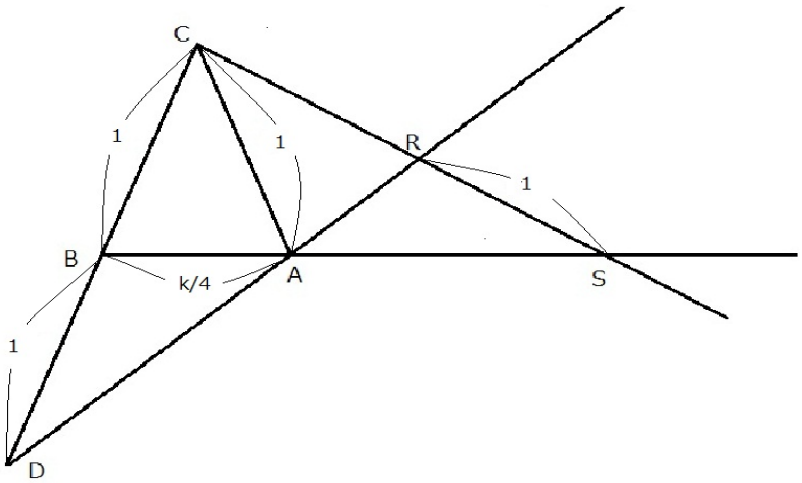
$$\cos\frac{x}{3} = \cos\left(\frac{x'}{3} + \frac{\pi}{6}\right) = \cos\frac{x'}{3}\cos\frac{\pi}{6} - \sin\frac{x'}{3}\sin\frac{\pi}{6} = \frac{\sqrt{3}}{2}\cos\frac{x'}{3} - \frac{1}{2}\sin\frac{x'}{3}$$

より、$\cos\frac{x}{3}$ は MR 数となる。

$\pi \leq x < \frac{3\pi}{2}$、$\frac{3\pi}{2} \leq x < 2\pi$ のときも、同様に鋭角に帰着して考えることで、$\cos\frac{x}{3}$ は MR 数となることがわかる。 **証明終**

$\cos x$ が MR 数なら、$\sin x$ も MR 数であることは、(上の証明中にも出てきたが) 容易にわかる。また、同様にして $\sin x$ が MR 数なら、$\sin\frac{x}{3}$ も MR 数である。

定理 3.8 実数 k を $0 < k < 8$ とする。$\triangle ACB$ は $AC = BC = 1$、$AB = \frac{k}{4}$ の二等辺三角形とする。点 D を直線 CB 上の点で、B が線分 CD の中点となるようにとる。点 S は半直線 BA 上の点で $S \neq A$ かつ $S \neq B$、点 R は直線 DA と直線 CS の交点であり、$RS = 1$ とする。このとき、$AS = \sqrt[3]{k}$ となる。



証明　C を通る線分 AB の平行線を引き、直線 DA との交点を E とする。すると、$\triangle ABD \sim \triangle ECD$ である。ただし、$\sim$ は、三角形の相似を表すものとする。このとき、B は線分 DC の中点だから $DB : DC = 1 : 2$ であり、$AB : EC = 1 : 2$ となるので、$EC = 2AB = \dfrac{k}{2}$ となる。また、$\triangle ECR \sim \triangle ASR$ であるから、$CR : SR = EC : AS$ より、$(k/2)/CR = AS/1$ を得る。$AS = x$ とおけば、$CR = \dfrac{k}{2x}$ となる。M を線分 AB の中点とする。ピタゴラスの定理より、

$$\left[1+\frac{k}{2x}\right]^2 = CS^2 = CM^2+MS^2 = [CB^2-BM^2]+MS^2 = \left[1^2-\left(\frac{k}{8}\right)^2\right]+\left[x+\frac{k}{8}\right]^2$$

両端の式を x についてまとめると、$4x^4+kx^3-4kx-k^2=0$ となる。因数分解をすると $(4x+k)(x^3-k)=0$ を得るが、$4x+k>0$ より、$x^3-k=0$ となる。したがって、x は k の実三乗根となる。　**証明終**

系 3.9 x は MR 数とする。このとき、$\sqrt[3]{x}$ も MR 数となる。

証明　x は MR 数とする。$0<|x|<8$ のとき、上の図において、点 A を $(0,0)$、点 B を $(-\dfrac{|x|}{4},0)$ とすれば、各点は MR point、各直線を MR line としてとれる。定理 3.8 より、点 S は $\left(\sqrt[3]{|x|},0\right)$ であるから、$\sqrt[3]{x}$ は MR 数である。

$8 \leq |x|$ のとき、$\dfrac{1}{|x|}$ は MR 数であり、$0<\dfrac{1}{|x|}<8$ となる。点 A を $(0,0)$, 点 B を $\left(-\dfrac{1}{4|x|},0\right)$ とすれば、各点は MR point、各直線は MR line としてとれる。定理 3.8 より、点 S は $\left(\sqrt[3]{\dfrac{1}{|x|}},0\right)$ であるから、$\sqrt[3]{\dfrac{1}{|x|}}$ は MR 数となる。MR 数は体をなすので、$\sqrt[3]{x}$ も MR 数である。　**証明終**

これにより MR 数の集合は euclidean であることに加え、さらに角の三等分、三乗根で閉じていることがわかった。このような体を vietean という。

次に、$\mathbb{V}, \mathbb{V}'$ をそれぞれ次のように定義する。

$$\mathbb{V} \stackrel{\text{def}}{=} \left\{ x \in \mathbb{R} \;\middle|\; \begin{array}{l} \text{ある自然数 } n \text{ とある 4 次以下の体の拡大の列} \\ \mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_n (\subset \mathbb{R}) \text{ が存在し、} x \in F_n \end{array} \right\}$$

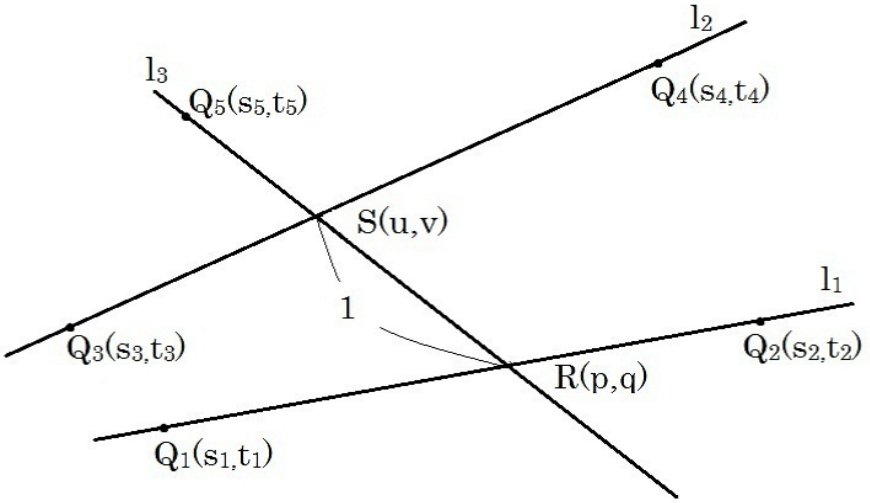
$$\mathbb{V}' \stackrel{\text{def}}{=} \left\{ x \in \mathbb{C} \;\middle|\; \begin{array}{l} \text{ある自然数 } n \text{ とある 4 次以下の体の拡大の列} \\ \mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_n (\subset \mathbb{C}) \text{ が存在し、} x \in F_n \end{array} \right\}$$

定義より、明らかに $\mathbb{V} \subset \mathbb{V}' \cap \mathbb{R}$ が成立する。次の定理により、直ちに、$\mathbb{V} = \mathbb{V}' \cap \mathbb{R}$ が成立することがわかる。

定理 3.10 次が成り立つ。
(1) $x \in \mathbb{R}$ とする。x が MR 数であることと $x \in \mathbb{V}$ であることは同値である。
(2) $x \in \mathbb{C}$ とする。x が MR 複素数であることと $x \in \mathbb{V}'$ であることは同値である。

