6 The Transcendence of e and π

For this section and the next, we will make use of

$$I(t) = \int_0^t e^{t-u} f(u)\, du,$$

where t is a complex number and $f(x)$ is a polynomial with complex coefficients to be specified later (depending on the application). Integration by parts gives

$$I(t) = e^t \sum_{j=0}^{\infty} f^{(j)}(0) - \sum_{j=0}^{\infty} f^{(j)}(t) = e^t \sum_{j=0}^{n} f^{(j)}(0) - \sum_{j=0}^{n} f^{(j)}(t), \tag{8}$$

where n is the degree of $f(x)$. If $f(x) = \sum_{j=0}^{n} a_j x^j$, we set

$$\overline{f}(x) = \sum_{j=0}^{n} |a_j| x^j.$$

Then

$$|I(t)| \leq \left| \int_0^t |e^{t-u} f(u)|\, du \right| \leq |t| \max\{|e^{t-u}|\} \max\{|f(u)|\} \leq |t| e^{|t|} \overline{f}(|t|).$$

Theorem 16. *The number e is transcendental.*

Proof. Assume e is a root of

$$g(x) = b_0 + b_1 x + \cdots + b_r x^r \in \mathbb{Z}[x],$$

where $b_0 \neq 0$. Let p be a prime $> \max\{r, |b_0|\}$, and define

$$f(x) = x^{p-1}(x-1)^p(x-2)^p \cdots (x-r)^p.$$

Consider

$$J = b_0 I(0) + b_1 I(1) + \cdots + b_r I(r).$$

Since $g(e) = 0$, the contribution of the first summand on the right-hand side of (8) to J is 0. Thus,

$$J = -\sum_{k=0}^{r} \sum_{j=0}^{n} b_k f^{(j)}(k),$$

where $n = (r+1)p - 1$. The definition of $f(x)$ implies that many of the terms above are zero, and we can write

$$J = -\sum_{j=p-1}^{n} b_0 f^{(j)}(0) + \sum_{k=1}^{r} \sum_{j=p}^{n} b_k f^{(j)}(k).$$

Each of the terms on the right is divisible by $p!$ except for

$$f^{p-1}(0) = (p-1)!(-1)^{rp}(r!)^p,$$

where we have used that $p > r$. Thus, since $p > |b_0|$ as well, we see that J is an integer which is divisible by $(p-1)!$ but not by p. In other words, J is an integer with

$$|J| \geq (p-1)!.$$

Since

$$\overline{f}(k) = k^{p-1}(k+1)^p(k+2)^p \cdots (k+r)^p \leq (2r)^n \quad \text{for } 0 \leq k \leq r,$$

we deduce that

$$|J| \leq \sum_{j=0}^{r} |b_j||I(j)| \leq \sum_{j=0}^{r} |b_j| j e^j \overline{f}(j) \leq c\left((2r)^{(r+1)}\right)^p,$$

where c is a constant independent of p. This gives a contradiction and establishes the theorem. $\square$

It helps to be aware of the following lemmas.

Lemma 1. *If α and β are algebraic numbers, then so are $\alpha \pm \beta$, $\alpha\beta$, and α/β (if $\beta \neq 0$). If α and β are algebraic integers, then so are $\alpha \pm \beta$ and $\alpha\beta$.*

Lemma 2. *If α is an algebraic number with minimum polynomial $g(x) \in \mathbb{Z}[x]$ and if b is the leading coefficient of $g(x)$, then $b\alpha$ is an algebraic integer.*

Lemma 3. *If α is an algebraic integer and α is rational, then α is a rational integer.*

In addition, it would be helpful to be familiar with the fundamental theorem of elementary symmetric functions.

