数学史（第２回）
古代ギリシア３大不可能問題

1. Euclid の比例論

講義で述べます. あとで補足します.

2. 古代ギリシアの 3 大不可能問題

有理数解をもたない 3 次方程式は, コンパスと定規のみを用いて作図可能性を問う下記の古代ギリシアの 3 大不可能問題において重要な働きをする.

(1) (立方体倍積問題）与えられた立方体の 2 倍の体積をもつ立方体の一辺を作図せよ.
(2) (角の 3 等分問題）任意に角度が与えられたとき, その角度を 3 等分せよ.
(3) (円積問題）円が与えられたとき, それと同じ面積をもつ正方形を作図せよ.

もちろん, 特殊な器具を用いれば作図することはできる.
まず, 作図の定義（ルール）を思いだそう.

定義 2.1. (作図の定義) 作図とは定規 (目盛りはついていない) とコンパスを用いて、次のルールで有限操作を経て, 与えられた条件から求める図形を作り出すことである：

(1) 定規は与えられた 2 点を結ぶ直線を引くために使うことができる.
(2) コンパスは与えられた点を中心に, 与えられた半径の円を描くためにだけに使うことができる.

上のルールで正 3 角形, 正 4 角形, 正 5 角形, 正 6 角形が定規とコンパスでかけることは小学校で経験済みだと思う. それでは, 正 7 角形, 正 9 角形を書くことができるであろうか？
これに対してガウスは次の素晴らしい定理を提出した. ユークリッドの原論以来 2000 年の快挙といわれている.

定理 2.2. $n = 2^k p_1 p_2 \cdots p_r$ (p_i は素数, $r \geq 0$) に対して正 n 角形が定規とコンパスでかけるための必要十分条件は, 素数 p_i が異なり, かつ, それぞれがフェルマー数になることである.

7 はフェルマー数でないので, 正 7 角形は書けない. また, 正 9 角形は, $9 = 3^2$ となるので書けない,
ガウスは 19 歳のとき, 正 17 角形がコンパスと定規で書けることに気がついて数学者の道に進むことを決めたといわれている.

簡単なことではあるが, 正の整数, 有理数 ($\frac{p}{q}, p, q \in \mathbb{N}$) は構成できることはわかる. しかしここまではコンパスの使用は本質的ではない. コンパスを用いると次の数が構成できる.

補題 2.3. a が定規とコンパスで実現できる長さに対する数とする. このとき, $\sqrt{a}$ を長さに持つ線分を定規とコンパスで書ける.

このような数を作図可能数というが, 次のように特徴付けられることが知られている.

定理 2.4. ある数 α が作図可能であるための必要十分条件は, α が有理数から平方根と四則演算を何回か作用させて得られることである.

定理 2.4 より一般に, 数 a, b がコンパスと定規で表すことができれば, $a+b, a-b, ab, a/b, \sqrt{a}$ は, 再びコンパスと定規で書き表せる. このように表せる「数」は, 「代数的数」という性質を持つ数の集合に含まれる.

ここで, a が, 代数的数とは, 多項式 $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n$ ($\alpha_0, \ldots, \alpha_n$ は整数) の解になるときをいう. つまり,

$$\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_n a^n = 0.$$

「作図可能な数」は, 代数的数になることが 19 世紀に開発された「体」という概念を用いて解決される.

ところで, 全ての「数」が代数的数であるかというと, そうではない数があることが 19 世紀に示された. そのような数を「超越数」という.

(1) (エルミート, 1873 年) 自然対数の底 e は超越数である.
(2) (リンデマン, 1882 年) 円周率 π は超越数である.

π が超越数であるので, $\sqrt{\pi}$ も超越数になる. よって, 与えられた円と同じ面積をもつ正方形は作図できないことが証明できる.

