ピタゴラス三角形と体論

ロイロット博士

2026 年 3 月

自己紹介

- ハンドル名: ロイロット博士
  （シャーロック・ホームズ「まだらの紐」に登場する犯人の名前）
- 職業: 某企業の「社内情シス」
- 数学との関わり: 興味を持ってるだけの素人
  代数、位相空間論、集合論などちょこっとずつ齧って勉強中

問題

三辺の長さがすべて自然数である直角三角形の一つの鋭角を
$r\pi$ とするとき、r の値は無理数でなければならないことを証明せよ。

数学セミナー 2025 年 12 月「エレガントな解答をもとむ」第 1 問
出題: 佐久間一浩先生

本講演の内容

- この問題に対して私が応募した解答を紹介
- 使用した概念や定理をやや詳しめに説明
- ときどき脱線

有理数・無理数とは

- 有理数： 整数 a, b によって $\frac{a}{b}$ と表される数
- 無理数： 有理数ではない実数

無理数性の証明は一般には難しい

- ネイピア数: $e = \sum_{n=0}^{\infty} \frac{1}{n!}$ を使って証明（割と易しい）。

- 円周率: $\pi = \frac{a}{b}$ （a, b は整数）としたとき、

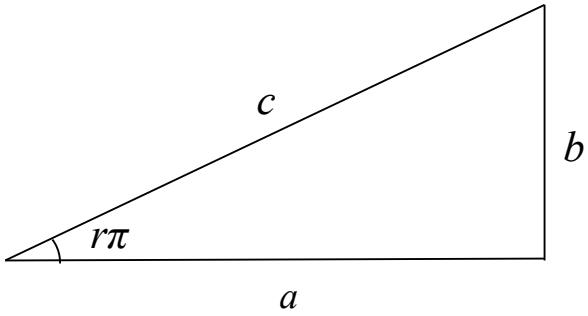
$$I_n = \int_{-1}^{1} (1-x^2)^n \cos(\frac{\pi x}{2}) dx, \quad J_n = \frac{a^{2n+1} I_n}{n!}$$

  で定まる J_n が整数で、n が十分大きいとき $0 < J_n < 1$ となることから矛盾（ちょっと難しい）。

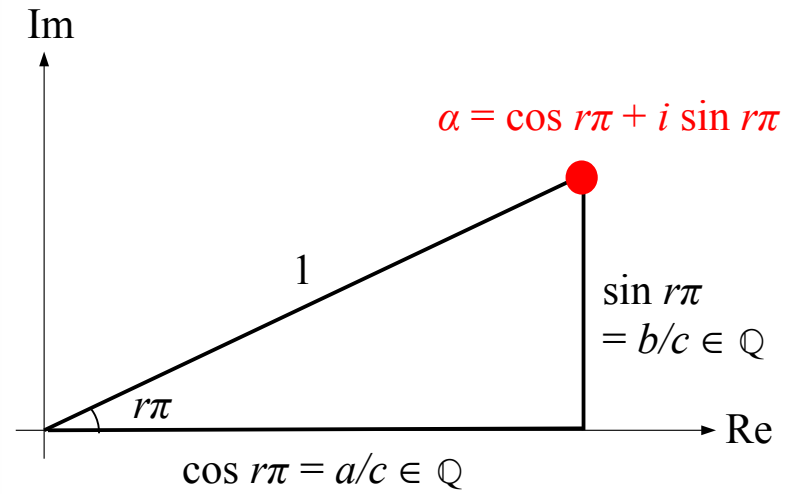
- オイラーの定数: 有理数か無理数かは未解決（超難しい）。

背理法でスタート

三辺が自然数 a, b, c の直角三角形（ピタゴラス三角形）の一つの鋭角が $r\pi$ で、かつ r が有理数であると仮定する。



複素平面上にプロット


Im
$\alpha = \cos r\pi + i \sin r\pi$
1
$\sin r\pi$
$= b/c \in \mathbb{Q}$
$r\pi$
Re
$\cos r\pi = a/c \in \mathbb{Q}$

