Chapter Two
The transcendence of e and π.

The fantasy calculation at the end of the last lecture, a fantasy because the linear combination of the intermediate series I_n did not vanish (it is a positive rational number), does give us a goal to pursue: find a series representation for e^z that provides better-than-expected approximations to particular values of e^z. And the hope that it *might* be possible to manipulate the power series for e^z so that when it is divided into a main term, intermediate term, and tail, a linear combination of the intermediate terms vanishes, can be realized. We just need to rethink what we expect of an approximating main term for such a series.

One way to think about the failure of the simple truncation of the power series for e^z idea to establish the transcendence of e is that we are expecting too much of the series–we are hoping that the truncated series, which leads to the main term which is a polynomial approximation to e^z, will lead to very good approximations for all values e^n. But we only need good approximations for a few values, rather than *all* values, and we want that approximation to be a very good one. To accomplish this we do not need the intermediate sum to vanish for all values of z but only for those values for which we wish to have good approximations to e^z. This puts us, and Hermite and others, on a new quest: find a polynomial that offers very good approximations of the values under consideration but not particularly good approximations to other values. In particular, we want to find a polynomial that provides a good approximation to e^z at a point $z = a$, but is not necessarily any better than the previous truncation attempt for other values of z. And, in the proof of the transcendence of e we find approximations for each of the powers of e that appears in the assumed nontrivial integral, algebraic equation

$$r_0 + r_1 e + r_2 e^2 + \cdots + r_d e^d = 0, r_d \neq 0.$$

Perhaps surprisingly, this can be accomplished by taking an appropriate integer multiple of the function e^z, which we will see is best thought of as a linear combination of exponential functions. The idea is to take integral combinations of e^z so that the appropriately chosen intermediate term vanishes at each of the values $z = 0, 1, \ldots, d$.

If we want the intermediate sum to vanish at the values $z = 0, 1, \ldots, d$, the obvious thing to try is to manipulate the power series for e^z so that the intermediate sum is divisible by each of the polynomials $z, z-1, z-2, \ldots, z-d$. Having the intermediate sum divisible by the product $z(z-1)(z-2)\cdots(z-d)$ does not suffice, for reasons we will point out later. The source of the correct integer coefficients is the polynomial:

$$P(z) = z^{p-1}(z-1)^p \cdots (z-d)^p. \tag{1}$$

The exponent p will be taken to be a sufficiently large prime number in the proof. For now we just point out that $P(z)$ has a zero of order $p-1$ at $z = 0$ and of order p at each of $z = 1, \ldots, d$; the higher order of vanishing at $z = 1, \ldots, d$, together with the requirement that p be a prime number, will play a role in showing that the *small* integer we obtain is nonzero.

The point of the above discussion is that we have not only the single polynomial $P(z)$ that vanishes at each of the points $z = 0, 1, \ldots, d$ but so do each of the polynomials $P^{(n)}(z)$ for $1 \le n \le p-1$. The reason these derivatives are important is because they introduce factorials into our proof, and we saw in our fantasy calculations in the previous chapter that factorials could play a major role.

If we rewrite the polynomial $P(z)$ as

$$P(z) = c_{p-1}z^{p-1} + c_p z^p + \cdots + c_{(d+1)p-1}z^{(d+1)p-1}, \tag{2}$$

and then sum Ps first through $(p-1)$st derivatives, we obtain the sum:

$$\sum_{n=1}^{p-1} P^{(n)}(z) = \sum_{N=p-1}^{(d+1)p-1} \left(N!c_N \sum_{n=N-p+1}^{N-1} \frac{z^n}{n!} \right) . \tag{3}$$

