Transcendence of e and π

$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ is an algebraic number}\} = \{\alpha \in \mathbb{C} \mid \exists\, f \in \mathbb{Q}[X] \setminus \{0\} \;\; f(\alpha) = 0\}$

Thm 1 (Hermite, 1873) $e \notin \overline{\mathbb{Q}}$.

Thm 2 (Lindemann, 1882) $\pi \notin \overline{\mathbb{Q}}$ (more generally, $0 \neq \alpha \in \overline{\mathbb{Q}} \Rightarrow e^{\alpha} \notin \overline{\mathbb{Q}}$).

Cor. It is impossible to "square the circle". [$e^{\pi i} = -1 \in \mathbb{Q}$]

Thm 3 (stated by Lindemann; details worked out by Weierstrass, 1885).

If $\alpha_1, \dots, \alpha_n \in \overline{\mathbb{Q}}$ distinct, $\beta_1, \dots, \beta_n \in \overline{\mathbb{Q}} \setminus \{0\} \Rightarrow \beta_1 e^{\alpha_1} + \cdots + \beta_n e^{\alpha_n} \neq 0$.

The proofs below are due to Hilbert (1893), who significantly simplified Hermite's arguments.

Basic formulas: $\forall k \in \mathbb{N}$ (a) $\int_0^{\infty} t^k e^{-t}\,dt = k! \Rightarrow$

(b) $\forall f \in t^k \mathbb{Z}[t]$ $\quad \int_0^{\infty} f(t) e^{-t}\,dt \in \mathbb{Z} \cdot k!$, $\quad \frac{1}{k!} \int_0^{\infty} f(t) e^{-t}\,dt \equiv \left(\frac{f}{t^k}\right)(0) \pmod{(k+1)}$.

Pf of Thm 1. Let $a_0, \dots, a_n \in \mathbb{Z}$ $(n \geq 1)$, $a_0 \neq 0$. We want to show that $S = \sum_{j=0}^{n} a_j e^j \overset{?}{\neq} 0$. For any $f \in \mathbb{C}[t]$,

$$S \int_0^{\infty} f(t) e^{-t}\,dt = \sum_{j=0}^{n} a_j e^j \left(\int_j^{\infty} + \int_0^{j} \right) = \sum_{j=0}^{n} \left(a_j \int_0^{\infty} f(t+j) e^{-t}\,dt + a_j e^j \int_0^{j} f(t) e^{-t}\,dt \right) =$$

$$= \underbrace{\int_0^{\infty} \underbrace{\left(\sum_{j=0}^{n} a_j f(t+j) \right)}_{g(t)} e^{-t}\,dt}_{S_1} + \underbrace{\sum_{j=0}^{n} a_j e^j \int_0^{j} f(t) e^{-t}\,dt}_{S_2}$$

Goal: choose $f \in \mathbb{Z}[t]$ so that (1) $g(t) \in t^m \mathbb{Z}[t]$ $(m \gg 0)$ $(\Rightarrow S_1/m! \in \mathbb{Z})$; (2) $S_1/m! \neq 0$; (3) $|S_2/m!| < 1$.

(1),(2) $\Rightarrow$ $|S_1/m!| \geq 1$ $\overset{(3)}{\Rightarrow}$ $S_1 + S_2 \neq 0 \Rightarrow S \neq 0$.

Take $f(t) = t^m \prod_{j=1}^{n} (t-j)^{m+1}$ $(m \geq 1)$. Then $g(t) \in t^m \mathbb{Z}[t]$

$\overset{(b)}{\Rightarrow}$ $\underbrace{S_1/m! \in \mathbb{Z}}_{(1)}$ and (by (c)) $S_1/m! \equiv \left(\frac{g}{t^m}\right)(0) = a_0 \left((-1)^n n!\right)^{m+1} \pmod{(m+1)}$

$\neq 0 \pmod{(m+1)}$ if $m \gg 0$.

$\Rightarrow$ (2)

Finally, $\sup_{t \in [0,n]} |f(t)| \leq c_1 \cdot c_2^m \Rightarrow |S_2| \leq c_3 \cdot c_4^m \Rightarrow \left|\frac{S_2}{m!}\right| < 1$ if $m \gg 0$

(3).

Proof of $\pi \notin \overline{\mathbb{Q}}$: if $\pi \in \overline{\mathbb{Q}}$, so is $\alpha_1 = i\pi \in \overline{\mathbb{Q}}$, hence $\exists\, g \equiv (X-\alpha_1)\cdots(X-\alpha_d) \in \mathbb{Q}[X]$

$0 = 1 + e^{i\pi} = 1 + e^{\alpha_1} \Rightarrow 0 = (1+e^{\alpha_1})\cdots(1+e^{\alpha_d}) = 1 + \sum_{k=1}^{d} \sum_{|J|=k} e^{\alpha_J}$, $J \subset \{1,\dots,d\}$, $\alpha_J = \sum_{j\in J} \alpha_j$

Theorem on symmetric functions $\Rightarrow \prod_{|J|=k} (X - \alpha_J) \in \mathbb{Q}[X]$.