複素数 α を根にもつ多項式

α の複素共役を $\bar{\alpha}$ とすると

$$\alpha + \bar{\alpha} = 2\cos r\pi,\ \alpha\bar{\alpha} = 1$$

根と係数の関係から、複素数 α は次の 2 次多項式 $\psi(x)$ の根。

$$\psi(x) = x^2 - (2\cos r\pi)x + 1$$

仮定より $\cos r\pi$ が有理数だから $\psi(x)$ は有理数係数。

従って $\psi(x)$ は α の有理数体 $\mathbb{Q}$ 上の最小多項式。←何それ？

体について

体とは四則演算が定義された代数系のこと。

- 代表的な体：有理数体 $\mathbb{Q}$, 実数体 $\mathbb{R}$, 複素数体 $\mathbb{C}$
- $a + b\sqrt{2}$ $(a, b \in \mathbb{Q})$ の形で表される実数の全体 $\mathbb{Q}(\sqrt{2})$ も体。
  （ $\sqrt{2}$ が分母に現れた場合も「分母の有理化」で消せる。）
- 素数 p を法とする剰余類 $\mathbb{Z}/p\mathbb{Z}$ $(= \mathbf{F}_p)$ も体（有限体の代表例）。
- 体 K の元を係数とする有理式の全体 $K(x)$ も体。

体の拡大

体 K に対して、$K \subset L$ かつ演算と単位元を共有する体 L を K の拡大体といい、組 $L : K$ を体の拡大という。
（ L/K と書くことが多いが、ここでは $L : K$ と書く。）
また、このとき K を L の部分体という。

- $\mathbb{C} : \mathbb{R}, \quad \mathbb{R} : \mathbb{Q}, \quad \mathbb{C} : \mathbb{Q}, \quad \mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ はどれも体の拡大。

単純拡大

体の拡大 $L : K$ があるとき、$\theta \in L,\ \theta \notin K$ をみたす θ に対して、

$K \cup \{\theta\}$ から有限回の四則演算によってできる L の元の全体 $K(\theta)$ は K の拡大体。

このような拡大 $K(\theta) : K$ を単純拡大という。

［例］$\mathbb{Q}(\sqrt{2}) : \mathbb{Q}, \quad \mathbb{Q}(\pi) : \mathbb{Q}, \quad \mathbb{C} : \mathbb{R}$（ $\mathbb{C} = \mathbb{R}(i)$ だから）

代数拡大，超越拡大

- $L : K$ において、K 上の 0 でない多項式 $f(x)$ があって $\theta \in L$ が $f(\theta) = 0$ をみたすとき、θ は K 上で代数的という。

  代数的でないときは超越的という。

- 全ての L の元 θ が K 上で代数的となる体の拡大 $L : K$ を、代数拡大という。

  ［例］$\mathbb{Q}(\sqrt{2}) : \mathbb{Q}, \quad \mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}, \quad \bar{\mathbb{Q}} : \mathbb{Q}$（$\bar{\mathbb{Q}}$ は代数的数の体）

- 代数拡大でない体の拡大を超越拡大という。

  ［例］$\mathbb{R} : \mathbb{Q}, \quad \mathbb{Q}(\pi) : \mathbb{Q}$（$\pi$ は $\mathbb{Q}$ 上超越的だから）

多項式の既約性

K 上の多項式が、1 次以上の K 上の多項式の 2 個以上の積にならないとき、K 上で既約という。既約でない場合は可約という。

［例］

- $x^2 - 2$ は $\mathbb{Q}$ 上で既約（$\pm\sqrt{2} \notin \mathbb{Q}$ だから）
- $x^2 - 2$ は $\mathbb{R}$ 上で可約

  $\because\ x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$
- $x^4 + x^3 + x^2 + x + 1$ は $\mathbb{Q}$ 上で既約（証明は後で）

最小多項式

$L : K$ において、$\theta \in L$ が K 上で代数的のとき、$f(\theta) = 0$ をみたす K 上の 0 でない多項式 $f(x)$ のうち、

最小次数かつモニック（最高次の係数が 1）

であるものを、θ の K 上の最小多項式という。

最小多項式の例

- $\sqrt{2}$ の $\mathbb{Q}$ 上の最小多項式

$$x^2 - 2$$

- $\sqrt{2}$ の $\mathbb{R}$ 上の最小多項式

$$x - \sqrt{2}$$

- i（虚数単位）の $\mathbb{R}$ 上（または $\mathbb{Q}$ 上）の最小多項式

$$x^2 + 1$$

最小多項式の唯一性

θ の K 上の最小多項式は、存在すれば唯一である。

[証明] 異なる多項式 $f(x), g(x)$ がどちらも θ の K 上の最小多項式とする。$f(\theta) = g(\theta) = 0$ であるから、K 上の多項式 $h(x)$ を

$$h(x) = f(x) - g(x)$$

で定めると、$h(\theta) = 0$ である。$f(x), g(x)$ がモニックだから $h(x)$ の次数はこれらより小さく、かつ 0 ではない。

これは $f(x), g(x)$ が最小多項式であることに反する。 □

最小多項式の性質

$L : K$ を体の拡大、$f(x)$ を K 上の多項式、$\theta \in L$ とする。

- $f(\theta) = 0$ ならば $f(x)$ は θ の K 上の最小多項式で割り切れる。
- θ の K 上の最小多項式は K 上で既約。
- $f(\theta) = 0$ かつ $f(x)$ が K 上で既約、かつモニックならば、$f(x)$ は θ の K 上の最小多項式。

