e も π も超越数

若林誠一郎

1. e の定義

$$e \overset{\text{def}}{=} \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n = 2.7182\cdots:\ \text{Napier (ネイピア) 数}$$

(John Napier (1550–1617))

瞬間複利 例えば２０年間で預けたお金が２倍になる (すなわち利子が２０年で１０割の) 銀行に預けるより，２年ごとの複利で２年ごとに預金が 1.1 倍になる (すなわち利子が２年で１割の) 銀行に預けた方が得であることは明らかで，２０年で $(1+1/10)^{10}$ 倍になる．１年ごとに預金が 1.05 倍になる複利で預けると，２０年で $(1+1/20)^{20}$ になる．さらに複利の期間を短くして，$20/n$ 年ごとに預金が $(1+1/n)$ 倍になる複利で預けると，２０年で $(1+1/n)^n$ になる．$n\to\infty$ とすると，瞬間複利ということになり，２０年で預金が e 倍になる．

収束について

$$\begin{aligned}
a_n &:= \left(1+\frac{1}{n}\right)^n = 1 + n\cdot\frac{1}{n} + \frac{n(n-1)}{2!}\frac{1}{n^2} + \frac{n(n-1)(n-2)}{3!}\frac{1}{n^3} \\
&\quad + \cdots + \frac{n!}{n!}\frac{1}{n^n} \\
&= 1 + 1 + \frac{1}{2!}\left(1-\frac{1}{n}\right) + \frac{1}{3!}\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right) \\
&\quad + \cdots + \frac{1}{p!}\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\cdots\left(1-\frac{p-1}{n}\right) \\
&\quad + \cdots + \frac{1}{n!}\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\cdots\left(1-\frac{n-1}{n}\right)
\end{aligned}$$

$$\begin{aligned}
&\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\cdots\left(1-\frac{p-1}{n}\right) \\
&< \left(1-\frac{1}{n+1}\right)\left(1-\frac{2}{n+1}\right)\cdots\left(1-\frac{p-1}{n+1}\right)
\end{aligned}$$

より $a_n < a_{n+1}$ である．また

$$\begin{aligned}
a_n &< 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!} \\
&< 1 + 1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^{n-1}} < 3
\end{aligned}$$

ここで $n! = 2 \cdot 3 \cdot \cdots \cdot n \geq 2^{n-1}$ を用いた. 故に $\{a_n\}$ は上に有界な単調増加数列である. 実数の連続性の公理より $\{a_n\}$ は収束する.

◎ $A_n := 1 + \dfrac{1}{1!} + \dfrac{1}{2!} + \cdots + \dfrac{1}{n!}$ とおくと,

(1) $$e = \lim_{n\to\infty} A_n$$

証明 $a_n < A_n < 3$ であった. また $A_n < A_{n+1}$ は明らか. 故に $\{A_n\}$ も収束する. $n \geq p$ に対して

$$\begin{aligned} a_n >& 1 + \frac{1}{1!} + \frac{1}{2!}\Big(1 - \frac{1}{n}\Big) + \frac{1}{3!}\Big(1 - \frac{1}{n}\Big)\Big(1 - \frac{2}{n}\Big) \\ &+ \cdots + \frac{1}{p!}\Big(1 - \frac{1}{n}\Big)\Big(1 - \frac{2}{n}\Big)\cdots\Big(1 - \frac{p-1}{n}\Big) \end{aligned}$$

であった. $n \to \infty$ とすると, $\dfrac{1}{n} \to 0$ より

$$e \geq 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{p!} = A_p > a_p$$

次に $p \to \infty$ として

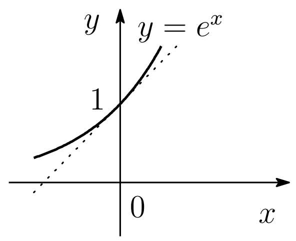
$$e \geq \lim_{p\to\infty} A_p \geq e$$

故に (1) が示された. □

2. 指数関数

$y = e^x$ の $(x, y) = (0, 1)$ におけるグラフの接線の傾きが 1 であることを示せる (微積分の教科書参照). すなわち

$$\lim_{h\to 0} \frac{e^h - 1}{h} = 1$$



指数法則 $a > 0,\ b > 0,\ x, y \in \mathbb{R}$ に対して

$$a^x a^y = a^{x+y}, \quad (a^x)^y = a^{xy}, \quad a^x b^x = (ab)^x$$

指数法則より $\dfrac{d}{dx}e^x = e^x$ であり, $a > 0$ に対して $a^x = e^{x \log a}$ であることが分かる.