証明 (1) x を MR 数とすると、$P_n(x, 0)$ は MR point である。このとき、点 P_n を末項とし、各点が定義 3.1 の (1) または (2) をみたしている点列 $P_1, \ldots, P_n$ が存在する。$0 \leq i \leq n$ について、P_i の座標成分がそれぞれ $\mathbb{V}$ の元になることを i の帰納法で示す。$P_1(0,0), P_2(1,0), P_3(0,1)$ は自明である。i まで成り立つとし、$i+1$ のときを考える。$P_{i+1} = R(p,q)$ とする。R が (1) を充たす点だとすれば、RC 数のときと同様に成り立つ。

R が (2) を充たす点だとする。点列 $P_1, \ldots, P_i$ の中の点 $Q_1(s_1, t_1)$、$Q_2(s_2, t_2)$ を通る直線を l_1 とし、点列 $P_1, \ldots, P_i$ の中の点 $Q_3(s_3, t_3)$、$Q_4(s_4, t_4)$ を通る直線を l_2 とする。R は l_1 上の点とする。点列 $P_1, \ldots, P_i$ の中の点 $Q_5(s_5, t_5)$ をとる。S は直線 l_2 上の点で、Q_5, R, S は同一直線上にあり、$RS = 1$ とする。このとき、p, q は $s_1, \ldots, s_5, t_1, \ldots, t_5$ の四則演算からなる値を係数とする 4 次多項式の根となることを示す。



直線 l_1 の方程式は $y - t_1 = \left(\dfrac{t_2 - t_1}{s_2 - s_1}\right)(x - s_1)$ である。$a = \dfrac{t_2 - t_1}{s_2 - s_1}$、$b = -as_1 + t_1$ とおくと、l_1 は

$$y = ax + b$$

となる。同様に l_2 の直線の方程式は、$c = \dfrac{t_4 - t_3}{s_4 - s_3}$、$d = -cs_3 + t_3$ とおくと、

$$y = cx + d$$

となる。また、直線 l_3 は R, Q_5 を通るから、直線 l_3 の方程式は

$$y - q = \left(\frac{t_5 - q}{s_5 - p}\right)(x - p)$$

である。点 S は l_2 と l_3 の交点であるから、それぞれの式より、

$$u = \frac{p(t_5 - q) - (q - d)(s_5 - p)}{(t_5 - q) - c(s_5 - p)}, \qquad v = \frac{(d + cp)(t_5 - q) - cq(s_5 - p)}{(t_5 - q) - c(s_5 - p)}$$

となる。一方、$RS = 1$ より、$(u - p)^2 + (v - q)^2 = 1$ が成り立つ。これに上の式を代入して、

$$\left(\frac{p(t_5 - q) - (q - d)(s_5 - p)}{(t_5 - q) - c(s_5 - p)} - p\right)^2 + \left(\frac{(d + cp)(t_5 - q) - cq(s_5 - p)}{(t_5 - q) - c(s_5 - p)} - q\right)^2 = 1$$

が成立する。R は l_1 上の点だから、$q = ap + b$ である。これを代入して、p について整理すると、

$$\begin{aligned} & \alpha^2(a^2+1)p^4 + 2\{\alpha^2(a\gamma - s_5) + \alpha\gamma(a^2+1)\}p^3 \\ + \; & \{\alpha^2(\gamma^2 + {s_5}^2 - 1) + 4\alpha\beta(a\gamma - s_5) + \beta^2(a^2-1)\}p^2 \\ + \; & 2\{\alpha(\gamma - s_5 c) + \alpha\beta(\gamma^2 + {s_5}^2) + \beta^2(a\gamma + s_5)\}p + \{\beta^2(\gamma^2 - {s_5}^2) - (\gamma + cs_5)^2\} \\ = \; & 0 \end{aligned}$$

を得る。ただし、$\alpha = a - c$, $\beta = b - d$, $\gamma = b - t_5$ とする。この式より、p は 4 次多項式の根としてとれることがわかる。よって、$p \in \mathbb{V}$ となる。また、$q = ap + b \in \mathbb{V}$ もわかる。

(1) の逆を示す前に (2) を示そう。

(2) $x + yi$ を MR 複素数とする。定理 3.5 により x, y は MR 数より、$x, y \in \mathbb{V} \subset \mathbb{V}'$ である。また、$i \in \mathbb{V}'$ より、$x + iy \in \mathbb{V}'$ となる。

次に、$\mathbb{V}'$ の各元は MR 複素数であることを示す。

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_n (\subset \mathbb{C})$$

を 4 次以下の体の拡大の列とする。各 i について、F_i のすべての元は MR 複素数であることを i についての帰納法で示す。$i = 0$ のときは、$F_0 = \mathbb{Q}$ より自明である。i まで成り立つとして、$i + 1$ のときを考える。

$[F_{i+1} : F_i] = 2$ なら RC 複素数のときと同様にして成り立つ。

$[F_{i+1} : F_i] = 3$ のとき。$\alpha \in F_{i+1} \setminus F_i$ とし、$F_i \subset F_i(\alpha) \subseteq F_{i+1}$ とする。このとき

$$[F_{i+1} : F_i] = [F_{i+1} : F_i(\alpha)][F_i(\alpha) : F_i] = 3$$

であるから、$[F_i(\alpha):F_i]=1$ または 3 であるが、$F_i \subsetneq F_i(\alpha)$ より $[F_i(\alpha):F_i]=3$ である。よって、

$$F_{i+1}=F_i(\alpha)$$

である。α が MR 複素数となることを示す。α の F_i 上最小多項式を $f(x)=x^3+ax^2+bx+c$ とする。$x-a/3$ を代入し、$g(x)=f(x-a/3)=x^3+Ax+B$ とする。ただし A、B は a, b, c で表わせるから $A,B\in F_i$ であり、$g(x)$ は F_i 上の多項式となる。$\beta=\alpha+a/3$ とおくと $g(\beta)=0$ となるから、β は $g(x)$ の根となる。$F_i(\alpha)=F_i(\beta)$ より、始めから $g(x)$ について考えればよいことがわかった。

カルダノの方法より $g(x)=0$ の 3 つの解は

$$y+z,\quad \omega y+\omega^2 z,\quad \omega^2 y+\omega z$$

と書ける。ただし、

$$y^3=\frac{1}{2}(-B+\sqrt{B^2+4A^3/27}),\quad z^3=\frac{1}{2}(-B-\sqrt{B^2+4A^3/27}),\quad \omega=e^{\frac{2\pi i}{3}}$$

となる。帰納法の仮定より F_i の元は MR 複素数であり、y^3、z^3 は F_i の元とルートで表わされているので MR 複素数である。ここで、y, z, ω が MR 複素数となることを示す。y^3 は MR 複素数であるから、p, q を MR 数として、$y^3=p+qi$ とおくことができ、さらに、オイラーの公式によって、

$$p+qi=re^{i\theta}=r(\cos\theta+i\sin\theta)$$

とできる。ここで

$$r=\sqrt{p^2+q^2},\ \cos\theta=\frac{p}{\sqrt{p^2+q^2}},\ \sin\theta=\frac{q}{\sqrt{p^2+q^2}}$$

であり、r, $\cos\theta$, $\sin\theta$ はそれぞれ MR 数である。ここで、

$$y=\sqrt[3]{p+qi}=\sqrt[3]{r}e^{(\frac{\theta}{3}+\frac{2l\pi}{3})i}=\sqrt[3]{r}\left(\cos\left(\frac{\theta}{3}+\frac{2l\pi}{3}\right)+i\sin\left(\frac{\theta}{3}+\frac{2l\pi}{3}\right)\right)$$

に注意する。ただし、l は整数とする。系 3.7 と系 3.9 により $\sqrt[3]{r}$, $\cos\left(\frac{\theta}{3}+\frac{2l\pi}{3}\right)$, $\sin\left(\frac{\theta}{3}+\frac{2l\pi}{3}\right)$ は MR 数である。よって、

$$y=\sqrt[3]{r}\left(\cos\left(\frac{\theta}{3}+\frac{2l\pi}{3}\right)+i\sin\left(\frac{\theta}{3}+\frac{2l\pi}{3}\right)\right)$$