どれも証明は容易。

分母の有理化

θ が K 上で代数的ならば、任意の $K(\theta)$ の元は、
K の元 と θ の和と積（θ の K 係数多項式の形）で表される。

［証明］任意の $K(\theta)$ の元は、ある K 上の多項式 $f(x), g(x)$ を用いて $f(\theta)/g(\theta)$ $(g(\theta) \neq 0)$ と表される。

θ の K 上の最小多項式を $h(x)$ とすると、$g(\theta) \neq 0, h(\theta) = 0$ かつ $h(x)$ は既約だから、$g(x)$ と $h(x)$ は互いに素。従って、

$$s(x)g(x) + t(x)h(x) = 1$$

をみたす K 上の多項式 $s(x), t(x)$ がとれて $f(\theta)/g(\theta) = s(\theta)f(\theta)$ □

拡大次数

体の拡大 $L : K$ において、L は次の演算によって K 上のベクトル空間とみなすことができる。

- 加法： $(u, v) \mapsto u + v \quad (u, v \in L)$
- スカラー乗法： $(\lambda, u) \mapsto \lambda u \quad (\lambda \in K,\ u \in L)$

このベクトル空間の次元（基底の個数）を $L : K$ の拡大次数といい、$[L : K]$ で表す。

［例］ $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3, \quad [\mathbb{C} : \mathbb{R}] = 2, \quad [\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$

拡大次数と最小多項式の次数

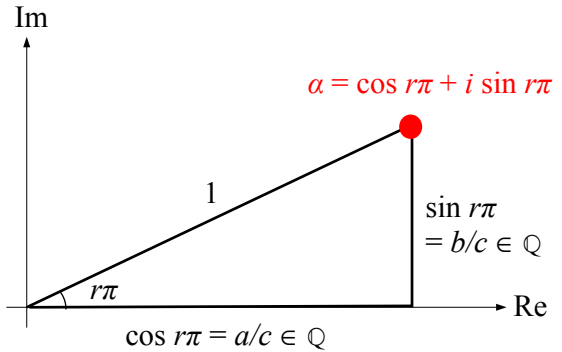
単純代数拡大 $K(\theta) : K$ の次数 $[K(\theta) : K]$ は、
θ の K 上の最小多項式の次数に等しい。

［証明］θ の K 上の最小多項式の次数を n とすると、$K(\theta)$ を K 上のベクトル空間とみたとき、n 個の $K(\theta)$ の元

$$1,\ \theta,\ \theta^2, \cdots, \theta^{n-1}$$

は一次独立、かつ任意の $K(\theta)$ の元はこれらの線型結合で表される。
従ってこれら n 個の組は $K(\theta)$ の K 上の基底である。 □

再び複素数 α について



$r = m/n$ $(m, n \in \mathbb{N})$ とすると、$\alpha = e^{r\pi i} = e^{m\pi i/n}$ より

$\alpha^{2n} = e^{2m\pi i} = 1$ となるから、α は 1 の $2n$ 乗根。

1 の n 乗根

n 乗して 1 になる複素数を、1 の n 乗根という。

1 の n 乗根は $\mathbb{C}$ 上の多項式 $x^n - 1$ の根だから、高々 n 個。

$$\zeta_n = e^{2\pi i/n} \ (= \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n})$$

としたとき、

$$\zeta_n^k \ (= e^{2k\pi i/n}) \quad (k = 1, 2, \cdots, n)$$

で表される n 個の複素数はどれも 1 の n 乗根。

従って 1 の n 乗根はちょうど n 個。

1 の原始 n 乗根

n 乗して初めて 1 になる複素数を、1 の原始 n 乗根という。

正整数 k に対して、

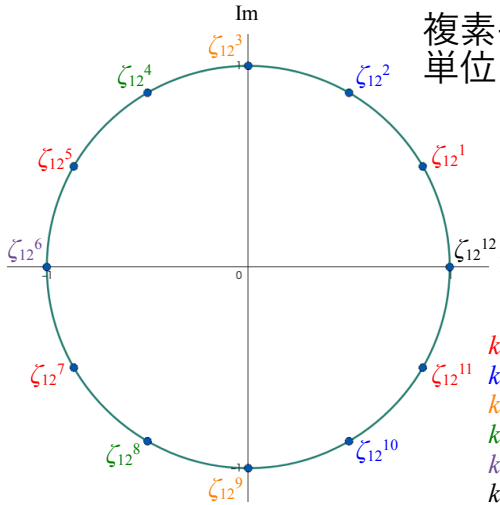
$$\zeta_n^k \ (= e^{2k\pi i/n}) \text{ が 1 の原始 } n \text{ 乗根} \quad \Leftrightarrow \quad k \text{ と } n \text{ が互いに素}$$