複素数 z に対する e^z の定義 複素数 $z=x+iy$ ($i=\sqrt{-1}$, $x,y\in\mathbb{R}$) に対して

$$e^z(=e^{x+iy})\overset{\mathrm{def}}{=}e^x(\cos y+i\sin y)$$

と定義する. そのとき

$$e^{x_1+iy_1}e^{x_2+iy_2}=e^{(x_1+x_2)+i(y_1+y_2)} \tag{2}$$

$$\lim_{h\to 0}\frac{e^{ih}-1}{ih}=1 \tag{3}$$

証明 三角関数の加法定理を用いて,

$$\begin{aligned}
&\text{“(2) の左辺”}=e^{x_1+x_2}(\cos y_1+i\sin y_1)(\cos y_2+i\sin y_2)\\
&=e^{x_1+x_2}\{(\cos y_1\cos y_2-\sin y_1\sin y_2)+i(\sin y_1\cos y_2+\cos y_1\sin y_2)\}\\
&=e^{x_1+x_2}(\cos(y_1+y_2)+i\sin(y_1+y_2))=\text{“(2) の右辺”}
\end{aligned}$$

故に (2) が示された. $h\in\mathbb{R}$ のとき, 定義より

$$\frac{e^{ih}-1}{ih}=\frac{\cos h+i\sin h-1}{ih}=\frac{\cos h-1}{ih}+\frac{\sin h}{h}\to 1\ (\ h\to 0)$$

ここで $\displaystyle\lim_{h\to 0}\frac{\cos h-1}{ih}=0$, $\displaystyle\lim_{h\to 0}\frac{\sin h}{h}=1$ を用いた. よって (3) が示された. □

指数法則 (2) は三角関数の加法定理と同値である. $\theta\in\mathbb{R}$ として

$$\begin{cases}\cos\theta=\dfrac{1}{2}(e^{i\theta}+e^{-i\theta})\\[2mm] \sin\theta=\dfrac{1}{2i}(e^{i\theta}-e^{-i\theta})\end{cases}$$

また $e^{i\pi}=\cos\pi+i\sin\pi=-1$ である.

3. e の超越性

$\alpha\in\mathbb{C}$ (複素数) に対して, α が整数を係数とするある代数方程式の解であるとき, すなわち 自然数 m と整数 a_0, a_1, $\cdots$, a_m を $a_0\neq 0$ かつ $a_0\alpha^m+a_1\alpha^{m-1}+\cdots+a_{m-1}\alpha+a_m=0$ を満たすように選べるとき, α は代数的数であるという. 方程式の両辺を a_0 で割れば, α が最高次の係数が 1 である有理数を係数とする代数方程式の解であること同値である.

例 $\sqrt{2}$ は $x^2-2=0$ の解より, $\sqrt{2}$ は代数的数. α が有理数ならば, 自然数 p と整数 q を適当に選んで $\alpha=\dfrac{q}{p}$ と書ける. 故に α は $px-q=0$

の解であり, α は代数的数である. α が代数的数でないとき, α は超越数であるという.

注意 代数的数の全体は可算 (無限) 個, すなわち代数的数のすべてに番号を打って, 番号順に $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \cdots$ と並べることができる. 超越数の全体は非可算 (無限) 個である.

定理 1 (Ch. Hermite(エルミート), 1873) e は超越数である.

注意 Ian Stewart の証明が [M] に載っていて, 以下の証明はそれを転記したものである.