Putting together the terms 1 and e^{α_J} for $\alpha_J = 0$, we obtain a relation

$0 = a + \sum_{\ell=1}^{n} e^{\beta_\ell}$, $0 < a \in \mathbb{Z}$, $h(X) = b \prod_{\ell=1}^{n} (X - \beta_\ell) \in \mathbb{Z}[X]$, $h(0) \neq 0$

So it remains to prove (the case $N=1$ of) the following:

Proposition 1. If $a_0 \in \mathbb{Z}\setminus\{0\}$, $a_1, \dots, a_N \in \mathbb{Z}$, $h_1, \dots, h_N(X) \in \mathbb{Z}[x]$, $(h_1 \cdots h_N)(0) \neq 0$,

then $S = a_0 + \sum_{k=1}^{N} a_k \sum_{h_k(\beta)=0} e^{\beta} \neq 0$. (taking all roots β with multiplicities)

Pf of Proposition 1: $\forall\, f \in \mathbb{C}[t]$

$$S \int_0^\infty f(t) e^{-t}\,dt = \underbrace{a_0 \int_0^\infty f(t) e^{-t}\,dt}_{S_1} + \underbrace{\int_0^\infty \Big(\underbrace{\sum_{k=1}^{N} a_k \sum_{h_k(\beta)=0} f(t+\beta)}_{g(t)} \Big) e^{-t}\,dt}_{S_2} + \underbrace{\sum_{k=1}^{N} a_k \sum_{h_k(\beta)=0} \int_0^\beta f(t) e^{-t}\,dt}_{S_3}$$

Take $f = t^m (h_1 \cdots h_N)^{m+1}$, for $m \gg 0$:

(a) $f \in t^m \mathbb{Z}[t]$, $(f/t^m)(0) = (h_1 \cdots h_N)(0)^{m+1} = b^{m+1}$, $b \in \mathbb{Z}\setminus\{0\}$

$\Rightarrow S_1 \in \mathbb{Z} m!$, $S_1/m! = a_0 b^{m+1} \pmod{(m+1)} \not\equiv 0 \pmod{(m+1)}$ for $m \gg 0$

(b) $g \in t^{m+1}\mathbb{Z}[t] \Rightarrow S_2 \in \mathbb{Z}(m+1)!$

So $\|(S_1+S_2)/m!\| \in \mathbb{Z}\setminus\{0\}$, $|(S_1+S_2)/m!| \geq 1$ for $m \gg 0$

(c) $|S_3| \leq c_1 \cdot c_2^m \Rightarrow |S_3/m!| < 1$ for $m \gg 0$

$\Rightarrow S_1 + S_2 + S_3 \neq 0 \Rightarrow S \neq 0$.

Pf of Thm 3: if $\beta_1, \dots, \beta_n \in \overline{\mathbb{Q}}$ are distinct, $\alpha_1, \dots, \alpha_n \in \overline{\mathbb{Q}}\setminus\{0\} \Rightarrow \sum_{j=1}^{n} \alpha_j e^{\beta_j} \neq 0$.

Hilbert wrote that the above arguments work in this case, but gave no details. We show how to deduce Thm 3 from the above Proposition 1 (which was proved by Hilbert in the case $N=1$). Assume that $\sum_{j=1}^{n} \alpha_j e^{\beta_j} = 0$.

Step 1: reduction to the case $\forall j\ \alpha_j \in \mathbb{Q}\setminus\{0\}$.

$\forall j=1,\dots,n \quad \exists f_j(X)=\prod_{k=1}^{d_j}(X-\alpha_{j,k}) \in \mathbb{Q}[X]$, $f_j(\alpha_j)=0$, $\alpha_{j,1}=\alpha_j$

We have $0=\prod_{\underline{k}}\left(\sum_{j=1}^{n}\alpha_{j,k_j}e^{\beta_j}\right)=\sum_{\ell}\alpha'_\ell e^{\beta'_\ell}$, $\beta'_\ell\in\overline{\mathbb{Q}}$ distinct

$\underline{k}=(k_1,\dots,k_n)$, $1\le k_j\le d_j$

Each α'_ℓ = polynomial (with coeff. in $\mathbb{Z}$) in $\{\alpha_{j,k}\}$, symmetric under the permutations of $\{\alpha_{j,1},\dots,\alpha_{j,d_j}\}$ $\forall j$
$\Downarrow$ (thm on symmetric functions)

α'_ℓ = " " in {the coefficients of $f_1,\dots,f_n$}

$\Rightarrow \alpha'_\ell\in\mathbb{Q}$. Moreover, $\alpha'_\ell\neq 0$ for some ℓ: put a lexicographic order on $\mathbb{C}$: $z\le w \iff \begin{cases}\mathrm{Re}(z)<\mathrm{Re}(w)\\ \text{OR}\\ \mathrm{Re}(z)=\mathrm{Re}(w),\ \mathrm{Im}(z)\le\mathrm{Im}(w)\end{cases}$; if β_n is maximal among $\{\beta_1,\dots,\beta_n\}$ with respect to this order, then $e^{\beta'_\ell}$ for $\beta'_\ell=d_1\cdots d_n\beta_n$ will appear with coefficient $\alpha'_\ell=\prod_{j=1}^{n}\prod_{k_j=1}^{d_j}\alpha_{n,k_j}\neq 0$.