は MR 複素数となる。同様に、z も MR 複素数である。また、

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

より、ω は MR 複素数となる。よって、$g(x)$ の根 β は MR 複素数となる。したがって、F_{i+1} は MR 複素数の集合となる。

$[F_{i+1}:F_i]=4$ のとき、3 のときと同様に $\alpha \in F_{i+1} \setminus F_i$ とすると、$F_i \subset F_i(\alpha) \subseteq F_{i+1}$ である。よって、$[F_{i+1}:F_i]=[F_{i+1}:F_i(\alpha)][F_i(\alpha):F_i]=4$ が成り立つ。このとき、$[F_i(\alpha):F_i]=2$ もしくは 4 となる。$[F_i(\alpha):F_i]=2$ のときは、$[F_{i+1}:F_i(\alpha)]=2$ であるから、F_{i+1}/F_i は二次拡大を 2 回繰り返したものである。この場合は、MR 複素数は RC 複素数と同様に、平方根で閉じているので、証明できたことになる。$[F_i(\alpha):F_i]=4$ のとき、すなわち $F_{i+1}=F_i(\alpha)$ のとき、α の F_i 上最小多項式は 4 次である。4 次方程式の解はフェラーリの方法により、3 次方程式の解に帰着できる。よって、拡大次数が 3 のときと同様に α が MR 複素数であることがわかり、F_{i+1} は MR 複素数から成る集合となる。以上より、4 次以下の体の拡大の列は MR 複素数からなることがわかった。

(1) の逆を示す。$x \in \mathbb{V}$ とする。$\mathbb{V} \subset \mathbb{V}' \cap \mathbb{R}$ より、x は MR 複素数ある。よって、ある二つの MR 数 p, q によって $x=p+qi$ と表わせる。しかし x は実数でもあるから $x=p$ である。よって、x は MR 数となる。 **証明終**

MR 複素数かつ実数ならば、MR 数であることから、次の系は明らかである。

系 3.11 $\mathbb{V}=\mathbb{V}' \cap \mathbb{R}$ である。

4 応用

これまでの議論から、RC 複素数は 2 次以下の方程式を繰り返し解く操作の中で得られた数全体であり、MR 複素数は 4 次以下の方程式を繰り返し解く操作の中で得られた数全体であるということが分かった。この章では、これまでの内容の応用として、ギリシャの三大作図問題と正多角形の作図に関して考察することにする。

円積問題

与えられた円と同じ面積の正方形を定木とコンパス、つまり RC で作図できるかという問題である。ここでは、MR でも作図可能であるかを考える。与えられた円の半径の長さを r とし、作図したい正方形の一辺の長さを x とすると、$x^2=\pi r^2$ が成り立ち、これを x について解けば $x=r\sqrt{\pi}$ である。従って作図できるためには、単位円の面積 π に対する $\sqrt{\pi}$ の作図が必要である。作図可能な数である RC 複素数や MR 複素数は代数的数であるが、1882 年ドイツの数学者リンデマンが π が超越数であることを証明したことで、円積問題が RC と MR での作図において否定的に解決されることとなった。

ここでは π が超越数であるというリンデマンの定理を証明する。ところで、与えられた正方形と同じ面積の円を作図できるかどうかという可能性については、円積問題の可能性と同値であるので、これも不可能である。

リンデマンの定理の準備として、次の命題が必要である。

命題 4.1 ある代数的整数が有理数であるとき、それは有理整数である。つまり、$\mathbb{Z}_{\overline{\mathbb{Q}}} \cap \mathbb{Q} = \mathbb{Z}$ である。ただし、$\mathbb{Z}_{\overline{\mathbb{Q}}}$ は $\mathbb{Z}$ の $\overline{\mathbb{Q}}$ ($\mathbb{Q}$ の代数閉包) の中での整閉包とする。

証明　$\dfrac{r}{q} \in \mathbb{Q}$ ($r, q \in \mathbb{Z}$ は互いに素であるとする) をとって、$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ の解であるとする。

つまり、

$$\left(\frac{r}{q}\right)^n + a_{n-1}\left(\frac{r}{q}\right)^{n-1} + a_{n-2}\left(\frac{r}{q}\right)^{n-2} + \cdots + a_2\left(\frac{r}{q}\right)^2 + a_1\left(\frac{r}{q}\right) + a_0 = 0$$

である。よって、

$$r^n + a_{n-1}qr^{n-1} + a_{n-2}q^2r^{n-2} + \cdots + a_2q^{n-2}r^2 + a_1q^{n-1}r + a_0q^n = 0$$

であり、

$$r^n = -(a_{n-1}qr^{n-1} + a_{n-2}q^2r^{n-2} + \cdots + a_2q^{n-2}r^2 + a_1q^{n-1}r + a_0q^n)$$

がわかる。従って、$q \mid r^n$ となる。

もし $q \neq \pm 1$ であれば、$p \mid q$ をみたす素数 p が存在する。よって、$p \mid r^n$ である。従って、$p \mid r$ となるが、これは r と q が互いに素であることに矛盾するので、$q = \pm 1$ である。以上から、$\dfrac{r}{q} \in \mathbb{Z}$ を得る。　**証明終**

補題 4.2 $K/\mathbb{Q}$ は有限次ガロア拡大であり、$\beta_1, \beta_2, \ldots, \beta_n \in K$ は重複を許すことにする。ここで、$\forall \sigma \in Gal(K/\mathbb{Q})$ に対して、multi-set として $\{\beta_1, \ldots, \beta_n\} = \{\sigma(\beta_1), \ldots, \sigma(\beta_n)\}$ であると仮定する。

このとき、$f(x_1, x_2, \ldots, x_n)$ が $\mathbb{Q}$ 係数の $x_1, \ldots, x_n$ の対称式であり、$f(\beta_1, \ldots, \beta_n)$ が代数的整数ならば、$f(\beta_1, \ldots, \beta_n) \in \mathbb{Z}$ である。

証明　いま $\sigma(f(\beta_1, \ldots, \beta_n)) = f(\sigma(\beta_1), \ldots, \sigma(\beta_n))$ であるが、他方で f が対称式であることと β_i の性質から $f(\sigma(\beta_1), \ldots, \sigma(\beta_n)) = f(\beta_1, \ldots, \beta_n)$ が成り立つ。従って $\sigma(f(\beta_1, \ldots, \beta_n)) = f(\beta_1, \ldots, \beta_n)$ である。つまり $f(\beta_1, \ldots, \beta_n) \in \mathbb{Q}$ である。命題 4.1 により $f(\beta_1, \ldots, \beta_n) \in \mathbb{Z}$ である。　**証明終**

定理 4.3 (リンデマン, 1882) 円周率 π は超越数である。(つまり、π は $\mathbb{Q}$ 上代数的でない。)

証明　背理法で証明する。π は $\mathbb{Q}$ 上代数的であると仮定する。すると $i\pi$ も $\mathbb{Q}$ 上代数的である (ただし $i = \sqrt{-1}$)。$\theta = i\pi$ とおき、θ の $\mathbb{Q}$ 上の共役全体を

$$\theta = \theta_1, \theta_2, \ldots, \theta_n$$

とする。また自然数 l を

$$l\theta_1, l\theta_2, \ldots, l\theta_n$$

が代数的整数となるようにとっておく。

$$\{\delta_1\theta_1 + \delta_2\theta_2 + \cdots + \delta_n\theta_n \mid \delta_i = 0, 1\}$$

を multi-set と考え、2^n 個の元の中で 0 でないものがちょうど k 個あったとする。それらを $\alpha_1, \alpha_2, \ldots, \alpha_k$ とする。また $\alpha_{k+1} = \alpha_{k+2} = \cdots = \alpha_{2^n} = 0$ とおく。このとき、multi-set として

$$\{\delta_1\theta_1 + \delta_2\theta_2 + \cdots + \delta_n\theta_n \mid \delta_i = 0, 1\} = \{\alpha_j | 1 \leq j \leq 2^n\} \tag{6}$$