証明 背理法を用いて示そう (e が代数的数であると仮定して矛盾を導く). 今自然数 m と整数 $a_0\ (\neq 0), a_1, \cdots, a_m$ を

$$a_0 e^m + a_1 e^{m-1} + \cdots + a_{m-1} e + a_m = 0 \tag{4}$$

を満たすように選べたと仮定する. $e \neq 0$ より $a_m \neq 0$ と仮定してよい. p を $p > m$, $p > |a_m|$ を満たす素数とする.

$$f(x) := \frac{x^{p-1}(x-1)^p(x-2)^p\cdots(x-m)^p}{(p-1)!},$$
$$F(x) := f(x) + f'(x) + \cdots + f^{(mp+p-1)}(x)$$

そのとき $0 < x < m$, $j = 0, 1, 2, \cdots, m$ に対して $|x - j| < m$ より,

$$|f(x)| \leq \frac{m^{p-1}m^{mp}}{(p-1)!} = \frac{m^{mp+p-1}}{(p-1)!} \quad (\ 0 < x < m) \tag{5}$$

また $f(x)$ は $(mp+p-1)$ 次の多項式であるので, $f^{(mp+p)}(x) \equiv 0$ である. 故に

$$-\frac{d}{dx}(e^{-x}F(x)) = e^{-x}[F(x) - F'(x)] = e^{-x}f(x)$$

故に微積分学の基本定理より

$$\begin{aligned} a_{m-j}\int_0^j e^{-x}f(x)\,dx &= a_{m-j}[-e^{-x}F(x)]_0^j \\ &= a_{m-j}F(0) - a_{m-j}e^{-j}F(j) \quad (\ j = 0, 1, 2, \cdots, m) \end{aligned} \tag{6}$$

(6) の両辺に e^j をかけて j について足し合わせて (4) を用いて,

$$\sum_{j=0}^m a_{m-j}e^j \int_0^j e^{-x}f(x)\,dx = F(0)\sum_{j=0}^m a_{m-j}e^j - \sum_{j=0}^m a_{m-j}F(j)$$
$$= -\sum_{j=0}^m a_{m-j}F(j) = -\sum_{j=0}^m \sum_{k=0}^{mp+p-1} a_{m-j}f^{(k)}(j)$$

次の主張が成り立つ:

(i) 整数 j, k が $0 \leq j \leq m$, $0 \leq k < p-1$ を満たすならば, $f^{(k)}(j) = 0$

(ii) $f^{(p-1)}(0)$ は p で割り切れない

(iii) $f^{(p-1)}(j) = 0$ ($j = 1, 2, \cdots, m$)

(iv) $0 \leq j \leq m$, $p \leq k \leq mp + p - 1$ のとき, $f^{(k)}(j)$ は p で割り切れる整数

実際, $0 \leq k < p-1$ のとき $f^{(k)}(x)$ は $x(x-1)\cdots(x-m)$ で割り切れるので, (i) は明らか. $f^{(p-1)}(0) = (-1)^p(-2)^p \cdots (-m)^p$ であり, p は素数で $p > m$ より, (ii) が分かる. $1 \leq j \leq m$ のとき $f(x) = (x-j)^p g_j(x)$ と表せるので, (iii) も明らか.

$$f(x) = \frac{x^{p-1}}{(p-1)!}\, g_0(x), \quad g_0(x) = (x-1)^p \cdots (x-m)^p$$

より, $p \leq k \leq mp + p - 1$ ならば $k - p + 1 \geq 1$ で

$$\begin{aligned} f^{(k)}(0) &= \binom{k}{p-1} g_0^{(k-p+1)}(0) \\ &= \binom{k}{p-1} p \Big(\frac{d}{dx}\Big)^{k-p} \Big\{ \frac{g_0(x)}{(x-1)} + \cdots + \frac{g_0(x)}{(x-m)} \Big\}\Big|_{x=0} \end{aligned}$$