［証明］$d = \gcd(k, n)$ とすると、正整数 m に対して

$$(\zeta_n^k)^m = 1 \quad \Leftrightarrow \quad n \mid km \quad \Leftrightarrow \quad n/d \mid m$$

$d > 1$ ならば $m = n/d$ とすると $m < n$ かつ $(\zeta_n^k)^m = 1$ となるから ζ_n^k は 1 の原始 n 乗根ではない。$d = 1$ ならば $(\zeta_n^k)^m = 1$ から $n \leq m$ が従うから ζ_n^k は 1 の原始 n 乗根。 □

［例］円の 12 等分



複素平面上で
単位円を12等分する

［ ζ_{12}^{k} の分類 ］

k=1,5,7,11 → 原始12乗根
k=2,10 → 原始6乗根
k=3,9 → 原始4乗根
k=4,8 → 原始3乗根
k=6 → 原始2乗根
k=12 → 原始1乗根

円分多項式

1 の原始 n 乗根を 1 つずつ全て根に持つ $\mathbb{C}$ 上のモニックな多項式 $\Phi_n(x)$ を、円分多項式という。

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} (x - e^{2k\pi i/n})$$

実際の円分多項式

$$
\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= x + 1 \\
\Phi_3(x) &= x^2 + x + 1 \\
\Phi_4(x) &= x^2 + 1 \\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1 \\
\Phi_6(x) &= x^2 - x + 1 \\
\Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_8(x) &= x^4 + 1 \\
\Phi_9(x) &= x^6 + x^3 + 1
\end{aligned}
$$

円分多項式の（すごい）性質

- 【性質 1】$x^n - 1 = \prod_{d|n} \Phi_d(x)$

  ［例］ $x^{12} - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x)$

- 【性質 2】$\Phi_n(x)$ の係数は全て整数

- 【性質 3】$\Phi_n(x)$ は $\mathbb{Q}$ 上で既約

  これは次と同値。

  $\Phi_n(x)$ は全ての 1 の原始 n 乗根の $\mathbb{Q}$ 上の最小多項式

【性質1】の証明

$$f(x) = x^n - 1, \quad g(x) = \prod_{d|n} \Phi_d(x)$$

とおくと、これらはどちらもモニックかつ重根を持たない。

$f(\theta) = 0$ ならば、θ は 1 の n 乗根だから、ある d に対する 1 の原始 d 乗根である。$d \nmid n$ と仮定すると $n \equiv k \pmod{d}$, $k < d$ となる正整数 k が $\theta^k = 1$ となるから矛盾。従って $d \mid n$ より $g(\theta) = 0$ である。

$g(\theta) = 0$ ならば、θ はある n の約数 d に対する 1 の原始 d 乗根である。このとき θ は 1 の n 乗根でもあるから、$f(\theta) = 0$ である。

従って根の集合が一致するから $f(x) = g(x)$ である。 □

【性質2】の証明

$1 \leq k < n$ となる全ての k に対して $\Phi_k(x)$ は整数係数と仮定する。

$$f(x) = \prod_{d|n, d<n} \Phi_d(x)$$

とおくと（ $n = 1$ のときは $f(x) = 1$ ）、【性質1】より、

$$x^n - 1 = f(x)\Phi_n(x)$$

$x^n - 1$ と $f(x)$ は整数係数かつモニックだから、$\Phi_n(x)$ も整数係数。

従って累積帰納法により全ての n に対して $\Phi_n(x)$ は整数係数。 □

【性質 3】（既約性）の証明のために

【補題】

$f(x), g(x), h(x)$ が $\mathbb{Q}$ 上のモニック多項式で、次をみたすとする。

$$f(x) = g(x)h(x)$$

このとき、$f(x)$ が整数係数ならば $g(x), h(x)$ も整数係数。

$\Rightarrow$ これを証明するために、代数的整数という概念を用いる。

代数的整数

整数係数のモニック多項式の根となる複素数を代数的整数という。

- （普通の）整数は代数的整数。
- 整数でない有理数は代数的整数ではない。
- $\sqrt{2}, \sqrt[3]{2}, \ i, \ \dfrac{-1+\sqrt{3}i}{2}$ は代数的整数。
- $x^5 - 6x + 3$ の根（べき根で表現できない）も代数的整数。

