π の超越性

S14M075 箱木 祐也

1 はじめに

代数的数とは $\mathbb{Z}$-係数方程式 $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0$ の解となる複素数のことであり, 特に $a_n = 1$ のとき代数的整数と呼ばれる. $x^2 - 2 = 0$ の解である $\sqrt{2}$ をはじめとし, 様々な具体例を作ることは容易である. 一方で, 代数的数でないものを **超越数**というが, これに関してはそれほど知られていない. Lindemann は 1882 年に円周率 π が超越数であることを示した. 本稿ではその証明を与える.

2 鍵となる補題

n 変数多項式 $F(x_1, \cdots, x_n)$ が, 任意の置換 $\sigma \in S_n$ に対して,

$$F(x_{\sigma(1)}, \cdots, x_{\sigma(n)}) = F(x_1, \cdots, x_n)$$

を満たすとき, つまり変数 $x_1, \cdots, x_n$ の順序の置き換えに対し不変であるとき F を**対称式**という. 特に,

$$\begin{aligned}
s_1 &= s_1(x_1, \cdots, x_n) = x_1 + \cdots + x_n, \\
s_2 &= s_2(x_1, \cdots, x_n) = x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n, \\
&\ \vdots \\
s_n &= s_n(x_1, \cdots, x_n) = x_1 x_2 \cdots x_n
\end{aligned}$$

は対称式で $x_1, \cdots, x_n$ の**基本対称式**と呼ばれる. これらは X の恒等式

$$(X - x_1) \cdots (X - x_n) = X^n - s_1 X^{n-1} + s_2 X^{n-2} + \cdots + (-1)^n s_n$$

によって定義される. 実は $F(x_1, \cdots, x_n)$ が $\mathbb{Z}$-係数対称式とすると, 基本対称式 $s_1, \cdots, s_n$ の $\mathbb{Z}$-係数多項式として表すことができる (**対称式の基本定理**). すなわち,

$$F(x_1, \cdots, x_n) = Q(s_1, \cdots, s_n)$$

となる $\mathbb{Z}$-係数多項式 Q が存在する. 次が本稿で鍵となる補題である.

補題

γ を n 次代数的整数, $\gamma = \gamma_1, \cdots, \gamma_n$ をその共役とする. 勝手な n 変数 $\mathbb{Z}$-係数対称式 F に対し $F(\gamma_1, \cdots, \gamma_n)$ は整数である.

Proof. γ の最小多項式を $P(x) = x^n + a_1 x^{n-1} + \cdots + a_n (a_i \in \mathbb{Z})$ とする. これは次のようにもかける.

$$P(x) = (x - \gamma_1) \cdots (x - \gamma_n) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n.$$

いま $P(x)$ は $\mathbb{Z}$-係数多項式より $s_i = s_i(\gamma_1, \cdots, \gamma_n)$ も整数. 一方で, 対称式の基本定理より, ある $\mathbb{Z}$-係数多項式 Q が存在し $F(x_1, \cdots, x_n) = Q(s_1, \cdots, s_n)$ とかける. すると $s_i = s_i(\gamma_1, \cdots, \gamma_n)$ が整数なので $F(\gamma_1, \cdots, \gamma_n)$ も整数とわかる. □

3 定理の証明

背理法により, π を代数的数と仮定する. まず $\sqrt{-1}$ は $x^2+1=0$ の解, つまり代数的数だから, 積の $\sqrt{-1}\pi$ も代数的数である. $\theta = \sqrt{-1}\pi$ の共役を $\theta = \theta_1, \theta_2, \cdots, \theta_d$ とする. オイラーの関係式 $1 + e^{\sqrt{-1}\pi} = 0$ より $(1+e^{\theta_1})\cdots(1+e^{\theta_d}) = 0$ が成り立つ. この左辺を展開すると,

$$\sum_{j=1}^{2^d} e^{\delta_1^{(j)}\theta_1 + \cdots + \delta_d^{(j)}\theta_d} = 0 \qquad (\delta_1^{(j)}, \cdots, \delta_d^{(j)} \text{は } 0 \text{ または } 1 \text{ すべて動く})$$