ここで

$$\binom{k}{l} = \frac{k!}{l!(k-l)!} \quad (0 \leq l \leq k)$$

故に $f^{(k)}(0)$ は p で割り切れる整数である. また $1 \leq j \leq m$ のとき

$$f^{(k)}(j) = \binom{k}{p} p g_j^{(k-p)}(j)$$

ここで

$$g_j(x) = x^{p-1}(x-1)^p \cdots (x-j+1)^p (x-j-1)^p \cdots (x-m)^p$$

よって $f^{(k)}(j)$ は p で割り切れる整数であり, 以上より (iv) が示された.

$$I := -\sum_{j=0}^{m} \sum_{k=0}^{mp+p-1} a_{m-j} f^{(k)}(j)$$

とおけば, (i), (iii) より

$$I = -a_m f^{(p-1)}(0) - \sum_{j=0}^{m} \sum_{k=p}^{mp+p-1} a_{m-j} f^{(k)}(j)$$

(iv) より $\displaystyle\sum_{j=0}^{m} \sum_{k=p}^{mp+p-1} a_{m-j} f^{(k)}(j)$ は p で割り切れ, (ii) と a_m が p で割り切れないことより, $-a_m f^{(p-1)}(0)$ も p で割り切れない. したがって I は p で割り切れない整数である. 特に

$$|I| \geq 1 \tag{7}$$

一方 $x > 0$ ならば $e^{-x} \leq 1$ であるので, (5) を用いて

$$\begin{aligned} |I| &= \left|\sum_{j=0}^{m} a_{m-j} e^j \int_0^j e^{-x} f(x)\, dx\right| \leq \sum_{j=1}^{m} |a_{m-j}| e^j \int_0^j \frac{m^{mp+p-1}}{(p-1)!}\, dx \\ &\leq \sum_{j=0}^{m} |a_{m-j}| e^j \frac{m^{(m+1)p}}{(p-1)!} \to 0 \quad (\ p \to \infty) \end{aligned}$$

これは (7) に矛盾する. ここで, $a > 0$ に対して $\dfrac{a^p}{(p-1)!} \to 0$ ($p \to \infty$) であることと (付録 補題 A.1 参照), いくらでも大きい素数が存在することを用いた (付録 補題 A.2 参照). 故に e は超越数である. □

4. π の超越性

定理 1 の証明中の論法と $e^{i\pi} + 1 = 0$ を用いて, 次の定理を示すことができる.

定理 2 (F. von Lindemann(リンデマン), 1882) π は超越数である.

証明 [M] にしたがって証明を与える. π が代数的数であると仮定して矛盾を導こう. そのとき $i\pi$ も代数的数である (付録 補題 A.5 参照). 有理数を係数とする多項式 $\theta_1(x) = x^n + \gamma_1 x^{n-1} + \cdots + \gamma_{n-1} x + \gamma_n$ で $\theta_1(i\pi) = 0$ を満たすものがある. $\alpha_1 = i\pi$ とおいて, $\alpha_2, \cdots, \alpha_n \in \mathbb{C}$ を選んで

$$\theta_1(x) = \prod_{j=1}^{n} (x - \alpha_j)$$

と書ける (付録 定理 A.3 参照). $e^{i\pi} + 1 = 0$ より

$$(e^{\alpha_1} + 1)(e^{\alpha_2} + 1) \cdots (e^{\alpha_1} + 1) = 0$$

また

$$(e^{\alpha_1}+1)(e^{\alpha_2}+1)\cdots(e^{\alpha_n}+1)=1+\sum_{k=1}^{n}\sum_{1\le j_1<j_2<\cdots<j_k\le n} e^{\alpha_{j_1}+\alpha_{j_2}+\cdots+\alpha_{j_k}}$$

ここで $\displaystyle\sum_{1\le j_1<j_2<\cdots<j_k\le n}$ は $1\le j_1<j_2<\cdots<j_k\le n$ を満たす自然数の組 $(j_1,j_2,\cdots,j_k)$ について足し合わせることを意味する.