であることに注意する。

ここで、π, l, k によって定まる定数 c を、

$$c = 2^{2k} l^k e \times (\max\{|\alpha_i| \mid i = 1, \ldots, k\})^{k+1}$$

と定める。ここで、次の主張を示したい。

主張 4.4 十分大きな素数 p に対して、

$$(p-1)! \leq |J_p| \leq c^p$$

を満たす数 J_p が存在する[10]。

c は定数であるので、十分大きな自然数 r に対して、

$$(r-1)! > c^r$$

を満たすことは、簡単に証明できる[11]。つまり、十分大きな素数 p に対しては、主張 4.4 を満たす J_p は存在しないことになり、背理法による証明が完了する。

以下、主張 4.4 を証明しよう。

オイラーの等式 $e^{i\pi} + 1 = 0$ より次の等式を満たす。

$$(1 + e^{\theta_1})(1 + e^{\theta_2}) \cdots (1 + e^{\theta_n}) = 0$$

従って、

$$\sum_{\substack{\delta_i = 0,1 \\ i = 1,2,\ldots,n}} e^{\delta_1\theta_1 + \delta_2\theta_2 + \cdots + \delta_n\theta_n} = 0$$

[10] J_p は、(9) で定義される。主張 4.4 の右の不等式は、複素積分の評価によって証明される。それに対して、左の不等式は、代数的に証明できる。左の不等式を証明するためには、(i) J_p は整数、(ii) $(p-1)! \mid J_p$、(iii) $p \nmid J_p$ を証明するのである。

[11] 例えば、$\lim_{r\to\infty} \frac{c^r}{(r-1)!} = 0$ から証明できる。

となる。このとき、(6) より、

$$(2^n - k) + e^{\alpha_1} + e^{\alpha_2} + \cdots + e^{\alpha_k} = 0 \tag{7}$$

を満たす。ここで素数 p を

$$p > \max\left\{\left|l\alpha_1 l\alpha_2 \cdots l\alpha_k\right|, 2^n - k, |\alpha_1|, |\alpha_2|, \ldots, |\alpha_k|\right\} \tag{8}$$

となるようにとる。

ここで、

$$f_p(x) := l^{kp} x^{p-1}(x-\alpha_1)^p(x-\alpha_2)^p \cdots (x-\alpha_k)^p$$

$$I_p(z) := e^z \int_0^z e^{-x} f_p(x)dx \qquad (z \in \mathbb{C})$$

とおく。また $m := deg(f_p) = kp + p - 1$ とおく。部分積分を繰り返すと、

$$\begin{aligned}
I_p(z) &= e^z\left[-e^{-x}f_p(x)\right]_0^z - \left(-e^z\int_0^z e^{-x}f_p'(x)dx\right) \\
&= e^z\left[-e^{-x}f_p(x)\right]_0^z + e^z\left[-e^{-x}f_p'(x)\right]_0^z + e^z\int_0^z e^{-x}f_p''(x)dx \\
&= e^z\sum_{i=0}^{m}\left[-e^{-x}f_p^{(i)}(x)\right]_0^z \\
&= e^z\sum_{i=0}^{m}\left(f_p^{(i)}(0) - e^{-z}f_p^{(i)}(z)\right) \\
&= e^z\sum_{i=0}^{m}f_p^{(i)}(0) - \sum_{i=0}^{m}f_p^{(i)}(z)
\end{aligned}$$

となる。ここで $f_p^{(m+1)}(z) = 0$ に注意する。このとき、J_p を次のように定義する。

$$\begin{aligned}
J_p &:= -(I_p(\alpha_1) + I_p(\alpha_2) + \cdots + I_p(\alpha_k)) \\
&= -(e^{\alpha_1} + e^{\alpha_2} + \cdots + e^{\alpha_k})\sum_{i=0}^{m}f_p^{(i)}(0) \\
&\quad + \sum_{i=0}^{m}f_p^{(i)}(\alpha_1) + \sum_{i=0}^{m}f_p^{(i)}(\alpha_2) + \cdots + \sum_{i=0}^{m}f_p^{(i)}(\alpha_k) \\
&= (2^n - k)\sum_{i=0}^{m}f_p^{(i)}(0) + \sum_{i=0}^{m}\left(\sum_{j=1}^{k}f_p^{(i)}(\alpha_j)\right)
\end{aligned} \tag{9}$$

上の式変形で (7) を用いた。

まず、主張 4.4 の左の不等式を証明する。そのためには、

主張 4.5 J_p は 0 でない有理整数であり、$(p-1)!$ で割り切れる。

を証明すれば十分である。これを示そう。

まず、

$$\forall i \geq 0 \text{ に対して、} f_p^{(i)}(0) \text{ と } f_p^{(i)}(\alpha_1) + f_p^{(i)}(\alpha_2) + \cdots + f_p^{(i)}(\alpha_k) \text{ は有理整数}$$

であることを示す。なぜなら、$f_p(x) = x^{p-1}(lx - l\alpha_1)^p(lx - l\alpha_2)^p \cdots (lx - l\alpha_k)^p$ の各係数は $\mathbb{Z}$ 係数で $l\alpha_1, \ldots, l\alpha_k$ の対称式であり、$\forall \sigma \in Gal(\mathbb{Q}(\theta_1, \ldots, \theta_n)/\mathbb{Q})$ に対して、multi-set として $\{l\alpha_1, \ldots, l\alpha_k\} = \{\sigma(l\alpha_1), \ldots, \sigma(l\alpha_k)\}$ であるので、従って補題 4.2 により

$$f_p(x) \text{ の各係数は有理整数}$$

であることが分かる。よって、任意の $i \geq 0$ に対して $f_p^{(i)}(0) \in \mathbb{Z}$ である。

また任意の $i \geq 0$ と任意の $1 \leq j \leq k$ に対して $f_p^{(i)}(\alpha_j)$ は代数的整数である。実際、$f_p(x)$ の i 階微分は

$$f_p^{(i)}(x) = \sum_{s_0+s_1+\cdots+s_k=m-i} c_{s_0 s_1 \cdots s_k} \cdot l^{kp} x^{s_0}(x-\alpha_1)^{s_1} \cdots (x-\alpha_k)^{s_k} \quad (c_{s_0 s_1 \cdots s_k} \in \mathbb{Z})$$

と書けるが、ここで、

$$g_{s_0 s_1 \cdots s_k}(x) := l^{kp} x^{s_0}(x-\alpha_1)^{s_1} \cdots (x-\alpha_k)^{s_k}$$

とおく。$t = 1, 2, \ldots, k$ に対し $s_t \neq 0$ ならば、任意の j に対して $g_{s_0 s_1 \cdots s_k}(\alpha_j) = 0$ である。もし $s_t = 0$ となる t が存在すれば、

$$\begin{aligned} g_{s_0 s_1 \cdots s_k}(x) &= l^{kp} x^{s_0}(x-\alpha_1)^{s_1} \cdots (x-\alpha_{t-1})^{s_{t-1}}(x-\alpha_{t+1})^{s_{t+1}} \cdots (x-\alpha_k)^{s_k} \\ &= l^{p-s_0}(lx)^{s_0} \cdot \prod_{j \neq t} l^{p-s_j}(lx - l\alpha_j)^{s_j} \end{aligned}$$