代数的整数は和と積で閉じる (1/2)

a, b を代数的整数とすると、ある整数係数のモニック多項式 $f(x), g(x)$ があって $f(a) = g(b) = 0$ となる。

$m = \deg(f), n = \deg(g)$ とし、$m \times n$ 次の多項式 $h(x)$ を次で定める。

$$h(x) = \prod_{1 \leq i \leq m, 1 \leq j \leq n} (x - (a_i + b_j))$$

ただし $a_1, \cdots, a_m$ は $f(x)$ の、$b_1, \cdots, b_n$ は $g(x)$ の全部の根とする。
（重根は重複度分並べる）$h(a + b) = 0$ は明らか。

このとき、$a_1, \cdots, a_m$ の基本対称式は $f(x)$ の係数だから整数。
$b_1, \cdots, b_n$ の基本対称式も同様に整数。

代数的整数は和と積で閉じる (2/2)

$h(x)$ の係数は、$a_i + b_j$ $(1 \leq i \leq m, 1 \leq j \leq n)$ の基本対称式。

これは $a_1, \cdots, a_m$ からみると対称式だから、

対称式は基本対称式の多項式で表される

という定理を用いると、整数係数の $b_1, \cdots, b_n$ の多項式になる。

これはさらに $b_1, \cdots, b_n$ からみても対称式だから、結局 $h(x)$ の係数は整数。モニックであることは明らか。

従って $a + b$ は代数的整数。同様に ab も代数的整数。 □

【補題】の証明

$f(x) = g(x)h(x)$ を $\mathbb{C}$ 上で考える。

$f(x)$ はモニックかつ整数係数だから、根は全て代数的整数。

$g(x)$ は $f(x)$ を割り切るから、$g(x)$ の根も全て代数的整数。

$g(x)$ もモニックだから、係数は根の和と積で、やはり代数的整数。

一方 $g(x)$ は有理数係数。有理数かつ代数的整数は整数。

従って $g(x)$ は整数係数。$h(x)$ も同様。 □

「牛刀を用いて鶏を割く」如き証明

円分多項式の規約性の証明（1/4）

ζ を 1 の原始 n 乗根 とし、$f(x)$ を ζ の $\mathbb{Q}$ 上の最小多項式とする。

p が n を割り切らない素数のとき、$f(\zeta^p) = 0$ であることを示す。

そうでないと仮定すると、ζ^p は $f(x)$ と異なる $\mathbb{Q}$ 上の最小多項式 $g(x)$ をもち、ζ, ζ^p はどちらも 1 の n 乗根だから、

$$x^n - 1 = f(x)g(x)s(x) \tag{1}$$

一方、$g(\zeta^p) = 0$ だから多項式 $g(x^p)$ は ζ を根に持ち、

$$g(x^p) = f(x)t(x) \tag{2}$$

【補題】より $f(x), g(x), s(x), t(x)$ は全て整数係数。

円分多項式の規約性の証明（2/4）

ここから、有限体 $\mathbf{F}_p$（p を法とする剰余類が作る体）の代数閉包（全ての多項式が根を持つ拡大体）$\bar{\mathbf{F}}_p$ 上で考える。

$f(x), g(x), s(x), t(x)$ を $\mathbf{F}_p$ 上に移した多項式を $\bar{f}(x), \bar{g}(x), \bar{s}(x), \bar{t}(x)$ とすると、(2) より

$$\bar{g}(x^p) = \bar{f}(x)\bar{t}(x)$$

$\bar{\mathbf{F}}_p$ 上では $(s+t)^p = s^p + t^p$ であり、またフェルマーの小定理より $\mathbf{F}_p$ の元は p 乗しても変わらないから $(\bar{g}(x))^p = \bar{g}(x^p)$ である。従って、

$$(\bar{g}(x))^p = \bar{f}(x)\bar{t}(x)$$

これより $\bar{\mathbf{F}}_p$ 上で $\bar{f}(x)$ と $\bar{g}(x)$ は共通根を持つ。

円分多項式の規約性の証明（3/4）

一方、(1) より $\bar{\mathbf{F}}_p$ 上で、

$$x^n - 1 = \bar{f}(x)\bar{g}(x)\bar{s}(x)$$

$\bar{f}(x)$ と $\bar{g}(x)$ は共通根を持つから、$x^n - 1$ は重根を持つ。

従って、$x^n - 1$ の形式微分 nx^{n-1} は $x^n - 1$ と共通根を持つ。

しかし、整数として p は n を割り切らないから $\bar{\mathbf{F}}_p$ 上の nx^{n-1} の根は 0 のみで、これは $x^n - 1$ の根ではないから矛盾。