とかける. 次に 2^d 個の数 $\delta_1^{(j)}\theta_1 + \cdots + \delta_d^{(j)}\theta_d$ の中で 0 でないものが n 個あったとし $\alpha_1, \cdots, \alpha_n$ とおく. すなわち,

$$\{\alpha_1, \cdots, \alpha_n\} = \{\delta_1^{(j)}\theta_1 + \cdots + \delta_d^{(j)}\theta_d \mid 1 \leqq j \leqq 2^d\} \setminus \{0\}.$$

いま $q = 2^d - n (> 0)$ とおくと, 次をみたす.

$$q + e^{\alpha_1} + \cdots + e^{\alpha_n} = 0. \tag{1}$$

実は §3.2 の**主張**から $s_n(\ell\alpha_1, \cdots, \ell\alpha_n) = \ell\alpha_1 \cdots \ell\alpha_n$ は整数であることを知っているので $\ell\alpha_1 \cdots \ell\alpha_n$ に出てくるどの素因数よりも大きい素数 p をとり固定する. ℓ を θ の最小多項式の最高次の係数として, 次の f を考える.

$$f(x) = \ell^{np} x^{p-1}(x-\alpha_1)^p \cdots (x-\alpha_n)^p, \qquad m = \deg(f) = p(n+1) - 1.$$

以下で f の x に関する $j(=0,1,2,\cdots)$ 階微分を $f^{(j)}$ とかく.

3.1 準備と方針

まず t を複素数とし, 次の積分を考える.

$$I(t) = \int_0^1 t e^{t(1-x)} f(tx) dx.$$

部分積分を繰り返して,

$$I(t) = e^t \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(t) \tag{2}$$

を得る. ここで次の量を考える.

$$J = -(I(\alpha_1) + \cdots + I(\alpha_n)).$$

すると (2) より,

$$J = -\left((e^{\alpha_1} + \cdots + e^{\alpha_n}) \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} \sum_{k=1}^{n} f^{(j)}(\alpha_k) \right).$$

ここで (1) より $e^{\alpha_1} + \cdots + e^{\alpha_n} = -q$ だから,

$$J = q \sum_{j=0}^{m} f^{(j)}(0) + \sum_{j=0}^{m} \sum_{k=1}^{n} f^{(j)}(\alpha_k). \tag{3}$$

この J を 2 通りに評価することで矛盾を導く.

3.2　各 j に対し, $f^{(j)}(0)$ が整数であること

まずは補題を用いて, 次を示す.

主張. 各 $i = 1, \cdots, n$ に対し, $s_i = s_i(\ell\alpha_1, \cdots, \ell\alpha_n)$ は整数.

Proof. 今だけ r 変数の基本対称式を s_i^r とかくことにすると $\alpha_1, \cdots, \alpha_n$ の決め方から次が成立する (例 1 参照).

$$s_i^n(\ell\alpha_1, \cdots, \ell\alpha_n) = s_i^{2^d}(\delta_1^{(1)}\ell\theta_1 + \cdots + \delta_d^{(1)}\ell\theta_d, \cdots, \delta_1^{(2^d)}\ell\theta_1 + \cdots + \delta_d^{(2^d)}\ell\theta_d).$$

いま $x_1, \cdots, x_d$ を変数として,

$$P_i(x_1, \cdots, x_d) = s_i^{2^d}(\delta_1^{(1)}x_1 + \cdots + \delta_d^{(1)}x_d, \cdots, \delta_1^{(2^d)}x_1 + \cdots + \delta_d^{(2^d)}x_d)$$