であるので $g_{s_0 s_1 \cdots s_k}(\alpha_t)$ は代数的整数である。従って、任意の $s_0, \ldots, s_k$ に対して $g_{s_0 s_1 \cdots s_k}(\alpha_t)$ が代数的整数なので、$f_p^{(i)}(\alpha_t)$ も代数的整数である。$\sum_{j=1}^{k} f_p^{(i)}(\alpha_j)$ は $\mathbb{Q}$ 係数の $\alpha_1, \ldots, \alpha_k$ の対称式であり、かつ代数的整数なので、補題 4.2 により

$$\sum_{j=1}^{k} f_p^{(i)}(\alpha_j) \in \mathbb{Z}$$

である。以上から、

$$J_p \in \mathbb{Z}$$

であることがわかった。

次に $J_p \neq 0$ かつ $(p-1)! \mid J_p$ を示す。

$$f_p^{(i)}(0) = 0 \qquad (i < p-1) \tag{10}$$

$$f_p^{(i)}(\alpha_j) = 0 \quad (i < p,\ 1 \leq j \leq k) \tag{11}$$

は明らかである。$f_p^{(i)}(x)$ のすべての係数は $i!$ で割れるから

$$i \geq p \text{ なら } p! \mid f_p^{(i)}(0), \tag{12}$$

$$(p-1)! \mid f_p^{(p-1)}(0) \tag{13}$$

である。

次に

$$i \geq p \text{ であるとき } p! \mid \sum_{j=1}^{k} f_p^{(i)}(\alpha_j) \tag{14}$$

を示す。まず、

$$q(y) = (y - l\alpha_1)^p \cdots (y - l\alpha_k)^p$$

とおく。$q(y)$ の各係数は $\mathbb{Z}$ 係数の $l\alpha_1, \ldots, l\alpha_k$ の対称式であり、$\forall \sigma \in Gal(\mathbb{Q}(\theta_1, \ldots, \theta_n)/\mathbb{Q})$ に対して、multi-set として $\{l\alpha_1, \ldots, l\alpha_k\} = \{\sigma(l\alpha_1), \ldots, \sigma(l\alpha_k)\}$ であるので、従って補題 4.2 により、$q(y) \in \mathbb{Z}[y]$ である。よって、

$$q(y) = \sum_{s=0}^{kp} a_s y^s \quad (a_s \in \mathbb{Z})$$

と書けるので、

$$q(lx) = \sum_{s=0}^{kp} a_s l^s x^s \quad (a_s \in \mathbb{Z})$$

となる。よって、

$$f_p(x) = x^{p-1} q(lx) = \sum_{s=0}^{pk} a_s l^s x^{s+p-1}$$

である。i 階微分は、

$$f_p^{(i)}(x) = \sum_{s=0}^{kp} (s+p-1)(s+p-2)\cdots(s+p-i) \cdot a_s l^s x^{s+p-1-i}$$

であるので、任意の α_j に対して、

$$f_p^{(i)}(\alpha_j) = \sum_{s=0}^{kp} (s+p-1)(s+p-2)\cdots(s+p-i) \cdot a_s l^{i+1-p} (l\alpha_j)^{s+p-1-i}$$

である。いま、

$$\sum_{j=1}^{k} f_p^{(i)}(\alpha_j) = \sum_{s=0}^{kp} (s+p-1)(s+p-2)\cdots(s+p-i) \cdot a_s l^{i+1-p} \left(\sum_{j=0}^{k} (l\alpha_j)^{s+p-1-i} \right)$$

であるが、$l\alpha_j \in \mathbb{Z}_{\overline{\mathbb{Q}}}$ なので、補題 4.2 により $a_s l^{i+1-p}\left(\sum_{j=0}^{k}(l\alpha_j)^{s+p-1-i}\right) \in \mathbb{Z}$ である。$(s+p-1)(s+p-2)\cdots(s+p-i)$ は i 個の連続する自然数の積なので、$i!$ で割れる。従って、(14) が示された。

今、

$$f_p^{(p-1)}(x) = (p-1)!l^{kp}(x-\alpha_1)^p(x-\alpha_2)^p\cdots(x-\alpha_k)^p + xg(x)$$

を満たす $g(x) \in \overline{\mathbb{Q}}[x]$ がある。よって、

$$f_p^{(p-1)}(0) = (-1)^{kp}(p-1)!(l\alpha_1 l\alpha_2\cdots l\alpha_k)^p$$

である。ここで、補題 4.2 により、$l\alpha_1 l\alpha_2\cdots l\alpha_k \in \mathbb{Z}$ に注意する。p は (8) を満たすので $|\, l\alpha_1 l\alpha_2\cdots l\alpha_k \,| < p$ であり、かつ p が $(p-1)!$ を割らないので

$$p \text{ は } f_p^{(p-1)}(0) \text{ を割らない。} \tag{15}$$

p は $2^n - k < p$ ととっていたので

$$p \nmid 2^n - k \tag{16}$$

である。(10), (11), (12), (13), (14), (15), (16) によって、

$$J_p = (2^n-k)\sum_{i=0}^{m} f_p^{(i)}(0) + \sum_{i=0}^{m}\left(\sum_{j=1}^{k} f_p^{(i)}(\alpha_j)\right)$$

は $(p-1)!$ で割れるが $p!$ では割れない。これで主張 4.5 が示された。

次に、主張 4.4 の右の不等式を証明する。

$|\alpha_M| := \max_{1\leq j\leq k}\{|\alpha_j|\}$ とおくと、

$$
\begin{aligned}
& |I(\alpha_M)| \\
= & \left| e^{\alpha_M} \int_0^{\alpha_M} e^{-x} f_p(x) dx \right| \\
= & \left| e^{\alpha_M} \int_0^{1} e^{-\alpha_M x} f_p(\alpha_M x) \cdot \alpha_M dx \right| \\
= & \left| e^{\alpha_M} \int_0^{1} e^{-\alpha_M x} \cdot l^{kp} \cdot (\alpha_M x)^{p-1} (\alpha_M x - \alpha_1)^p (\alpha_M x - \alpha_2)^p \cdots (\alpha_M x - \alpha_k)^p \cdot \alpha_M dx \right| \\
\leq & |e^{\alpha_M}| \cdot l^{kp} \cdot |\alpha_M|^p \int_0^1 |e^{-\alpha_M x}| x^{p-1} (|\alpha_M| x + |\alpha_1|)^p (|\alpha_M| x + |\alpha_2|)^p \cdots (|\alpha_M| x + |\alpha_k|)^p dx \\
= & e^{Re(\alpha_M)} \cdot l^{kp} \cdot |\alpha_M|^p \int_0^1 e^{-Re(\alpha_M) x} x^{p-1} (|\alpha_M| x + |\alpha_1|)^p (|\alpha_M| x + |\alpha_2|)^p \cdots (|\alpha_M| x + |\alpha_k|)^p dx \\
\leq & e^{Re(\alpha_M)} \cdot l^{kp} \cdot |\alpha_M|^p \cdot \max\{e^{-Re(\alpha_M)}, 1\} \cdot (|\alpha_M| + |\alpha_1|)^p (|\alpha_M| + |\alpha_2|)^p \cdots (|\alpha_M| + |\alpha_k|)^p \\
\leq & e^p \cdot l^{kp} \cdot |\alpha_M|^p (|\alpha_M| + |\alpha_1|)^p (|\alpha_M| + |\alpha_2|)^p \cdots (|\alpha_M| + |\alpha_k|)^p \\
\leq & e^p \cdot l^{kp} \cdot |\alpha_M|^p \cdot |2\alpha_M|^{kp}
\end{aligned}
$$

が成り立つ。上の式変形で、$p > Re(\alpha_M)$ を使っている。これは、p の選び方 (8) から満たされることに注意する。従って、

$$
\begin{aligned}
|J_p| & \leq k \cdot e^p \cdot l^{kp} \cdot |\alpha_M|^{kp+p} \cdot 2^{kp} \\
& \leq 2^{kp} \cdot e^p \cdot l^{kp} \cdot |\alpha_M|^{kp+p} \cdot 2^{kp} = c^p
\end{aligned}
$$