一辺の長さが 1 の立方体の体積は 1 であるので, 体積 2 をもつ立方体の体積の一辺は

$$x^3 - 2 = 0$$

を満たすことがわかる. 故に, 立方体倍積問題は, 3 次方程式 $x^3 - 2 = 0$ を満たす実数が作図可能であるかという問題に変換できる. この不可能性と角の 3 等分問題の不可能性を示すのに「ガロアの体論」を利用する. ここでは, 角の 3 等分問題について触れる.

2.1. **角の 3 等分問題.** 今角度 θ を 3 等分するとする. このとき, $\frac{\theta}{3}$ が作図できることと, $\cos\theta$ が作図できることが同等であることは, 単位円を描くと理解できる.

$a = \cos\theta$ とおくと, 3 倍角の公式を用いて

$$\cos\theta = 4\cos^3\frac{\theta}{3} - 3\cos\frac{\theta}{3}$$

ここで $x = \cos^3\frac{\theta}{3}$ とおくと,

$$4x^3 - 3x - a = 0.$$

$\theta = 60^\circ$ のとき, $a = \frac{1}{2}$ となるので, $4x^3 - 3x - \frac{1}{2} = 0$, すなわち, $8x^3 - 6x - 1 = 0$ を満たす実数根が作図できるという問題に変換できる.

2.2. **有理数根を持つ 3 次方程式.** この節では, 有理数係数をもつ 3 次方程式と作図可能数との関係について述べる.

有理係数からなる 3 次方程式 $x^3 + ax^2 + bx + c = 0$ が有理数根 λ を一つ持つとすると,

$$x^3 + ax^2 + bx + c = (x - \lambda)(x^2 + px + q) = 0$$

$p = \lambda + a$, $q = \lambda^2 + a\lambda + b$) と変形でき, 2 次方程式 $x^2 + px + q = 0$ の根は, 根の公式より,

$$x = \frac{-p + \sqrt{p^2 - 4q}}{2}, \quad x = \frac{-p - \sqrt{p^2 - 4q}}{2}$$

となる. p, q は有理数より, これらの根は作図することができる.

逆に,

定理 2.5. 有理数係数からなる 3 次方程式 $x^3+ax^2+bx+c=0$ がもし, a,b,c から出発して, 定規とコンパスを有限回用いて作図可能な根を持てば, 少なくとも一つの有理数根をもつ.

すなわち,

定理 2.6. 有理数係数からなる 3 次方程式が有理数根を持たなければ, その根は, いずれも作図可能数ではない.

証明: 「ガロアの体論」を用いるので略.

□

この応用として, 角の 3 等分問題の不可能性が示される.

定理 2.7. 角の *3* 等分問題は一般には不可能である.

証明 $\theta=60^\circ$ のとき, 導かれた 3 次方程式 $8x^3-6x=1$ の実数根の作図可能性を調べる. $y=2x$ とおき, 方程式を $x^3-3x=1$ に変形する.
この方程式が有理数解 α を持つとして矛盾を示す.
実数解 $\alpha=\frac{q}{p}$ $(\gcd(p,q)=1)$ と表せたとする. このとき,

$$\left(\frac{q}{p}\right)^3-3\left(\frac{q}{p}\right)=1$$
$$q^3-3p^2q=p^3$$
$$q(q^2-3p^2)=p^3$$

$\gcd(p,q)=1$, すなわち, 共通因数を持たないので, $q=\pm1$. また,

$$q^3=p^3+3p^2q=p^2(p+3q)$$

と変形ができるので, 同じ理由から, $p=\pm1$. 故に, $\alpha=\pm1$.
ところで, $\alpha=\pm1$ のとき, 方程式 $x^3-3x=1$ を満たすことはないので矛盾. よって, α は有理数ではない.
故に, 定理 2.7 から, 角 $\theta=60^\circ$ の 3 等分は, コンパスと定規で作図できない.