従って仮定が誤りであり、$f(\zeta^p) = 0$ が示された。

円分多項式の規約性の証明（4/4）

$\zeta_n = e^{2\pi i/n}$ とすると、任意の 1 の原始 n 乗根は n と互いに素な正整数 k によって ζ_n^k で表される。

k は n を割り切らない素数 $p_1, p_2, \cdots, p_m$ によって $k = p_1 p_2 \cdots p_m$ と素因数分解される。

ζ_n の $\mathbb{Q}$ 上の最小多項式 $f(x)$ に対して、先に示したことにより、

$$f(\zeta_n) = f(\zeta_n^{p_1}) = f((\zeta_n^{p_1})^{p_2}) = \cdots = f(\zeta_n^{p_1 p_2 \cdots p_m}) = f(\zeta_n^k) = 0$$

従って、$f(x)$ は全ての 1 の原始 n 乗根を根に持つ。

これより $\Phi_n(x) = f(x)$ が従うから、$\Phi_n(x)$ は $\mathbb{Q}$ 上で既約。 □

ここまでのまとめ

- 複素数 θ が $\mathbb{Q}$ 上で代数的ならば、θ の $\mathbb{Q}$ 上の最小多項式が唯一存在する。
- 複素数 $\zeta_n^k = e^{2k\pi i/n}$ $(k, n \in \mathbb{N})$ は、k, n が互いに素のとき、かつそのときに限り、1 の原始 n 乗根である。
- 1 の原始 n 乗根は $\mathbb{Q}$ 上で代数的で、最小多項式は円分多項式 $\Phi_n(x)$ である。

この事実を用いて、問題の解答を完成させる。

問題（再掲）

三辺の長さがすべて自然数である直角三角形の一つの鋭角を
$r\pi$ とするとき、r の値は無理数でなければならないことを証明せよ。

数学セミナー 2025 年 12 月「エレガントな解答をもとむ」第 1 問
出題: 佐久間一浩先生

問題の解答（1/4）

ピタゴラス三角形の一つの鋭角を $r\pi$ とし、r が有理数と仮定する。

$r = m/n$（m, n は互いに素な正整数）とすることができる。

n が奇数ならば、もう一つの鋭角は、

$$\frac{1}{2}\pi - \frac{m}{n}\pi = \frac{n-2m}{2n}\pi$$

で、$n-2m$ と $2n$ は互いに素。従って初めから n は偶数としてよい。

このとき $\dfrac{m}{n}\pi < \dfrac{1}{2}\pi$ より $n > 2m \geq 2$ であるから、$n \geq 4$ である。

問題の解答（2/4）

複素数 α を次で定める。

$$\alpha = e^{m\pi i/n} \ (= \cos(m\pi/n) + i\sin(m\pi/n) \ )$$

α は次の 2 次多項式 $\psi(x)$ の根。

$$\psi(x) = x^2 - (2\cos(m\pi/n))x + 1$$

ピタゴラス三角形の条件より $\cos(m\pi/n)$ が有理数だから、$\psi(x)$ は有理数係数で、かつ根が虚数だから $\mathbb{Q}$ 上で既約。

従って $\psi(x)$ は α の $\mathbb{Q}$ 上の最小多項式で、その次数は 2 。

問題の解答（3/4）

一方、$\alpha = e^{m\pi i/n}$ だから、$\zeta_{2n} = e^{2\pi i/2n}$ とおくと $\alpha = \zeta_{2n}^{m}$ である。

n が偶数だから m は奇数で $m, 2n$ は互いに素。これより α は 1 の原始 $2n$ 乗根。

従って α の $\mathbb{Q}$ 上の最小多項式は、円分多項式 $\Phi_{2n}(x)$ である。

この次数を調べる。

問題の解答（4/4）

n が 4 以上の偶数だから、

$$1, \quad n-1, \quad n+1, \quad 2n-1$$

は異なる 4 個の $2n$ 未満の正整数で、どれも $2n$ と互いに素。
（ユークリッドの互助法を使って示せる。）

これより ζ_{2n}, ζ_{2n}^{n-1}, ζ_{2n}^{n+1}, ζ_{2n}^{2n-1} は異なる 4 個の 1 の原始 $2n$ 乗根。

従って、α の $\mathbb{Q}$ 上の最小多項式である $\Phi_{2n}(x)$ の次数は 4 以上。

これは先の結果と矛盾。

以上より、r は無理数でなければならない。 □

感想

- この問題を解くために、体論に登場する諸概念や基本的定理を勉強することができた。
- 特に、円分多項式の既約性という一筋縄ではいかない証明を、自分なりに理解することができた。
- いくつになっても数学は面白い。