なる $\mathbb{Z}$-係数多項式を考える. ここで $\delta_1^{(j)}, \cdots, \delta_d^{(j)}$ は 0 または 1 のすべてのパターンを動くことに注意する. すると $s_i^{2^d}$ が基本対称式であることから, 任意の $\sigma \in S_d$ に対し, 次が成立する.

$$\sigma P_i(x_1, \cdots, x_d) = P_i(x_{\sigma(1)}, \cdots, x_{\sigma(d)}) = P_i(x_1, \cdots, x_d).$$

したがって P_i もまた対称式であることがわかった. 定め方から $P_i(\ell\theta_1, \cdots, \ell\theta_d) = s_i^n(\ell\alpha_1, \cdots, \ell\alpha_n)$ が成立している. とり方から ℓ は θ の最小多項式の最高次の係数で, 一般論より $\ell\theta$ は代数的数であることに注意すると, 補題より主張が従う. □

例 1

4 次基本対称式のとき. $x_4 = 0$ とすると, 次のように s_i^4 は 3 次基本対称式 s_i^3 でかくことができる.
$s_2^4(x_1, x_2, x_3, 0) = x_1x_2 + x_1x_3 + x_10 + x_2x_3 + x_20 + x_30 = s_2^3(x_1, x_2, x_3)$.
$s_3^4(x_1, x_2, x_3, 0) = x_1x_2x_3 + x_1x_20 + x_1x_30 + x_2x_30 = s_3^3(x_1, x_2, x_3)$.

次に f を変形し,

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

とかき, $\ell x = X$ とおくと, 次のようにかきかえれる.

$$f(x) = x^{p-1}((X - \ell\alpha_1) \cdots (X - \ell\alpha_n))^p = x^{p-1}(X - s_1X^{n-1} + \cdots + (-1)^n s_n)^p.$$

よって, **主張**より $f(x)$ は $\mathbb{Z}$-係数多項式である. ゆえに, 各 j に対し $f^{(j)}(0)$ は整数であることが示せた.

3.3　各 j に対し, $f^{(j)}(\alpha_1) + \cdots + f^{(j)}(\alpha_n)$ が整数であること

まず簡単な計算により, 各 $k = 1, 2, \cdots, n$ に対して, ある $\mathbb{Z}$-係数多項式 $F_k(t_1, \cdots, t_n)$ が存在して,

$$\frac{1}{p!}f^{(j)}(\alpha_k) = F_k(\ell\alpha_1, \cdots, \ell\alpha_n)$$

をみたすようにとれる (例 2 参照). この多項式をまとめて $F(t_1, \cdots, t_n) = F_1(t_1, \cdots, t_n) + \cdots + F_n(t_1, \cdots, t_n)$ とかくと, これは $\mathbb{Z}$-係数多項式であり F_k のおき方から,

$$f^{(j)}(\alpha_1) + \cdots + f^{(j)}(\alpha_n) = p!F(\ell\alpha_1, \cdots, \ell\alpha_n)$$

となっている. これは左辺を見れば分かるように, 明らかに $\ell\alpha_1, \cdots, \ell\alpha_n$ の対称式であり $F(t_1, \cdots, t_n)$ も対称式である. いま $\ell\alpha_1, \cdots, \ell\alpha_n$ は ℓ の置き方から代数的整数だから, 補題の条件をみたし $F(\ell\alpha_1, \cdots, \ell\alpha_n)$ は整数. ゆえに, 各 j に対し $f^{(j)}(\alpha_1) + \cdots + f^{(j)}(\alpha_n)$ が整数であることが示せた.

例 2

$n = 2, p = 3, j = 3$ のとき. $f(x) = \ell^6 x^2 (x - \alpha_1)^3 (x - \alpha_2)^3$. $\frac{1}{3!} f^{(3)}(\alpha_1) = \ell(\ell\alpha_1)^2(\ell\alpha_1 - \ell\alpha_2)^3$. よって $F_1(t_1, t_2) = \ell t_1^2 (t_1 - t_2)^3$ とおけば, $\frac{1}{3!} f^{(3)}(\alpha_1) = F_1(\ell\alpha_1, \ell\alpha_2)$ をみたす. 同様に $F_2(t_1, t_2) = \ell t_2^2 (t_2 - t_1)^3$ とおけばよい. また $F_1(t_2, t_1) = F_2(t_1, t_2)$ より $F(t_1, t_2) = F_1(t_1, t_2) + F_2(t_1, t_2)$ は対称式である.