□

注意 2.8. 90° の角は三等分できる. 実際, $a=\cos 90^\circ=0$ より, $4x^3-3x=0$, すなわち,

$$4x(x^2-\frac{3}{4})=0$$
$$x=\frac{\sqrt{3}}{2},\quad x=-\frac{\sqrt{3}}{2}$$

となるから理解できる.

次に正 7 角形が作図不可能であることを示す.
正 7 角形の頂点が満たす方程式は $z^7-1=0$ である.
(円を 3 等分する点は, $z^3=1$ の解, $1,\omega,\omega^2$ であったことを思いだそう.)

$$\frac{z^7-1}{z-1}=z^6+z^5+z^4+z^3+z^2+z=0$$

で, 1 以外の頂点は, $z^6+z^5+z^4+z^3+z^2+z=0$ を満たす.

ここで, $y = z + \frac{1}{z}$ とおいて式変形をすると,

$$y^3 + y^2 - 2y - 1 = 0$$

となる. $z = \cos\theta + i\sin\theta$ と表示をすると, $y = z + \frac{1}{z} = 2\cos\theta$ (すなわち, 実数). よって, z が作図可能であることと $\cos\theta$ が作図可能であることが同等であることに注意をすると, $y^3 + y^2 - 2y - 1 = 0$ が有理数解を持たないことを示せばいいことになる.

命題 2.9. $y^3 + y^2 - 2y - 1 = 0$ が有理数解を持たない.

証明: 背理法で示す, 有理数解 $\alpha = \frac{q}{p}$ $(\gcd(p, q) = 1)$ を持つとする.

$$\begin{aligned}\left(\frac{q}{p}\right)^3 + \left(\frac{q}{p}\right)^2 - 2\frac{q}{p} - 1 &= 0\\ q^3 + pq - 2p^2q - p^3 &= 0\\ q\{q^2 + (p - 2p^2)\} &= p^3\end{aligned}$$

よって, $q \mid p^3$. $\gcd(p, q) = 1$ より, $q = \pm 1$. 同様に,

$$q^3 = p\{p^2 - 2pq - q\}$$

より, $p \mid q^3$, すなわち, $p = \pm 1$. 故に, $\alpha = \pm 1$.

しかしながら, $y^3 + y^2 - 2y - 1 = 0$ は, 1 または -1 を解に持たないので矛盾. 故に, $y^3 + y^2 - 2y - 1 = 0$ は有理数解を持たない. □

注意 2.10. 正 17 角形が作図可能であることの証明に興味がある学生は, 「ガウスが切り開いた道, シモン・G. ギンディキン (三浦伸夫訳), シュプリンガー・ジャパン」を参照せよ.

2.3. **立方体倍積問題.** 角の三等分と同じく, $x^3 - 2 = 0$ は有理数根を持たないので作図不可能である.

この問題は, 「デロスの問題」とも呼ばれている. 伝記によれば, あるときギリシアのデロス島に大きな悪疫が流行し, これを恐れた人々が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, 「余の神殿のまえにある正立方体の祭壇を二倍にせよ. しからば悪疫はたちどころにやむであろう」とご神託を得て取り組まれた問題とのことです. 解決には, 2000 年以上かかりましたが.

3. 20 世紀の不可能問題

[6] で指摘されているが, 20 世紀になされた特筆べき発見の一つに, 以下の学と自然科学と社会科学を貫く共通認識がある:

「世の中には私たちの知りえないことが, できないことが, 解決できない問題が存在する.」

20 世紀に示された限界を示している 3 つの有名な原理, 定理がある.

(1) ハイゼンベルクの不確定性原理
(2) ゲーテルの不完全性定理
(3) アローの社会福利における不完全性定理

があげられる.

これらの原理, 定理は, あることを厳密に実施することが不可能であることを示している.
特に, アローの社会福利における不完全性定理は, 社会資産の分配（近いところで震災基金の分配）や選挙方法で日常的に困難に直面することを示唆している定理である. つまり, 完全に (論理的に) 解決できることはできないということ.