Step 2: reduction to a relation of the form

$$(*)\qquad \sum_{\ell=1}^{N} a_\ell \sum_{h_\ell(\beta)=0} e^{\beta}=0,\qquad N\ge 1;\ a_1,\dots,a_N\in\mathbb{Z}\setminus\{0\},\ \underbrace{h_1,\dots,h_N}_{\text{distinct monic irreducible polynomials (in }\mathbb{Q}[X]\text{)}}\in\mathbb{Q}[X]$$

By Step 1, we can assume that $\sum_{j=1}^{n}\alpha_j e^{\beta_j}=0$, $\forall j\ \alpha_j\in\mathbb{Q}\setminus\{0\}$ ($\Rightarrow \alpha_j\in\mathbb{Z}\setminus\{0\}$), after multiplying the relation by a suitable integer, $\{\beta_j\}$ distinct.

$\forall j=1,\dots,n \quad \exists g_j(X)=\prod_{k=1}^{d'_j}(X-\beta_{j,k})\in\mathbb{Q}[X]$, $g_j(\beta_j)=0$, $\beta_{j,1}=\beta_j$

We have $0=\prod_{\underline{k}}\left(\sum_{j=1}^{n}\alpha_j e^{\beta_{j,k_j}}\right)=\sum_{\underline{j}}A_{\underline{j}}e^{B_{\underline{j}}}=\sum_{\underline{m}}\underline{\alpha}^{\underline{m}}\sum_{\underline{j},\ \underline{m}(\underline{j})=\underline{m}}e^{B_{\underline{j}}}$,

where $\underline{j}:\{1,\dots,d'_1\}\times\cdots\times\{1,\dots,d'_n\}\longrightarrow\{1,\dots,n\}$,

$\underline{k}=(k_1,\dots,k_n)$, $1\le k_j\le d'_j$, $B_{\underline{j}}=\sum_{\underline{k}}\beta_{\underline{j}(\underline{k}),\,\underline{k}(\underline{k})}$,

$A_{\underline{j}}=\prod_{\underline{k}}\alpha_{\underline{j}(\underline{k})}=\prod_{i=1}^{n}\alpha_i^{m_i(\underline{j})}$, $m_i(\underline{j})=|\underline{j}^{-1}(i)|$, $\underline{m}=(m_1,\dots,m_n)$, $m_1+\cdots+m_n=d'_1\cdots d'_n$,

$\underline{\alpha}^{\underline{m}}=\alpha_1^{m_1}\cdots\alpha_n^{m_n}$

For fixed $\underline{m}$, each coefficient of $F_{\underline{m}}(X) = \prod_{\underline{j},\, \underline{m}(\underline{j})=\underline{m}} (X - B_{\underline{j}})$ $\left(B_{\underline{j}} = \sum_{\underline{k}} \beta_{\underline{j}(\underline{k}),\, \underline{k}_{\underline{j}(\underline{k})}}\right.$

is a polynomial (with coeff. in $\mathbb{Z}$) in $\{\beta_{j,k}\}$, invariant under the permutations of $\{\beta_{j,1}, \dots, \beta_{j,d_j'}\}$ (for all $j=1,\dots,n$)

$\Downarrow$ thm on symmetric functions

$F_{\underline{m}}(X) \in \mathbb{Q}[X]$ and $0 = \sum_{\underline{m}} \sum_{F_{\underline{m}}(\beta)=0} e^{\beta} = 0$ $\left(\alpha^{\underline{m}}\right)$ (counting each β with multiplicity)

Writing each $F_{\underline{m}}$ as a product of powers of irreducible polynomials and redistributing the terms, we obtain a relation of the form (*) ($a_1 \neq 0$, by considering the largest terms, with respect to the lexicographic order of $\mathbb{C}$, of each set of exponents $\{\beta_{1,k_1}, \dots, \beta_{n,k_n}\}$ in $\sum_{j=1}^{n} \alpha_j e^{\beta_{j,k_j}}$).

Step 3: reduction to Proposition 1.

If the polynomials h_j in (*) satisfy $(h_1 \cdots h_N)(0) = 0$, then $h_j(X) = X$ for some j and (*) contradicts Proposition 1.

If $(h_1 \cdots h_N)(0) \neq 0$, after multiplying (*) by $\sum_{h_1(\beta)=0} e^{-\beta}$

we obtain a new relation of the form (*), this time with $(h_1 \cdots h_N)(0) = 0$, and we conclude as before.