3.4 $|J| \geqq (p-1)!$ であること

式 (3) の和の各項を, 以下のように場合分けして調べる.

(A) $j \leqq p - 1$ のとき. $f^{(j)}(x)$ は $x - \alpha_k$ でくくれるので $f^{(j)}(\alpha_k) = 0$.

(B) $j \leqq p - 2$ のとき. $f^{(j)}(x)$ は x^{p-1} でくくれるので $f^{(j)}(0) = 0$.

(C) $j \geqq p$ のとき. すぐにわかるように $f^{(j)}(x)$ のすべての係数は $j!$ で割り切れる. したがって §3.2 と §3.3 のことから $f^{(j)}(0)$ および $f^{(j)}(\alpha_1) + \cdots + f^{(j)}(\alpha_n)$ は $p!$ で割り切れる.

(D) $j = p - 1$ のとき. 計算により $f^{(p-1)}(0) = (-1)^n (p-1)! (\ell\alpha_1 \cdots \ell\alpha_n)^p$ がわかる. これと §3.2 のことから $f^{(p-1)}(0)$ は $(p-1)!$ で割り切れ p のとり方から, これは p では割り切れない.

以上より J は 0 でない整数かつ $(p-1)!$ で割り切れるとわかるので $|J| \geqq (p-1)!$ が示される.

3.5 矛盾を導く

まず $|I(\alpha_k)|$ を評価していく. 積分 $I(\alpha_k)$ の中身は $0 \leqq x \leqq 1$ であることと三角不等式を用いると,

$$|e^{(1-x)\alpha_k}| = e^{(1-x)\mathrm{Re}(\alpha_k)} \leqq e^{\mathrm{Re}(\alpha_k)},$$

$$|f(\alpha_k x)| = \ell^{np} |\alpha_k x|^{p-1} |\alpha_k x - \alpha_1|^p \cdots |\alpha_k x - \alpha_n|^p \leqq \ell^{np} |\alpha_k|^{p-1} (|\alpha_k| + |\alpha_1|)^p \cdots (|\alpha_k| + |\alpha_n|)^p$$

と評価できる. したがって $|I(\alpha_k)|$ は次のように評価できる.

$$|I(\alpha_k)| \leqq \int_0^1 |\alpha_k| |e^{(1-x)\alpha_k}| |f(\alpha_k x)| dx \leqq e^{\mathrm{Re}(\alpha_k)} (\ell^n |\alpha_k| (|\alpha_k| + |\alpha_1|) \cdots (|\alpha_k| + |\alpha_n|))^p.$$

ここで $c_k = \ell^n |\alpha_k| (|\alpha_k| + |\alpha_1|) \cdots (|\alpha_k| + |\alpha_n|)$ とおき $M = max\{e^{\mathrm{Re}(\alpha_1)}, \cdots, e^{\mathrm{Re}(\alpha_n)}\}$ とおけば, これは p に依存しない正の数であり,

$$|J| \leqq |I(\alpha_1)| + \cdots + |I(\alpha_n)| \leqq M(c_1^p + \cdots + c_n^p) \leqq M(c_1 + \cdots + c_n)^p \quad (\because c_k > 0)$$

となる. よって, このことと §3.4 のことを合わせると次のようになる.

$$(p-1)! \leqq |J| \leqq M(c_1 + \cdots + c_n)^p.$$

これは p が十分大きいとき成立しないので矛盾する. よって, π は超越数である. □

参考文献：塩川宇賢 (著), 『無理数と超越数』, 森北出版, 1999 年