4. 21 世紀の数学: 6 つの未解決問題

2000 年にクレイ研究所が未解決の難問 7 題を選択し, 百万ドルの懸賞をかけた. そのうちポアンカレ予想は 2002 年頃ロシアのペレルマンにより解決され, 2006 年にフィールズ賞対象になるもペレルマンにより辞退されている：

(1) リーマン予想
(2) バーチ＆スウインナートン・ダイアー予想
(3) $P \neq NP$ 問題
(4) ホッジ予想
(5) ポアンカレ予想
(6) ヤンーミズル方程式の質量ギャップ問題
(7) ナビエーストークス方程式の解の存在問題

4.1. ポアンカレ予想.

講義で取り上げましたが, この中でポアンカレ予想は 2002 年頃ペレルマンにより解決されたが, その解決方法は, 問題に関係する位相幾何学ではなく, 微分幾何学のリッチフローと数理物理学の方法であった. 現在は, 位相幾何学の方は, ポアンカレ予想を位相幾何学の理論で解決することをあきらめているようで, 証明の鍵となったサーストンの幾何化予想と異なるサーストンの問題に取り組んでいるらしい. それも最近解決されたようで, それほど明るい材料はないようだ.

4.2. リーマン予想.

リーマン予想も講義で何度か触れましたが, 素数の分布に関係する問題で多くの数学者が取り組んでいる. たぶん小学校から数えている (?), $1+2+3+\cdots$, $1^2+2^2+3^2+\cdots+$, $1^3+2^3+\cdots$, $1^n+2^n+\cdots$ の逆数の和, $\frac{1}{1^n}+\frac{1}{2^n}+\cdots$ の和に関係するのであるが, そのゼータ関数

$$\zeta(s)=\frac{1}{1^s}+\frac{1}{2^s}+\cdots+\frac{1}{n^s}+\cdots(s\in\mathbb{C}, s\neq 1)$$

のゼロ点 s (すなわち, $\zeta(s)=0$) が, $s=a+bi$ $(a,b\in\mathbb{R})$ と表示したとき, $a=\frac{1}{2}$ となるのが予想である.
次のオイラー表示から, 素数の分布とゼター関数は関係する: $s=a+bi$ $(a>1)$ に対して

$$\begin{aligned}\zeta(s)&=\Pi_{\{p:\text{素数全体}\}}(1-p^{-s})^{-1}\\&=(1-2^{-s})^{-1}(1-3^{-s})^{-1}(1-5^{-s})^{-1}\cdots\end{aligned}$$

また, 1631 年にヨハン・ファウルハーバーが次の関係式を発見している:

$$\begin{aligned}&1^{k-1}+2^{k-1}+\cdots+n^{k-1}\\&=\frac{1}{k}(n^k+_k C_1 n^{k-1}\cdot\frac{-1}{2}+_k C_2 n^{k-2}\cdot\frac{1}{6}+_k C_3 n^{k-3}\cdot 0+_k C_4 n^{k-4}\cdot\frac{-1}{30}+\cdots)\end{aligned}$$

ここで, $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0$, $B_4 = -\frac{1}{30}, \ldots$ はベルヌイ数とよばれ, 漸化式

$$ {}_{n+1}C_1 B_n + {}_{n+1}C_2 B_{n-1} + \cdots + {}_{n+1}B_n B_1 + B_0 = 0$$

から, B_n を順に求めることができる. 特に,

$$\zeta(2k) = \frac{2^{2k-2}\pi^{2k}|B_{2k}|}{2k!}$$

が成立する. しかしながら, 奇数 $k = 2n+1$ には簡単な表示は知られていない. $\zeta(3)$ が無理数であることは 1978 年にアペリにより証明されている.

リーマン予想については, 黒川信重氏の本 ([2][3]) を参照してください.