$$\theta_2(x)=\prod_{1\le j<k\le n}(x-(\alpha_j+\alpha_k))$$

とおくと, $\theta_2(x)$ の係数は α_1, $\cdots$, α_n の整数を係数とする対称式である (付録 定理A.3 の後を参照). 故に, α_1, $\cdots$, α_n の基本対称式に等しい $-\gamma_1$, γ_2, $\cdots$, $(-1)^n\gamma_n$ の整数を係数とする多項式である. よって $\theta_2(x)$ の係数は有理数である (定理 A.4 参照). 同様に

$$\theta_k(x)=\prod_{1\le j_1<j_2<\cdots<j_k\le n}(x-(\alpha_{j_1}+\alpha_{j_2}+\cdots+\alpha_{j_k}))\quad (\ k=1,2,\cdots,n)$$

とおくと, $\theta_k(x)$ の係数は有理数である.

$$\tilde{\theta}(x)=\theta_1(x)\theta_2(x)\cdots\theta_n(x)$$

とおき, 整数を係数にもつ多項式 $\theta(x)$ を, 零でない整数 c と 非負の整数 γ を選んで

$$\theta(x)=cx^{-\gamma}\tilde{\theta}(x),\quad \theta(0)\neq 0$$

なる形をもつように選ぶ. そのとき

$$\theta(x)=cx^r+c_1x^{r-1}+\cdots+c_r=c\prod_{j=1}^{r}(x-\beta_j)$$

と書ける. ここで c_1, $\cdots$, c_r は整数で, $c_r\neq 0$ を満たす.

(8) $$0=(e^{\alpha_1}+1)\cdots(e^{\alpha_n}+1)=e^{\beta_1}+e^{\beta_2}+\cdots+e^{\beta_r}+\gamma+1$$

である. p (>1) を素数として,

$$f(x):=c^sx^{p-1}\frac{\theta(x)^p}{(p-1)!},\quad s=rp-1$$
$$F(x):=f(x)+f'(x)+\cdots+f^{(s+p)}(x)$$

とおく．そのとき

$$\frac{d}{dx}[e^{-x}F(x)] = e^{-x}(F'(x) - F(x)) = -e^{-x}f(x)$$

故に

$$e^{-x}F(x) - F(0) = -\int_0^x e^{-y}f(y)\,dy$$

上の積分で $y = \lambda x$ と λ についての積分に変数変換して，

$$F(x) - e^x F(0) = -x\int e^{(1-\lambda)x}f(\lambda x)\,d\lambda \tag{9}$$

(8) より $\displaystyle\sum_{j=1}^{r} e^{\beta_j} = -(\gamma+1)$ であり，これと (9) で $x = \beta_j$ を代入して j について和をとって，

$$\sum_{j=1}^{r} F(\beta_j) + (\gamma+1)F(0) = -\sum_{j=1}^{r}\beta_j\int_0^1 e^{(1-\lambda)\beta_j}f(\lambda\beta_j)\,d\lambda \tag{10}$$

p が十分大なるとき, (10) の左辺が零でない整数であることを示そう．f の定義より，

$$\sum_{j=1}^{r} f^{(t)}(\beta_j) = 0 \quad (\ 0 \le t < p)$$

また $\displaystyle\sum_{j=1}^{r} f^{(t)}(\beta_j)$ ($t \ge p$) は整数で p で割り切れる．実際 $\theta(\beta_j) = 0$, $\displaystyle\left(\frac{d}{dx}\right)^t (x-\beta_j)^p|_{x=\beta_j} = 0$ ($0 \le t < p$)．故に $\displaystyle\sum_{j=1}^{r} f^{(t)}(\beta_j)$ ($t \ge p$) は β_1, $\cdots$, β_r の次数 $(s+p-t)$ ($\le s$) の整数を係数とする対称式で係数は p と c^s で割り切れる．よって定理 A.4 より $\displaystyle\sum_{j=1}^{r} f^{(t)}(\beta_j)$ は $pc^s\times$ 「$\dfrac{c_1}{c}$, $\cdots$, $\dfrac{c_r}{c}$ の s 次以下の整数を係数とする多項式」．故に $\displaystyle\sum_{j=1}^{r} f^{(t)}(\beta_j)$ は整数で p で割り切れる．k_t ($p \le t \le p+s$) を整数として

$$\sum_{j=1}^{r} f^{(t)}(\beta_j) = pk_t \quad (\ t = p, p+1, \cdots, p+s)$$

と表せて, (10) の左辺は K を整数として $Kp+(\gamma+1)F(0)$ の形で表せる. また整数 h_t を適当に選べば

$$
\begin{aligned}
&f^{(t)}(0)=0 \quad (\ 0\le t\le p-2)\\
&f^{(p-1)}(0)=c^s c_r^p\\
&f^{(t)}(0)=ph_t \quad (\ p\le t\le s+p)
\end{aligned}
$$