Theorem 17. *The number π is transcendental.*

Proof. Observe that if π were algebraic, then $i\pi$ would be as well (which we can see by using Lemma 1 or by observing that if $f(x) \in \mathbb{Z}[x]$ and $f(\pi) = 0$, then $g(x) = f(ix)f(-ix) \in \mathbb{Z}[x]$ and $g(i\pi) = 0$). It suffices therefore to show that $\theta = i\pi$ is transcendental. Assume otherwise. Let r be the degree of the minimal polynomial $g(x)$ for θ, and let $\theta_1 = \theta, \theta_2, \ldots, \theta_r$ denote the conjugates of θ. Let b denote the leading coefficient of $g(x)$. In particular, we will use momentarily that $b\theta_j$ is an algebraic integer (see Lemma 2). Since $e^{i\pi} = -1$, we deduce that

$$(1 + e^{\theta_1})(1 + e^{\theta_2}) \cdots (1 + e^{\theta_r}) = 0.$$

Multiplying the above expression on the left out, we obtain a sum of 2^r terms of the form e^{ϕ} where $\phi = \epsilon_1\theta_1 + \cdots + \epsilon_r\theta_r$ with $\epsilon_j \in \{0, 1\}$ for all j. Let $\phi_1, \ldots, \phi_n$ denote the non-zero expressions of this form so that (since the remaining $2^r - n$ values of ϕ are 0)

$$q + e^{\phi_1} + \cdots + e^{\phi_n} = 0,$$

where $q = 2^r - n$. Let p be a large prime, and let

$$f(x) = b^{np}x^{p-1}(x - \phi_1)^p \cdots (x - \phi_n)^p.$$

By the fundamental theorem of elementary symmetric functions and Lemma 2 and Lemma 3, $f(x) \in \mathbb{Z}[x]$; to see this more clearly, consider $\phi_1, \ldots, \phi_{2^r}$ as the complete set of ϕ's as above (so the first n are still the non-zero ones) and use that

$$\prod_{j=1}^{2^r}(x - \phi_j) = x^{2^r - n}\prod_{j=1}^{n}(x - \phi_j)$$

is symmetric in $\theta_1, \ldots, \theta_r$. Define

$$J = I(\phi_1) + \cdots + I(\phi_n).$$

From (8), we deduce that

$$J = -q\sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m}\sum_{k=1}^{n} f^{(j)}(\phi_k)$$

where $m = (n+1)p - 1$. Observe that the sum over k is a symmetric polynomial in $b\phi_1, \ldots, b\phi_n$ with integer coefficients and thus a symmetric polynomial with integer coefficients in the 2^r numbers $b\phi = b(\epsilon_1\theta_1 + \cdots + \epsilon_r\theta_r)$. Hence, by the fundamental theorem of elementary symmetric functions, we obtain that this sum is a rational number. Observe that Lemma 2 and Lemma 3 imply that the sum is furthermore a rational integer. Since $f^{(j)}(\phi_k) = 0$ for $j < p$, we deduce that the double sum in the expression for J above is a rational integer divisible by $p!$. Observe that $f^{(j)}(0) = 0$ for $j < p - 1$ and $f^{(j)}(0)$ is divisible by $p!$ for $j \geq p$. Also,

$$f^{(p-1)}(0) = b^{np}(-1)^{np}(p-1)!(\phi_1 \cdots \phi_n)^p.$$

From the fundamental theorem of elementary symmetric functions and Lemma 2 and Lemma 3, we deduce that $f^{(p-1)}(0)$ is a rational integer divisible by $(p-1)!$. Furthermore, if p is sufficiently large, then $f^{(p-1)}(0)$ is not divisible by p. If p is also $> q$, we deduce that

$$|J| \geq (p-1)!.$$

On the other hand, using the upper bound we obtained for $|I(t)|$, we have

$$|J| \leq \sum_{k=1}^{n} |\phi_k| e^{|\phi_k|}\overline{f}(|\phi_k|) \leq c_1 c_2^p$$

for some constants c_1 and c_2. We get a contradiction, completing the proof. $\square$