Notice that the right-hand side of this expression equals a sum of terms of the form $N!c_N$ times a portion of the power series for e^z, where the index of the sum, N, runs from $p-1$ to $(d+1)p-1$. This means that we have uncovered a linear combination of the series representation of e^z that has the desired vanishing intermediate sum:

$$\sum_{N=p-1}^{(d+1)p-1} N!c_N e^z =$$
$$\underbrace{\sum_{N=p-1}^{(d+1)p-1} \left(N!c_N \sum_{n=0}^{N-p} \frac{z^n}{n!} \right)}_{\text{main term } (M_p(z))} + \underbrace{\sum_{N=p-1}^{(d+1)p-1} \left(N!c_N \sum_{n=N-p+1}^{N-1} \frac{z^n}{n!} \right)}_{\text{intermediate term } (I_p(z))} + \underbrace{\sum_{N=p-1}^{(d+1)p-1} \left(N!c_N \sum_{n=N}^{\infty} \frac{z^n}{n!} \right)}_{\text{tail } (T_p(z))},$$

provided that we use the convention that an *empty* sum equals 0 (this occurs in the main term when $N = p-1$). As this last point is so important to the proof of the transcendence of e we offer below we make explicit the main terms as:

$$M_p(z) = \sum_{N=p}^{(d+1)p-1} \left(N!c_N \sum_{n=0}^{N-p} \frac{z^n}{n!} \right).$$

By construction we know that the intermediate term vanishes for $t = 1, 2, \ldots, d$; so for each of these values we have

$$e^t \sum_{N=p-1}^{(d+1)p-1} N!c_N = M_p(t) + T_p(t).$$

On the other hand, when $t = 0$ the intermediate term does not vanish, since the polynomial $P(z)$ only has order of vanishing $p-1$ at $t = 0$. However the tail series clearly vanishes at $t = 0$ so, for $t = 0$, we have the representation:

$$e^0 \sum_{N=p-1}^{(d+1)p-1} N! c_N = M_p(0) + I(0) \ .$$

The above representations for e^t when $t = 0, 1, \ldots, d$ are the technical tools we need to establish the transcendence of e.

Theorem. *The number e is transcendental.*

Proof. We begin by again assuming that e is algebraic and so there exist integers $r_0, r_1, \ldots, r_d$, $r_d \neq 0$, such that

$$r_0 + r_1 e + r_2 e^2 + \cdots + r_d e^d = 0 \ . \tag{4}$$

Step 1. When we multiply the equation $r_0 + r_1 e + r_2 e^2 + \cdots + r_d e^d = 0$ by $N! c_N$ and sum from $N = p - 1$ to $(d+1)p - 1$ we obtain

$$r_0 \sum_{N=p-1}^{(d+1)p-1} N! c_N + r_1 e^1 \sum_{N=p-1}^{(d+1)p-1} N! c_N + \cdots + r_d e^d \sum_{N=p-1}^{(d+1)p-1} N! c_N = 0 \tag{5}$$

We recall the representations from above:

$$e^t \sum_{N=p-1}^{(d+1)p-1} N! c_N = M_p(t) + T_p(t), \text{for } 1 \le t \le d,$$

$$\text{and, } e^0 \sum_{N=p-1}^{(d+1)p-1} N! c_N = M_p(0) + I_p(0). \tag{6}$$

We substitute these relationships into the presumed vanishing algebraic relationship (4), and rearranging, we have a familiar expression:

$$r_0\big(M_p(0)+I_p(0)\big)+r_1 M_p(1)+r_2 M_p(2)+\cdots+r_d M_p(d) = -r_1 T_p(1)-r_2 T_p(2)-\cdots-r_d T_p(d) \ ,$$

and therefore

$$\begin{aligned} \big|r_0\big(M_p(0) + I_p(0)\big) &+ r_1 M_p(1) + r_2 M_p(2) + \cdots + r_d M_p(d)\big| \\ &\le |r_1||T_p(1)| + |r_2||T_p(2)| + \cdots + |r_d||T_p(d)| \ , \end{aligned} \tag{7}$$

Step 2. In Step 3 we will show that the expression on the left-hand side of the above equation is a nonzero integer, and, moreover, that it is divisible by the relatively large integer $(p-1)!$. This is the amazing part of the proof. Before getting there we complete one of the more mundane parts of the proof, we provide an upper bound for the right-hand side of (8). Our estimate will, after we complete Step 3, show that (8) is an equality between a nonzero, positive integer and a number less than 1.