4.3. バーチ＆スウインナートン・ダイアー予想.

通称, 提案者の名前をとって, BSD 予想と呼ばれている. 予想の詳細を述べることはできないが, これもまた楕円の周長や誇張を求める際に現れる楕円関数に関連する楕円曲線といわれる”射影空間”における 3 次曲線の”有理点”を求めることに関連する.

これは, ディオファントス型不定 1 次方程式 $ax + by = c$ $(a, b, c \in \mathbb{Z})$ を, 2 次, 3 次不定方程式に拡張して考えることに関係している. 例えば, ディオファントスの本 (3 世紀頃) で取り扱われている, ”立方数 (有理数の 3 乗で表される数) に 2 を足したら平方数になる有理数を求める”問題は, $y^2 = x^3 + 2$ と式で表されるが, これが楕円曲線の例である. 答えは, $(x, y) = (\frac{17}{4}, \frac{71}{8})$.

また, 自然数 a が「合同数」というのを, a が有理数を長さにもつ直角三角形の面積として表されることをいうが, a が合同数であることと楕円曲線: $y^2 = x(x^2 - a^2)$ が無限に多くの有理数からなる解をもつことと同値であることが知られている.

フェルマーの最終定理も関連するらしい. フェルマーの最終定理は, $n \geq 3$ に対して, $x^n + y^n = z^n$ を満たす整数が存在するしないことであったが, この式を $d = 2, 3, \ldots$ に対して $X^3 + Y^3 = dZ^3$ を考えると, これを満たす解が無限に存在することがある. 例えば, $X^3 + Y^3 = 7Z^3$ を満たす整数解は, $P_0(1, -1, 0)$, $P_1 = (2, -1, 1)$, $P_3 = (5, 4, 3)$, $P_4 = (-17, 73, 38), \ldots$ と無限の解を構成するアルゴリズムが存在する. (しかも, すべて書き尽くすことができる) 但し, $P_n = (x_n, y_n, z_n)$ としたとき, $\gcd(x_n, y_n, z_n) = 1$ としてとる.

今, $X = \frac{Y_1 + 36dZ_1}{72d}$, $Y = \frac{-Y_1 + 36dZ_1}{72d}$, $Z = \frac{X_1}{12d}$ と変換し, $X^3 + Y^3 = Z^3$ に代入すると,

$$Y_1^2 Z_1 = X_1^3 - 432 d^2 Z_1^3$$

と楕円曲線が導かれる.

いずれにしても, 楕円曲線, 楕円関数の概念は, 大学院レベルの概念であるので, 魅力的ではあるが非常に難しい.

4.4. $P \neq NP$ 問題.

コンピュータの問題に関係する問題である. コンピュータの言語は, 2 進展開で記述される. 例えば, 2 は, 2 進数で表すと, 10. ここで, $2 = (10)_2$ と書くと, $3 = (11)_2$, $4 = (100)_2$, $5 = (101)_2$, $6 = (110)_2$, $7 = (111)_2$, $8 = (1000)_2 \ldots$ と表せるが, $|x|$ を 2 進展開の長さとすると, $|2^a| = a + 1$ であることが理解でき, $|x|$ は, $\log x$ に近いことがわかる. すなわち, だいたい, $x = 2^{|x|}$. $|x|$ を x の複雑度という.

例えば, 整数 x が素数であるかどうかは, $\sqrt{x}$ まで, $2, 3, 5, \ldots$ と割っていくことで判定できるので, 計算量は, $\sqrt{x}$ までのすべての自然数の数の積になる. 但し, 割り算の計算量はあまり影響しないのでカウントしない. 例えば, $x = 101$ の場合は, $\sqrt{x}$ は, だいたい 10 であるので, $2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 = 3628800$. $3628800 = (11011101011111100000000)_2$ より, $\sqrt{x}$ までの計算量は,

22. 一方, $101 = (1100101)_2$ より, $|101| = 7$. よって, $2^{\frac{|101|}{2}}$ は, 大体 $2^4 = 16$ となり, $2^{\frac{|x|}{2}}$ に近い. 故に, x が大きくなると指数的に計算量が増えることがわかる.

