1　eが超越数であることの証明

補題 1.1 (Hermite の不等式).　実係数の多項式

$$f(X) = \sum_{n=0}^{m} \frac{a_n}{n!} X^n$$

に対して

$$F(X) = \sum_{n=0}^{m} f^{(n)}(X), \qquad \overline{f}(X) = \sum_{n=0}^{m} \frac{|a_n|}{n!} |X|^n$$

とおく．このとき，任意の実数 x に対して

$$|F(x) - F(0)e^x| \leq |x| e^{|x|} \overline{f}(x)$$

が成り立つ．

証明.

$$\begin{aligned}
F(0) &= a_0 + a_1 + a_2 + \cdots + a_m, \\
F(X) &= \sum_{r=0}^{m} f^{(r)}(X) \\
&= \sum_{r=0}^{m} \sum_{n=r}^{m} \frac{a_n}{(n-r)!} X^{n-r} \\
&= \sum_{n=0}^{m} \sum_{r=0}^{n} \frac{a_n}{(n-r)!} X^{n-r} \\
&= \sum_{n=0}^{m} a_n \sum_{r=0}^{n} \frac{X^r}{r!}
\end{aligned}$$

ゆえに

$$\begin{aligned}
|F(x) - e^x F(0)| &= \left| \sum_{n=0}^{m} a_n \sum_{r=n+1}^{\infty} \frac{x^r}{r!} \right| \\
&\leq \sum_{n=0}^{m} |a_n| \sum_{r=n+1}^{\infty} \frac{|x|^r}{r!} \\
&= \sum_{n=0}^{m} \frac{|a_n||x|^{n+1}}{n!} \sum_{r=0}^{\infty} \frac{|x|^r}{(n+1)\cdots(n+r+1)} \\
&\leq \sum_{n=0}^{m} \frac{|a_n||x|^{n+1}}{n!} \sum_{r=0}^{\infty} \frac{|x|^r}{r!} \\
&= |x| e^{|x|} \overline{f}(x)
\end{aligned}$$

□

定理 1.2 (Hermite).　e は超越数である．

証明.　仮に e が代数的数であるとして矛盾が生じることを示す．いま

(1) $$a_0 + a_1 e + a_2 e^2 + \cdots + a_n e^n = 0, \qquad a_0 a_n \neq 0$$

を満たす整数 $a_0, a_1, a_2, \ldots, a_n$ が存在したとする．

素数 p として $n, |a_0|$ よりも大きいものをとり，$f(X)$ を次のように定める：

$$f(x) = \frac{1}{(p-1)!} X^{p-1}(X-1)^p \cdots (X-n)^p \tag{2}$$

$F(X), \overline{f}(X)$ を補題 1.1 で述べたとおりとし，$S = \sum_{r=0}^{n} a_r F(r)$ とおく．関係式 (1) より

$$S = \sum_{r=0}^{n} a_r (F(r) - e^r F(0))$$

であるから，Hermite の不等式を用いると

$$|S| \leq \sum_{r=0}^{n} |a_r| r e^r \overline{f}(r) \leq n e^n \overline{f}(n) \sum_{r=0}^{n} |a_r|$$

である．一方

$$\overline{f}(n) \leq \frac{1}{(p-1)!} n^{p-1}(n+1)^p \cdots (2n)^p = \frac{1}{n(p-1)!} \left(\frac{(2n)!}{(n-1)!} \right)^p \tag{3}$$

正の実数 a に対して $a^p/p! \to 0$ $(p \to \infty)$ であるから，(3) の右辺は p を大きくとればいくらでも小さくできる．ゆえに，大きな素数 p を 1 つとって

$$|S| < 1 \tag{4}$$

が成り立つようにできる．

次に，(2) を展開すると

$$\begin{aligned} f(X) &= \frac{1}{(p-1)!}(b_0 X^{p-1} + b_1 X^p + b_2 X^{p+1} + \cdots + b_{np} X^{(n+1)p-1}) \\ &= \frac{1}{(p-1)!}\left(c_{0,r}(X-r)^p + c_{1,r}(X-r)^{p+1} + \cdots + c_{np-1,r}(X-r)^{(n+1)p-1}\right) \end{aligned}$$

なる形に展開できる．ただし $r = 1, 2, \ldots, n$ であり，$b_i, c_{j,r}$ は整数である．このとき

$$\begin{aligned} &f(0) = f'(0) = \cdots = f^{(p-2)}(0) = 0, \\ &f^{(p-1)}(0) = b_0, \\ &f^{(i)}(0) \equiv 0 \pmod{p} \qquad (i \geq p), \\ &f(r) = f'(r) = \cdots = f^{(p-1)}(r) = 0, \\ &f^{(j)}(r) \equiv 0 \pmod{p} \qquad (j \geq p) \end{aligned}$$

となる．ゆえに

$$F(0) \equiv b_0 \pmod{p}, \qquad F(r) \equiv 0 \pmod{p}$$

したがって S は整数であり，

$$|S| \equiv a_0 b_0 \pmod{p} \tag{5}$$

$b_0 = n!$ だから，素数 p の取り方より $a_0 b_0$ は p で割りきれない．ところが (4) より S は 0 でなければならない．これは矛盾である．

したがって e は超越数でなければならない． □