となり、主張 4.4 の証明が完了した。 **証明終**

$\pi \notin \overline{\mathbb{Q}}$ であるので $\sqrt{\pi} \notin \overline{\mathbb{Q}}$ である。(仮に $\sqrt{\pi} \in \overline{\mathbb{Q}}$ ならば、$\pi = \sqrt{\pi}^2 \in \overline{\mathbb{Q}}$ であるので矛盾する。) $\mathbb{E}' \subset \mathbb{V}' \subset \overline{\mathbb{Q}}$ により $\sqrt{\pi} \notin \mathbb{E}', \mathbb{V}'$ である。従って、RC でも MR でも円積問題は否定的に解決された。

次に残りの三大作図問題の 2 つである立方体倍積問題と角の三等分問題について考察する。立方体倍積問題とは、与えられた立方体の 2 倍の体積を持つ立方体を作りなさい、という問題であり a と x をそれぞれ与えられた立方体の一辺の長さ、2 倍の体積を持つ立方体の一辺の長さ、とすると $x^3 = 2a^3$ が成り立つ。これを x について解くと $x = a\sqrt[3]{2}$ を得る。従って、立方体倍積問題は 1 から $\sqrt[3]{2}$ を作図しなさいという問題と同値である。角の三等分問題は、与えられた任意の角度に対してその $\frac{1}{3}$ 倍の角度が作図可能かどうかという問題である。これらの作図可

能性は体拡大の性質を適用して解決される。

立方体倍積問題

$\sqrt[3]{2}$ の $\mathbb{Q}$ 上最小多項式は、

$$f_{\mathbb{Q},\sqrt[3]{2}}(x) = x^3 - 2$$

であるから $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ となる。

従って、RC では作図不可能である。他方、MR では作図可能ということになる。補足として、直線と円以外に 2 次曲線の使用を許せば、放物線 $y = x^2$ と双曲線 $xy = 2$ の交点を作図することで $\sqrt[3]{2}$ が得られる。

角の三等分問題

MR を使えば、与えられた角の三等分線が作図できることは既に示した。$\cos\dfrac{\pi}{3} = \dfrac{1}{2}$ は RC でも作図可能である。ところで $\cos\pi = -1$ は作図可能な数であるから角度 π の三等分線は RC で作図可能である。

そこで $\dfrac{\pi}{3}$ の三等分線が作図可能かどうかを考える。つまり、$\cos\dfrac{\pi}{3}$ から $\cos\dfrac{\pi}{9}$ が作図可能か、言い換えると、$1/2$ から $\cos\dfrac{\pi}{9}$ が作図可能かどうかという問題を考える。ここで三倍角の公式 $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ に $\theta = \dfrac{\pi}{9}$ を代入する。

$$\frac{1}{2} = 4\cos^3\frac{\pi}{9} - 3\cos\frac{\pi}{9} \iff 4\cos^3\frac{\pi}{9} - 3\cos\frac{\pi}{9} - \frac{1}{2} = 0$$

$$\iff \left(2\cos\frac{\pi}{9}\right)^3 - 3\cdot\left(2\cos\frac{\pi}{9}\right) - 1 = 0$$

つまり、$2\cos\dfrac{\pi}{9}$ は

$$x^3 - 3x - 1 = 0$$

の解である。

命題 4.6 $x^3 - 3x - 1 \in \mathbb{Z}[x]$ は $\mathbb{Q}$ 上既約である。

証明に入る前に、次の補題を示す。

補題 4.7 $f(x) \in \mathbb{Z}[x]$ を定数でないモニック多項式とする。このとき

$$f(x) \text{ が } \mathbb{Q} \text{ 上可約} \quad \Longrightarrow \quad \forall p : \text{素数}\ ,\ \overline{f(x)} \text{は } \mathbb{F}_p \text{上可約}$$

証明　$f(x) \in \mathbb{Z}[x]$ に対して、$f(x)$ はモニック多項式なので、

$$
\begin{aligned}
& f(x) \text{ が } \mathbb{Q} \text{ 上可約} \\
\iff\ & f(x) \text{ が } \mathbb{Z} \text{ 上可約} \\
\iff\ & f(x) = g_1(x) \cdot g_2(x) \qquad (\exists g_i \in \mathbb{Z} \text{ はモニック}, deg(g_i) \geq 1;\ i = 1, 2) \\
\implies\ & \overline{f(x)} = \overline{g_1(x)} \cdot \overline{g_2(x)} \text{ in } \mathbb{F}_p[x] \ (\exists \overline{g_i} \in \mathbb{F}_p \text{ はモニック}, deg(\overline{g_i}) \geq 1;\ i = 1, 2) \\
\iff\ & \overline{f(x)} \text{ は } \mathbb{F}_p \text{ 上可約}
\end{aligned}
$$

である。　**証明終**

$x^3 - 3x - 1 \in \mathbb{Z}[x]$ が $\mathbb{Q}$ 上既約であることを証明する。

証明　補題の対偶を適用する。

$$\overline{x^3 - 3x - 1} = x^3 + x + 1 \text{ in } \mathbb{F}_2[x]$$

を考えると 0 も 1 も $x^3 + x + 1 \in \mathbb{F}_2[x]$ の根ではない。3 次のモニック多項式が因数分解できれば必ず解を持つので、従って $x^3 + x + 1$ は $\mathbb{F}_2$ 上既約。従って、$x^3 - 3x - 1 \in \mathbb{Z}[x]$ は $\mathbb{Q}$ 上既約である。　**証明終**

以上から、

$$\alpha := 2\cos\frac{\pi}{9} \text{の } \mathbb{Q} \text{ 上最小多項式は } f_{\mathbb{Q},\alpha}(x) = x^3 - 3x - 1 \text{ である。}$$

立方体倍積問題のときと同様に、$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ であるから、$2\cos\frac{\pi}{9}$ は RC では作図不可能であるが、MR では作図可能。従って、$\cos\frac{\pi}{9}$ が、つまり $\frac{\pi}{3}$ の三等分線が RC では作図不可能で、MR では作図可能である。

このように三等分線が作図可能な角度もあれば、三等分線が作図不可能な角度もある。

正多角形の作図

RC により正 3 角形や正方形、正 6 角形の作図は簡単にできる。$\sqrt{5}$ を作図することで正 5 角形が作図可能であろう。その他にも RC で作図可能である正多角形がユークリッドの原論に記されているが、正 17 角形の作図可能性は分かってはいないかった。しかし、1796 年ガウスが正 17 角形が RC で作図可能であることを証明した。ユークリッドの原論は紀元前 3 世紀頃のものといわれ、このように長い間、作図可能性が不明な正多角形が存在していた。RC で作図不可能な正多角形の例としては、先の角の三等分問題の議論から $\cos\frac{\pi}{9}$ が RC では作図不可能で MR では作図可能であるので、正 18 角形は RC で作図不可能で MR では作図可能であること

が分かる。さらにRCで角の二等分線の作図が可能であるので、正9角形についても同じことが言える。

ここでの目的は正n角形が作図可能であるための必要十分条件を与えることである。正n角形はオイラー関数$\varphi(n)$の値によって、RCやMRでの作図可能性を判定できる。この定理の証明のために円分体の理論、群論、ガロア理論を必要とする。最後に、ガウス-ワンツェルの定理を紹介する。

次は円分体$\mathbb{Q}(\zeta_n)$に関する定理である。以下、$\zeta_n = e^{\frac{2\pi i}{n}}$とする。

定理 4.8 $\mathbb{Q}(\zeta_n)/\mathbb{Q}$はガロア拡大であり、次が成り立つ。

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$$

$$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^{\times}$$

証明　ζ_nは$\mathbb{Q}$上の多項式$x^n - 1 = 0$の解であり、$\mathbb{Q}(\zeta_n)$は$x^n - 1 = 0$の全ての解を含むので、$\mathbb{Q}(\zeta_n)/\mathbb{Q}$はガロア拡大である。式

$$F_n(x) = \prod_{\substack{1 \le k \le n \\ (k,n)=1}} (x - {\zeta_n}^k)$$

を円周等分多項式という。$deg(F_n) = \varphi(n)$であることは明らかである。以下で$F_n(x)$がζ_nの$\mathbb{Q}$上最小多項式であることを示す。