定義 4.1. あるアルゴリズムが多項式時間問題といわれるのは, アルゴリズムのみに依存する多項式 $p(t)$ が存在して, どんなインプット x に対しても, アルゴリズムを遂行する時間が $p(|x|)$ 以内の時間であるときをいう. このような問題をクラス P に属する問題という.

f, g が多項式のとき, $f(g(t))$ が多項式になるので, クラス P に属する問題を組み合わせても, クラス P に属することがわかる.
典型的例は, 講義で説明したユークリッドの互除法である.

冒頭で述べたように, 合成数 x が与えられたとき, x の約数を求める問題は, P に属さない問題のように思える. しかし, 与えられた数 a が x の約数であるかは多項式時間の問題である. このように, うまい試行実験をしたとき多項式時間で解けるかもしれない.

定義 4.2. あるアルゴリズムが *NP* 問題であるとは, うまい試行実験をしたとき多項式時間でとける問題をいう.

定義から, $P \subset NP$ である. $P \neq NP$ であるという問題は, $P \subsetneq NP$ であるかどうかが問われている.

定義 4.3. *1971* 年にスティーブン・クックが定式化した概念で、クラス *NP* に属し、クラス *NP* に属する他の全問題が多項式時間帰着される問題を *NP* 完全という.

NP 完全の問題リストは, Garey and Johnson [5] に 300 以上あげられている.
$P \neq NP$ 問題は解決には遠いと 2002 年に [10] において竹内外史氏 (日本における基礎論の大家) が述べている.

4.5. **ナビエーストークス方程式の解の存在問題.**
ナビエーストークス方程式 (以下, NS 方程式) は現象につながる応用面で欠かせない偏微分方程式である. 人工の船や航空機の設計はナビエーストークス方程式 NS 方程式抜きには考えられない（らしい). 自動車の受ける空気抵抗, 高速列車が通過するトンネル内外の気流, 高層ビル間の強風といった幾何学的構造と流れの交互作用が問題となる工学的な課題に対して, シミュレーション（数値実験）を解明する際のルーチンな手段である（らしい）.
NS 方程式の数学的研究は, 前世紀にかなりの結果が蓄積されているが, ミレニアム賞の問題をはじめとするいくつかは未解決である.

4.6. **ホッジ予想, ヤンーミズル方程式の質量ギャップ問題.** これらの予想は私の能力を超えているので割愛します.

References

[1] R. Courant and H. E. Robins, 森口繁一監訳, **数学とは何か**, 原書第二版, 岩波書店, 2001 年.
[2] 黒川信重, **リーマン予想を解こう 新ゼータと因数分解からのアプローチ**, 技術評論社, 2014.
[3] 黒川信重, 小山信也, **リーマン予想のこれまでとこれから**, 日本評論社, 2009.
[4] 小林幹雄, 初等幾何, 共立出版, 2010 (初版 1958).
[5] M. R. Garey and D. S. Johnson, *Computers and intractability*, Free-man, 1979.
[6] ジェイムズ・D・スタイン (熊谷玲美その他訳), 不可能, 不確定, 不可能, 早川書房, 2011.
[7] J. J. Tattersall, 小松尚夫訳, **初等整数論 *9* 章**, 森北出版, 2008.
[8] 竹内外史, ***P* と *NP*ー計算量の根本問題**, 日本評論社, 1996.
[9] 西浦廉政編, **越境する数学**, 岩波書店, 2013.
[10] 一松信その他, **数学七つの未解決問題**, 森北出版, 2002.

[11] 矢野健太郎, 一松信解説, **角の三等分**, ちくま学芸文庫, 2006.