参考文献

- イアン・スチュアート, 『明解ガロア理論［原著第 3 版］』, 並木雅俊・鈴木治郎訳, 講談社, 2010
- 雪江明彦, 『整数論 1 初等整数論から p 進数へ』, 日本評論社, 2014

その他多くの Web サイトを参考にしました。ありがとうございます。

ここから補足

体の標数

体 K について、次の 2 ケースのどちらかが起こる。

① 1 を何個足し合わせても 0 にならない。

② 1 を n 個足し合わせたら 0 になる正整数 n が存在する。

①の場合、$\mathbb{N}$ が K に埋め込まれるから、$\mathbb{Z}, \mathbb{Q}$ も K に埋め込まれる。従って K は $\mathbb{Q}$ を部分体に持つ。このような体を標数 0 の体という。

②の場合、この性質を満たす正整数 n のうち最小のものを p とすると、これは素数である。なぜなら、$p = qr$ $(q, r \in \mathbb{N}, q < p, r < p)$ と仮定し、K において 1 を k 個足し合わせたものを $\bar{k}$ で表すと、$\bar{p} = \bar{q}\bar{r} = 0$ より $\bar{q} = 0$ または $\bar{r} = 0$ となって、p の最小性に反するからである。このような体を標数 p の体という。

標数 p の体について（1/3）

標数 p の体は、有限体 $\mathbf{F}_p$ を部分体に持つ。

［証明］K を標数 p の体とすると、$\mathbb{Z}$ から K への写像 $n \mapsto \bar{n}$ は環準同形写像である。

$\bar{p} = 0$ だから、$n \equiv 0 \pmod{p}$ と $\bar{n} = 0$ は同値であり、これより $n \equiv m \pmod{p}$ と $\bar{n} = \bar{m}$ は同値である。

$0 < n < p$ ならば n, p は互いに素だから $kn \equiv 1 \pmod{p}$ となる $k \in \mathbb{N}$ が存在し、このとき $\bar{k}\bar{n} = 1$ であるから $\bar{n}$ は逆元を持つ。

従って $\mathbb{Z}$ の像は p 個の元を持つ体、すなわち有限体 $\mathbf{F}_p$ であり、K は $\mathbf{F}_p$ を部分体に持つ。 □

標数 p の体について（2/3）

標数 p の体においては、次が成り立つ。

$$(s+t)^p = s^p + t^p$$

［証明］標数 0 の体上では $(s+t)^p$ は、

$$(s+t)^p = s^p + \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!} s^{p-k}t^k + t^p$$

と展開され、p が素数だから右辺中間各項の分母は p と互いに素で、係数は p の倍数になる。従って標数 p の体において同じ展開をすると、右辺は中間各項が全て消えて $s^p + t^p$ となる。 □

標数 p の体について（3/3）

（フェルマーの小定理）有限体 $\mathbf{F}_p$ においては $a^p = a$ である。

［証明］$a = 0$ のときは自明だから、以下 $a \neq 0$ とする。
${\mathbf{F}_p}^\times = \mathbf{F}_p \setminus \{0\}$ とすると、${\mathbf{F}_p}^\times$ 上で $x \mapsto ax$ で定まる写像は $a \neq 0$ だから単射であり、${\mathbf{F}_p}^\times$ が有限集合だから全単射である。従って、

$$\prod_{x \in {\mathbf{F}_p}^\times} ax = \prod_{x \in {\mathbf{F}_p}^\times} x$$

より $a^{p-1}(p-1)! = (p-1)!$ であり、$(p-1)! \neq 0$ より $a^{p-1} = 1$ が得られる。従って $a^p = a$ である。

代数閉包

任意の体 K には、代数拡大 $L:K$ で、L 上の全ての多項式が根を持つ（代数的に閉じている）ものが存在する。この L を K の代数閉包という。

（代数閉包の存在と一意性はシュタイニッツによって証明された。）

円分多項式の既約性の証明で $\mathbf{F}_p$ の代数閉包 $\bar{\mathbf{F}}_p$ を用いたが、実は代数閉包までは不要で、次の定理を用いて必要なだけ $\mathbf{F}_p$ を拡大すれば十分である。

既約多項式による体の拡大

体 K と K 上の 2 次以上の既約多項式 $f(x)$ に対し、
$f(x)$ の 1 つの根 θ によって $K(\theta)$ と表される拡大体が存在する。