と表せる. 故に (10) の左辺は K' を整数として $K'p+(\gamma+1)c^s c_r^p$ の形で表せる. $p>\gamma+1$, $p>c$, $p>c_r$ ならば, p が素数であることより (10) の左辺は零でない整数である. 一方

$$
\begin{aligned}
&\left|\int_0^1 e^{(1-\lambda)\beta_j} f(\lambda\beta_j)\,d\lambda\right|\\
&\le e^{|\mathrm{Re}\ \beta_j|}|c|^{s+p}|\beta_j|^{p-1}\int_0^1 \lambda^{p-1}\frac{\prod_{l=1}^r(\lambda|\beta_j|+|\beta_l|)^p}{(p-1)!}\,d\lambda\\
&\le e^{|\mathrm{Re}\ \beta_j|}|c|^{s+p}|\beta_j|^{p-1}\frac{\prod_{l=1}^r(|\beta_j|+|\beta_l|)^p}{p!}\to 0 \quad (\ p\to\infty)
\end{aligned}
$$

より (10) の右辺は $p\to\infty$ のとき 0 に収束する. これは矛盾である. したがって π は超越数である. ここで $x,y\in\mathbb{R}$ に対して

$$|e^{x+iy}|=e^x\le e^{|x|}$$

であることを用いた. □

5. 円積問題

ギリシアの三大難問: 定木とコンパスのみを使って, 次を作図せよ.

1. 角の 3 等分 (例えば, 角 60° ($=\pi/3$) を 3 等分せよ).
2. 立方体の倍積 $\cdots$ 与えられた立方体のちょうど 2 倍の体積をもつ立方体を作図せよ
   (長さ 1 が与えられたとき, $\sqrt[3]{2}$ の長さを作図せよ).
3. 円の正方形化 (円積問題) $\cdots$ 与えられた円と同じ面積をもつ正方形を作図せよ.

定木とコンパスによる作図: (座標) 平面上の点 $O(0,0)$, $E(1,0)$, $P_1(x_1, y_1)$, $\cdots$, $P_r(x_r,y_r)$ が与えられたとき, 直線としてはこれらの 2 点を通

る直線のみを考え, 円としてはこれらの点の 1 つを中心, これらの点の 2 点間の距離を半径とする円のみを考える. そのとき, これらの直線及び円の交点として得られる点を O, E, P_1, $\cdots$, P_r に追加する. 以下これを有限回繰り返して点 $P(x, y)$ が得られたとすると, x, y は 0, 1, x_1, x_2, $\cdots$, x_r, y_1, $\cdots$, y_r に 5 種の演算

(1) 加法　(2) 減法　(3) 乗法　(4) 除法　(5) 正の数の開平 ($\sqrt{\ }$)

を施して得られる実数である (逆もいえる). 特に x 及び y はそれぞれ m を自然数として 0, 1, x_1, x_2, $\cdots$, x_r, y_1, $\cdots$, y_r の有理式を係数とする 2^m 次の代数方程式の解である.

1839 年に Wantzel がギリシアの難問 1, 2 が作図不可能であることを示した (Galois の理論). ギリシアの難問 3 (円積問題) は長さ 1 が与えられたとき, $\sqrt{\pi}$ の長さを作図できるかという問題になる. π が超越数であることが示されたので, $\sqrt{\pi}$ も超越数であることが分かる (もし $\sqrt{\pi}$ が代数的数なら, 付録の補題 A.5 より π も代数的数になってしまう). したがって円積問題が作図不可能であることが分かる.