$\forall \sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$をとる。$\sigma$は$\{{\zeta_n}^k \mid 1 \le k \le n, (k,n) = 1\}$の置換と見なせる。$F_n(x)$の各係数は$\{{\zeta_n}^k \mid 1 \le k \le n, (k,n) = 1\}$の対称式であるから、$\sigma$の作用で各係数は不変である。従って、各係数は有理数である。さらに、${\zeta_n}^k$は全て代数的整数であるから、各係数は有理整数である。つまり、$F_n(x) \in \mathbb{Z}[x]$である。

次に、円周等分多項式$F_n(x)$が$\mathbb{Q}$上既約であることを示す。

ζ_nの$\mathbb{Q}$上最小多項式を$f_{\mathbb{Q},\zeta_n}(x)$とする。従って、$f_{\mathbb{Q},\zeta_n}(x)$は$x^n - 1$を割りきるので、あるモニック多項式$h(x) \in \mathbb{Z}[x]$があって、

$$x^n - 1 = f_{\mathbb{Q},\zeta_n}(x)h(x)$$

とかける。nと互いに素な自然数mに対して$f_{\mathbb{Q},\zeta_n}(\zeta_n^m) = 0$であれば欲しい結果$F_n(x) = f_{\mathbb{Q},\zeta_n}(x)$を得る。

いま$m = {p_1}^{\alpha_1}{p_2}^{\alpha_2} \cdots {p_s}^{\alpha_s}$ ($p_1 < p_2 < \cdots < p_s$は素数)と素因数分解する。もしも任意のp_iに対して$f_{\mathbb{Q},\zeta_n}(\zeta_n^{p_i}) = 0$ならば、$f_{\mathbb{Q},\zeta_n}((\zeta_n^{p_i})^{p_i}) = 0$であり、帰納的に$f_{\mathbb{Q},\zeta_n}(\zeta_n^{{p_i}^{\alpha_i}}) = 0$を得る。よって$\zeta_n^{{p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_s}^{\alpha_s}} = {\zeta_n}^m$も$f_{\mathbb{Q},\zeta_n}(x) = 0$の解である。従って、$n$と互いに素な任意の素数$p$に対して$f_{\mathbb{Q},\zeta_n}(\zeta_n^p) = 0$であることを示せば十分である。

仮定から、$f_{\mathbb{Q},\zeta_n}({\zeta_n}^p)h({\zeta_n}^p) = 0$ である。ここで $f_{\mathbb{Q},\zeta_n}({\zeta_n}^p) \neq 0$ と仮定すれば、$h({\zeta_n}^p) = 0$ である。$H(x) = h(x^p)$ とおけば、$H(\zeta_n) = 0$ なので、ある $q(x) \in \mathbb{Z}[x]$ が存在して、

$$h(x^p) = H(x) = f_{\mathbb{Q},\zeta_n}(x) \cdot q(x)$$

を満たす。

$$h(x^p) = x^{pt} + a_{t-1}x^{p(t-1)} + a_{t-2}x^{p(t-2)} + \cdots + a_0 \ (0 \leq t < n)$$

とおけば、p を法として、

$$\begin{aligned} h(x^p) &= x^{pt} + a_{t-1}x^{p(t-1)} + a_{t-2}x^{p(t-2)} + \cdots + a_0 \\ &\equiv x^{pt} + a_{t-1}^p x^{p(t-1)} + a_{t-2}^p x^{p(t-2)} + \cdots + a_0^p \qquad (\text{フェルマーの小定理より}) \\ &\equiv h(x)^p \pmod{p} \end{aligned}$$

であるから、

$$h(x)^p \equiv f_{\mathbb{Q},\zeta_n}(x) \cdot q(x) \pmod{p}$$

より、p を法として $f_{\mathbb{Q},\zeta_n}(x) = 0$ と $h(x) = 0$ は共通解を持つ。従って、次の式の右辺は重根を持つ。

$$x^n - 1 \equiv f_{\mathbb{Q},\zeta_n}(x)h(x) \pmod{p}$$

しかし、$f(x) := x^n - 1$ を x について微分すると、p と n は互いに素であったから $f'(x) = nx^{n-1} \not\equiv 0 \pmod{p}$ となっているので、$(f, f') = 1$ であり $f(x)$ は p を法として重根を持たない。$h({\zeta_n}^p) \neq 0$ が分かったので、n と互いに素な任意の素数 p に対して $f_{\mathbb{Q},\zeta_n}(\zeta_n^p) = 0$ である。

以上から、$F_n(x)$ は ζ_n の $\mathbb{Q}$ 上最小多項式である。従って、

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = deg(F_n) = \varphi(n)$$

を得る。

定理の後半の証明に入る。

$m \in \mathbb{N}$ を n と互いに素であるとすると、${\zeta_n}^m$ は ζ_n と共役であるから写像

$$\sigma_m : \mathbb{Q}(\zeta_n) \ni \zeta \longmapsto \zeta^m \in \mathbb{Q}(\zeta_n)$$

は $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ の元である。従って、群の間の準同型

$$(\mathbb{Z}/n\mathbb{Z})^\times \ni m \longmapsto \sigma_m \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

を得る。

$\sigma_m = \sigma_k$ ならば $\zeta^m = \zeta^k$ $(\zeta \in \mathbb{Q}(\zeta_n))$ であり、つまり $m \equiv k \pmod{n}$ を満たすので上の写像は単射である。また、定理の前半から、

$$\#\left(\mathbb{Z}/n\mathbb{Z}\right)^\times = \varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \#Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

より全射である。従って、

$$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^{\times}$$

を得る。 **証明終**

補題 4.9 G を位数 n の有限アーベル群とする。このとき、n の各約数 d に対して、位数 d の G の部分群が存在する。

証明 $|G| = n$ に関する帰納法で証明する。$n = 1$ はよい。$n > 1$ とし $n-1$ まで正しいとする。約数 $d = 1$ に対しては部分群 $\{1\}$ がある。$d > 1$ を考える。p を d の素因数ととれば、n の素因数となる。コーシーの定理から、G は位数 p の元 a を含む。従って、G は位数 p の部分群 $< a >$ を持つ。アーベル群の部分群は正規部分群であるから、$G \rhd < a >$ となる。よって商群 $G/ < a >$ が定義できる。ラグランジュの定理より $G/ < a >$ は位数が n/p $(< n)$ であり、さらにアーベル群である。帰納法の仮定から、位数 d/p である $G/ < a >$ の部分群 $H/ < a >$ が存在する。$G/ < a > \rhd H/ < a >$ であるから、$G \rhd H$ を満たす。従って、位数 d の G の部分群 H が存在する。 **証明終**

定理 4.10 次の (1), (2), (3) は同値である。

(1) 正 n 角形が RC(目盛の無い定木とコンパス) で作図可能。

(2) ζ_n が RC 複素数。

(3) オイラー関数 $\varphi(n)$ が 2 の冪である。

定理 4.11 次の (1), (2), (3) は同値である。

(1) 正 n 角形が MR(目盛付き定規 (距離が 1 の二点に印をつけた定規)) で作図可能。

(2) ζ_n が MR 複素数。

(3) オイラー関数 $\varphi(n)$ が 2 と 3 の冪の積である。

上の 2 つの定理は両方同時に証明する。

証明 (2)⇒(1) : RC についても MR についても明らか。
(1)⇒(2) : 複素数平面上で考える。正 n 角形の重心 C_0 (これは作図可能) を中心に持つ単位円 C をとる。正 n 角形の一つの頂点を A_1 とし、隣の頂点のうち一つを A_2 とおく。半直線 $\overrightarrow{C_0A_1}$ と円 C、半直線 $\overrightarrow{C_0A_2}$ と円 C の交点をそれぞれ C_1 と C_2 とおく。コンパスで長さ C_1C_2 をとっておき、コンパスの一つの足を $(1, 0)$ に置き、