[証明] K 上の多項式環 $K[x]$ をイデアル $(f(x))$ で割った剰余環 $K[x]/(f(x))$ を考え、これを L とする。

$f(x)$ が K 上既約だから、L は体である。

L において多項式 x が属する同値類を θ とすると、明らかに $L = K(\theta)$ かつ $f(\theta) = 0$ である。 □

形式微分

体 K 上の多項式

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

に対して

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1$$

で定まる多項式 $f'(x)$ を $f(x)$ の形式微分という。

（K の標数が $p > 0$ のとき、係数の $n, n-1, \cdots$ は $\mathbf{F}_p$ の元になる。）

$\mathbb{R}$ 上の多項式と同様に、和、積、および、べき乗の微分公式が成り立つことが証明できる。

重根と形式微分

体 K において、多項式 $f(x)$ が重根を持つための必要十分条件は、$f(x)$ $(\neq 0)$ とその形式微分 $f'(x)$ が共通根を持つことである。

[証明] $f(x)$ が重根 θ を持つとすると、$f(x) = (x-\theta)^2 g(x)$ と書け、かつ $f(x) \neq 0$ である。このとき $f'(x) = (x-\theta)((x-\theta)g'(x) + 2g(x))$ となるから、$f(x)$ と $f'(x)$ は共通根 θ を持つ。

逆に $f(x)$ $(\neq 0)$ と $f'(x)$ が共通根 θ を持つとすると、$f(\theta) = 0$ より $f(x) = (x-\theta)g(x)$ と書け、$f'(x) = (x-\theta)g'(x) + g(x)$ と $f'(\theta) = 0$ より $g(\theta) = 0$ だから $g(x) = (x-\theta)h(x)$ と書ける。従って $f(x) = (x-\theta)^2 h(x)$ $(h(x) \neq 0)$ となるから $f(x)$ は重根 θ を持つ。 □

「互いに素」に関する命題

m と n が互いに素な正整数で、n が奇数ならば、
$n-2m$ と $2n$ も互いに素である。

[証明]

m, n が互いに素で、n が奇数だから、$2m, n$ も互いに素。

これより $s(2m)+tn=1$ となる整数 s, t がある。

$(-s)(n-2m)+(s+t)n=1$ となるから、$n-2m, n$ も互いに素。

$n-2m$ は奇数だから、$n-2m, 2n$ も互いに素。 □

円分多項式の次数 (1/2)

$n \geq 7$ のとき、円分多項式 $\Phi_n(x)$ の次数は 4 以上

[証明]

n と互いに素な 4 個の n 未満の正整数があることを示せば良い。

- $n \equiv 0 \mod 4$ のとき

$$1, \quad n/2-1, \quad n/2+1, \quad n-1$$

は $n \geq 8$ のとき異なる 4 個の n 未満の正整数で、ユークリッドの互助法よりどれも n と互いに素。

円分多項式の次数 (2/2)

- $n \equiv 2 \mod 4$ のとき

$$1, \quad n/2-2, \quad n/2+2, \quad n-1$$

は $n \geq 10$ のとき異なる 4 個の n 未満の正整数で、ユークリッドの互助法よりどれも n と互いに素。

- n が奇数のとき

$$1, \quad (n-1)/2, \quad (n+1)/2, \quad n-1$$

は $n \geq 5$ のとき異なる 4 個の n 未満の正整数で、ユークリッドの互助法よりどれも n と互いに素。

$\cos r\pi$ について (1/2)

$\cos r\pi$ が有理数となる $0 < r < 1/2$ をみたす有理数 r は $1/3$ に限る。

[証明]

r は有理数だから、$r/2 = m/n$ とおく。ただし m, n は互いに素な正整数で、このとき $r = 2m/n$ である。

$\alpha = e^{r\pi i}$ とすると、$\cos r\pi$ が有理数だから α の $\mathbb{Q}$ 上の最小多項式は

$$x^2 - (2\cos r\pi)x + 1$$

であり、次数は 2 である。

$\cos r\pi$ について (2/2)

一方、$\alpha = e^{2m\pi i/n}$ で m, n は互いに素だから、α は 1 の原始 n 乗根。

従って α の $\mathbb{Q}$ 上の最小多項式は、円分多項式 $\Phi_n(x)$ である。

$n \geq 7$ のとき $\Phi_n(x)$ の次数は 4 以上だから、$\Phi_n(x)$ の次数が 2 になるのは $n = 3, 4, 6$ のときに限る。

このうち $0 < r < 1/2$ をみたすのは $n = 6, m = 1$ すなわち $r = 1/3$ のときに限る。 □