付録

補題 A.1 $a > 0$ に対して $\dfrac{a^n}{n!} \to 0$ ($n \to \infty$)

証明 実数の性質 (アルキメデスの公理) より, 自然数 n_0 を $n_0 + 1 \geq 2a$ を満たすように選べる. 故に $n > n_0$ に対して

$$0 < \frac{a^n}{n!} = \frac{a^{n_0}}{n_0!} \frac{a}{n_0+1} \frac{a}{n_0+2} \cdots \frac{a}{n} \leq \frac{a^{n_0}}{n_0!} 2^{-(n-n_0)} \to 0 \quad (n \to \infty)$$

故に補題が示された. □

補題 A.2 いくらでも大きい素数が存在する.

注意 1 より大きい整数で, 1 とそれ自身以外に正の約数をもたない数を素数という. 「整数 a, b に対して積 ab が素数 p で割り切れるならば, a, b のどちらかは p で割り切れる」という性質を示すことができる. さらに, 1 より大きいどんな整数も素数の積の形で (積の順序を無視すれば一通りに) 表せること (素因数分解定理) を帰納法を用いて示すことができる. 以下の証明でこの事実を用いる.

証明 背理法で示そう. 素数が有限個であると仮定する. それらを小さいものから並べて p_1, p_2, $\cdots$, p_n とする (p_n が最大の素数).

$$N := p_1 p_2 \cdots p_n + 1 \ (> p_n)$$

とおくと, N は $p_1, p_2, \cdots, p_n$ で割り切れない. これは素因数分解定理に矛盾する. 故にいくらでも大きい素数が存在する. $\square$

以下の2つの定理の証明については, 代数関係の本を参照されたい.

定理 A.3 (代数学の基本定理) 複素数を係数とする代数方程式 $a_0x^m + a_1x^{m-1} + \cdots + a_m = 0$ ($m \geq 1$, $a_0 \neq 0$) は必ず複素数の解をもつ. したがって剰余の定理より, 複素数 $\alpha_1, \cdots, \alpha_m$ を

$$a_0x^m + a_1x^{m-1} + \cdots + a_m = a_0 \prod_j^m (x - \alpha_j)$$

を満たすように選ぶことができる.

対称式 n 個の変数 $x_1, \cdots, x_n$ の多項式 $f(x_1, \cdots, x_n)$ に対して, $1 \leq j < k \leq n$ を満たす任意の自然数の組 (j, k) に対して

$$f(x_1, \cdots, x_{j-1}, x_k, x_{j+1}, \cdots, x_{k-1}, x_j, x_{k+1}, \cdots, x_n) = f(x_1, \cdots, x_n)$$

が成り立つとき, $f(x_1, \cdots, x_n)$ は $x_1, \cdots, x_n$ の対称式であるという (すなわちどの2つの変数 x_j と x_k を交換しても多項式 f が不変であるとき, f は対称式であるという).

$$\begin{aligned}
s_1(= s_1(x_1, \cdots, x_n)) &:= x_1 + x_2 + \cdots + x_n \\
s_2(= s_2(x_1, \cdots, x_n)) &:= \sum_{1 \leq j < k \leq n} x_j x_k \\
&\cdots \\
s_r(= s_r(x_1, \cdots, x_n)) &:= \sum_{1 \leq j_1 < j_2 < \cdots < j_r \leq n} x_{j_1} x_{j_2} \cdots x_{j_r} \\
&\cdots \\
s_n(= s_n(x_1, \cdots, x_n)) &:= x_1 x_2 \cdots x_n
\end{aligned}$$

とおくと, $s_1, s_2, \cdots, s_n$ は $x_1, \cdots, x_n$ の対称式になるが, 特にこれらの n 個の多項式を $x_1, \cdots, x_n$ の基本対称式という.

$$\prod_{j=1}^n (x - x_j) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n$$

である.

定理 A.4 $f(x_1, \cdots, x_n)$ をそれぞれ複素数, 実数, 有理数または整数を係数とする $x_1, \cdots, x_n$ の対称式とすると, $f(x_1, \cdots, x_n)$ はそれぞれ複素数, 実数, 有理数または整数を係数とする基本対称式 $s_1, \cdots, s_n$ の多項式として表すことができる.