We begin our estimate for the absolute value of the right-hand side of (8) by estimating each of the terms $|T_p(t)|$. For $t = 1, 2, \ldots, d$,

$$T_p(t) = \sum_{N=p-1}^{(d+1)p-1} \left(N! c_N \sum_{n=N}^{\infty} \frac{t^n}{n!} \right);$$

the simple change of variables $k = n - N$, and the observation that $\frac{(k+N)!}{k!N!} \geq 1$, yields,

$$N! \sum_{n=N}^{\infty} \frac{t^n}{n!} = \sum_{k=0}^{\infty} \frac{N!}{(k+N)!} t^{k+N} \leq t^N \sum_{k=0}^{\infty} \frac{t^k}{k!} = t^N e^t,$$

It follows from the triangle inequality that

$$|T_p(t)| \leq e^t t^{(d+1)p-1} \sum_{N=p-1}^{(d+1)p-1} |c_N| \; .$$

We next provide an upper bound for the sum $\displaystyle\sum_{N=p-1}^{(d+1)p-1} |c_N|$. To do this we first recall that $z^{p-1}(z-1)^p(z-2)^p \cdots (z-d)^p = \sum_{N=p-1}^{(d+1)p-1} c_N z^N$. So the $\sum_{N=p-1}^{(d+1)p-1} |c_N|$ may be bounded by a product of d terms each of which is a bound for the sum of the absolute values of the coefficients of the term $(z-t)^p$, for $t = 1, \ldots, d$. Since $(z-t)^p = \sum_{n=0}^{p} \binom{p}{n} (-t)^{p-n} z^n$, the sum of the absolute values of its coefficients is bounded by

$$\sum_{n=0}^{p} \left| \binom{p}{n} (-t)^{p-n} \right| \leq t^p \sum_{n=0}^{p} \binom{p}{n} = (2t)^p \; .$$

It follows that

$$\sum_{n=p-1}^{(d+1)p-1} |c_N| \leq \prod_{t=1}^{d} (2t)^p \leq \left((2d)^d\right)^p \; . \tag{8}$$

Since $1 \leq t \leq d$ we have

$$|T_p(t)| \leq e^d d^{(d+2)p-1} (2d)^{dp} \;\; = c_1 \, (c_2)^p$$

where the constants c_1 and c_2 are defined by $c_1 = e^d/d$ and $c_2 = d^2 \left(2d^2\right)^d$ depend only on e and its presumed algebraic degree which is at most d.

Thus we have established the following upper bound

$$\left| r_0 \big(M_p(0) + I_p(0) \big) + r_1 M_p(1) + r_2 M_p(2) + \cdots + r_d M_p(d) \right| \leq c_1 \left(\sum_{t=1}^{d} |r_t| \right) (c_2)^p \; . \tag{9}$$

Notice that we still have work to do because letting $p \to \infty$ the upper bound on the right-hand side of the above inequality (9) is unbounded. It will follow from what we called the amazing part of the proof, which we carry out in the next step, that it is possible to introduce a $(p-1)!$ into the denominator of the right-hand side of (9), and still have an integer on the inequality's left-hand side. This will allow us to obtain a contradiction as $p \to \infty$ and therefore conclude the e cannot be algebraic.

Step 3. We now come to the amazing part of the proof we have discussed: we establish that the integer in the left-hand side of (9) is nonzero and is divisible by $p-1$. Specifically we see that for all sufficiently large prime numbers p,

$$\frac{r_0}{(p-1)!} I_p(0) + \sum_{t=0}^{d} \frac{r_t}{(p-1)!} M_p(t)$$

is a *nonzero* integer.