もう一つの足で原点中心の単位円上かつ第一象限に点 P を取る。この点 P が ζ_n である。

(2)⇒(3)：先に示した $[\mathbb{Q}(\zeta_n):\mathbb{Q}]=\varphi(n)$ を適用する。

ζ_n が RC 複素数、つまり $\zeta_n\in\mathbb{E}'$ なので、$[\mathbb{Q}(\zeta_n):\mathbb{Q}]$ は 2 の冪である。同様に、ζ_n が MR 複素数、つまり $\zeta_n\in\mathbb{V}'$ なので、$[\mathbb{Q}(\zeta_n):\mathbb{Q}]$ は 2 と 3 の冪の積である。

(3)⇒(2)：オイラー関数 $\varphi(n)$ が 2 の冪であるとする。つまり $(\mathbb{Z}/n\mathbb{Z})^\times$ は位数が 2 の冪のアーベル群である。

従って先の補題 4.9 により、任意の $i\geq 1$ に対して $(G_i:G_{i-1})=2$ を満たすような部分群の列

$$0\subset G_1\subset G_2\subset\cdots\subset G_s=(\mathbb{Z}/n\mathbb{Z})^\times\simeq(\mathbb{Z}/n\mathbb{Z})^\times$$

が存在する。よって、ガロア理論の基本定理により、2 次拡大の繰り返しの列

$$\mathbb{Q}(\zeta_n)\supset\mathbb{Q}(\zeta_n)^{G_1}\supset\mathbb{Q}(\zeta_n)^{G_2}\supset\cdots\supset\mathbb{Q}(\zeta_n)^{G_s}=\mathbb{Q}$$

がとれる。従って、ζ_n は RC 複素数 である。

同様に、$(\mathbb{Z}/n\mathbb{Z})^\times$ が位数 2 と 3 の冪の積のアーベル群であれば、ζ_n は MR 複素数 である。 **証明終**

以上で、正 n 角形が作図可能であるための必要十分条件が得られた。以下では、よく知られたガウス-ワンツェルの定理を示す。

定義 4.12 2^l+1 の形の素数をフェルマー素数という。

命題 4.13 2^l+1 が素数であるならば、$2^l+1=2^{2^t}+1\quad(0\leq\exists t\in\mathbb{Z})$ の形でかける。

証明　$0<l$ は整数であるから、$0\leq a$ を整数とし $0<b$ を奇数として $l=2^ab$ とかける。

b が奇数であるから、

$$\begin{aligned}2^{2^ab}+1 &= (2^{2^a})^b+1\\ &= \left(2^{2^a}+1\right)\left((2^{2^a})^{b-1}-(2^{2^a})^{b-2}+\cdots-2^{2^a}+1\right)\end{aligned}$$

と因数分解されるが、2^l+1 が素数だから $b=1$ とならねばならない。 **証明終**

注意 4.14 従って、フェルマー素数とは $2^{2^t}+1$ の形の素数である、とも言える。$t=0,1,2,3,4$ であるとき、つまり

$$3,\ 5,\ 17,\ 257,\ 65537$$

がフェルマー素数であることが知られている。$t=5$ であるとき、

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

と素因数分解できることを 1732 年にオイラーが示した。今日でも、上記 5 つ以外のフェルマー素数は知られていない。また、有限個かどうかも未解決である。

ガウスは、奇素数 p に対して正 p 角形が RC で作図可能であるための必要十分条件が p がフェルマー素数のときであることを証明した。またワンツェルも、1837 年の論文でそれを含む結果を証明している。

定理 4.15 (ガウス-ワンツェル) $2 < n \in \mathbb{Z}$ とする。正 n 角形が RC で作図可能であるための必要十分条件は、$n = 2^k$ $(k \geq 2)$ または $p_1 < p_2 < \cdots < p_s$ $(s \geq 1)$ をフェルマー素数の列として $n = 2^k p_1 p_2 \cdots p_s$ $(k \geq 0)$ の形となることである。

証明 まずは、p を素数とし α を正整数として $\varphi(p^\alpha)$ を考える。1 以上 p^α 以下の全ての整数のうちで p^α と互いに素でないものは p の倍数、つまり、

$$p,\ 2p,\ 3p,\ \ldots,\ p^{\alpha-1}p = p^\alpha$$

の $p^{\alpha-1}$ 個である。従って、

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$$

を得る。

よって、$k \geq 2$ とし $n = 2^k$ であるとき、$\varphi(n) = 2^{k-1}$ であるから正しい。
$2 < p_1 < p_2 < \cdots < p_s$ を素数とし、α_0 が 0 以上で、 $\alpha_1, \ldots, \alpha_s$ を 1 以上の整数として n を

$$n = 2^{\alpha_0} {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_s}^{\alpha_s}$$

と素因数分解できたとする。このとき、

$$\begin{aligned} \varphi(n) &= \varphi(2^{\alpha_0})\varphi({p_1}^{\alpha_1})\varphi({p_2}^{\alpha_2}) \cdots \varphi({p_s}^{\alpha_s}) \\ &= \varphi(2^{\alpha_0}) \cdot {p_1}^{\alpha_1 - 1}(p_1 - 1){p_2}^{\alpha_2 - 1}(p_2 - 1) \cdots {p_s}^{\alpha_s - 1}(p_s - 1) \end{aligned}$$

が成り立つ。

ここで $\varphi(n) = 2^\beta$ であるとすれば、つまり先の定理から正 n 角形が RC で作図可能であるとすれば、素因数分解の一意性から $1 \leq \forall j \leq s$ に対して

$$\begin{aligned} \alpha_j - 1 &= 0 \\ p_j - 1 &= 2^{\beta_j} \end{aligned}$$

ただし $\alpha_0 \geq 1$ ならば $\beta = (\alpha_0 - 1) + \beta_1 + \beta_2 + \cdots + \beta_s$ であり、$\alpha_0 = 0$ ならば $\beta = \beta_1 + \beta_2 + \cdots + \beta_s$ である。よって、各 p_j はフェルマー素数で

$$n = 2^{\alpha_0} p_1 p_2 \cdots p_s$$

と表せる。逆にこのとき、

$$\begin{aligned} \varphi(n) &= \varphi(2^{\alpha_0} p_1 p_2 \cdots p_s) \\ &= \varphi(2^{\alpha_0})(p_1 - 1)(p_2 - 1) \cdots (p_s - 1) \\ &= 2^\beta \end{aligned}$$

であるから定理が示された。 **証明終**

MR についても同様なことがいえて、次の定理を得る。証明は定理 4.15 と同様である。

定理 4.16 $2 < n \in \mathbb{Z}$ とする。正 n 角形が MR で作図可能であるための必要十分条件は、$n = 2^k 3^m$ $(k, m \geq 0)$、または $3 < p_1 < \cdots < p_s$ $(s \geq 1)$ を各 $p_j - 1$ が 2 の冪と 3 の冪の積となる素数の列として $n = 2^k 3^m p_1 \cdots p_s$ の形となることである。

正 n 角形はほとんどの n に対して RC で作図不可能である。実際に 1000 までの n に対して RC で作図可能な正多角形は、

$$\begin{aligned} n \;=\; & 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, \\ & 102, 120, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272, 320, 340, 384, 408, 480, \\ & 510, 512, 514, 544, 640, 680, 768, 771, 816, 960 \end{aligned}$$

の５２個しかないことは容易にわかる。また、1000 以下のフェルマー素数は４つしかないので５２個の中に奇数が少ないことが分かる。

参考文献

「ガロワと方程式」草場公邦（朝倉書店）

「無理数と超越数」塩川宇賢（森北出版）

「類体論へ至る道」足立恒雄（日本評論社）

「GALOIS THEORY」Joseph Rotman（Springer）

「GEOMETRIC CONSTRUCTIONS」George E. Martin（Springer）

「THE HISTORICAL ROOTS OF ELEMENTARY MATHEMATICS」Baunt, Jones and Bedient (Dover)

「グレイゼルの数学史 (II)」 F.N. グレイゼル（大竹出版）

「ギリシア数学の探訪」上垣渉（日本評論社）