補題 A.5 α, β を代数的数とする. そのとき, $\alpha+\beta, \alpha\beta$ も代数的数である. さらに $\alpha \neq 0$ ならば $\dfrac{1}{\alpha}$ も代数的数である.

証明 α の満たす有理数係数の代数方程式を

$$p(x) = x^m + a_1 x^{m-1} + \cdots + a_m = 0$$

β の満たす有理数係数の代数方程式を

$$q(x) = x^n + b_1 x^{n-1} + \cdots + b_n = 0$$

とする. $\alpha_1 = \alpha$, $\beta_1 = \beta$ とおき, 複素数 $\alpha_2, \cdots, \alpha_m, \beta_2, \cdots, \beta_n$ を選んで, 定理 A.3 より

$$p(x) = \prod_{j=1}^{m}(x - \alpha_j), \quad q(x) = \prod_{k=1}^{n}(x - \beta_k)$$

と書ける. $-a_1, a_2, \cdots, (-1)^m a_m$ は $\alpha_1, \cdots, \alpha_m$ の基本対称式 ($\lambda_1, \cdots, \lambda_m$ の基本対称式に $\lambda_1 = \alpha_1, \cdots, \lambda_m = \alpha_m$ を代入したもの) である. 同様に, $-b_1, b_2, \cdots, (-1)^n b_n$ は $\beta_1, \cdots, \beta_n$ の基本対称式である.

$$r(x, \lambda_1, \cdots, \lambda_m, \zeta_1, \cdots, \zeta_n) := \prod_{j=1}^{m}\prod_{k=1}^{n}(x - \lambda_j - \zeta_k)$$

とおくと, $r(x, \lambda_1, \cdots, \lambda_m, \zeta_1, \cdots, \zeta_n)$ は $(x, \zeta_1, \cdots, \zeta_n)$ の多項式とみて, その各係数は $\lambda_1, \cdots, \lambda_m$ の整数を係数とする対称式になる. 故に定理 A.4 より係数は $\lambda_1, \cdots, \lambda_m$ の基本対称式の整数を係数とする多項式で表され, $r(x, \alpha_1, \cdots, \alpha_m, \zeta_1, \cdots, \zeta_n)$ は有理数を係数とする $(x, \zeta_1, \cdots, \zeta_n)$ の多項式である. さらにこれを x の多項式とみて, その各係数は $\zeta_1, \cdots, \zeta_n$ の有理数を係数とする対称式になっている. 故に同様にして $r(x, \alpha_1, \cdots, \alpha_m, \beta_1, \cdots, \beta_n)$ は有理数を係数とする x の多項式である. $r(x, \alpha_1, \cdots, \alpha_m, \beta_1, \cdots, \beta_n) = 0$ の解が $\alpha_j + \beta_k$ ($1 \leq j \leq m$, $1 \leq k \leq m$) であることより, 特に $\alpha + \beta$ は代数的数である. 同様に $\alpha\beta$ が代数的数であることを示せ

る. 今 $\alpha \neq 0$ と仮定する. そのとき $p(x) = 0$ の解のうち零であるものを除いて, $a_m \neq 0$ と仮定してよい. $\alpha_j \neq 0$ ($1 \leq j \leq m$) となる.

$$s(x, \lambda_1, \cdots, \lambda_m) := \prod_{j=1}^{m} (\lambda_j x - 1)$$

とおくと, $s(x, \lambda_1, \cdots, \lambda_m)$ は x の多項式とみて, 各係数が $\lambda_1, \cdots, \lambda_m$ の整数を係数とする対称式になる. 故に同様に $s(x, \alpha_1, \cdots, \alpha_m)$ は有理数を係数とする x の多項式で $\dfrac{1}{\alpha}$ は $s(x, \alpha_1, \cdots, \alpha_m) = 0$ の解になっているので, 代数的数である. $\square$

参考文献

[M] S. Mayer, The transcendence of π, 2006
(http://sixthform.info/maths/files/pitrans.pdf)