We establish the above claim in two steps–we first show that the displayed value is an integer, which amounts to showing that $(p-1)!$ divides each term, and we then show that this integer is nonzero, by showing that it is not divisible by p. It will be handy for each of these demonstrations to have the expression for $M_p(t)$ in view so we recall it here:

$$M_p(t) = \sum_{N=p}^{(d+1)p-1} \left(N! c_N \sum_{n=0}^{N-p} \frac{t^n}{n!} \right) = \sum_{N=p}^{(d+1)p-1} \left(c_N \sum_{n=0}^{N-p} \frac{N!}{n!} t^n \right)$$

To establish the first part of the claim we begin by observing that $N \geq p$ and $n \leq (N-p)$. The ratio $\dfrac{N!}{n!(N-n)!}$ is an integer so $\dfrac{N!}{n!}$ is an integer that is divisible by $(N-n)!$. Combining this with $N-n \geq p$ yields the stronger than announced result that for each t, $M_p(t)$ is divisible by $p!$. However, from our choice of the polynomial $P(z)$ which led to our intermediate terms, we see that $I_p(0) = (p-1)! c_{p-1}$, which is clearly divisible by $(p-1)!$, thus establishing the first part of the claim.

The second part of the claim follows from the observation that $c_{p-1} \neq 0$, it equals $(-1)^d (d!)^p$, and therefore, if we take $p > d$ it will not divide c_{p-1}. Thus we have

$$\frac{I_p(0)}{(p-1)!} \equiv c_{p-1} \mod p \text{ and for each } t \quad \frac{M_p(t)}{(p-1)!} \equiv 0 \mod p,$$

With the above claim in hand it is possible to conclude the proof that e is transcendental.

If we divide the inequality (9) by $(p-1)!$ we have the inequality

$$0 < \left| \frac{r_0}{(p-1)!} I_p(0) + \sum_{t=0}^{d} \frac{r_t}{(p-1)!} M_p(t) \right| \leq c_1 \left(\sum_{t=1}^{d} |r_t| \right) \frac{(c_2)^p}{(p-1)!\ ,}. \qquad (10)$$

Letting p approach infinity leads to a contradiction, thus establishing the transcendence of e.

As we mentioned in Chapter 1, the above proof is more allied with the one given by Hurwitz in 1893 that with Hermite's original proof. Yet Hermite's proof of 1873 did inspire Lindemann, who just under a decade later established the important theorem:

Lindemann(1882) *π is transcendental.*

Lindemann actually proved a more general result that is now widely known as the Hermite-Lindemann Theorem.

Theorem (The Hermite-Lindemann Theorem). *If α is a nonzero algebraic number then e^α is transcendental.*

Note that the transcendence of π follows: if π is algebraic then so is $i\pi$. Thus it should follow that $e^{i\pi} = -1$ is transcendental, which is clearly is not.

Sketch of proof of the Hermite-Lindemann Theorem. Suppose α is a nonzero algebraic number and e^α is algebraic and satisfies an integral polynomial equation:

$$r_0 + r_1 e^\alpha + r_2 e^{2\alpha} + \cdots + r_d e^{d\alpha} = 0, r_d \neq 0.$$

Using the series representation we obtain:

$$\begin{aligned}\sum_{N=p}^{(d+1)p-1} N! c_N e^{\alpha z} &= \underbrace{\sum_{N=p}^{(d+1)p-1} \left(N! c_N \sum_{n=0}^{N-p} \frac{(\alpha z)^n}{n!} \right)}_{\text{main term } (M_p(\alpha z))} \\ &+ \underbrace{\sum_{N=p-1}^{(d+1)p-1} \left(N! c_N \sum_{n=N-p+1}^{N-1} \frac{(\alpha z)^n}{n!} \right)}_{\text{intermediate term } (I_p(\alpha z))} + \underbrace{\sum_{N=p-1}^{(d+1)p-1} \left(N! c_N \sum_{n=N}^{\infty} \frac{(\alpha z)^n}{n!} \right)}_{\text{tail } (T_p(\alpha z))}, \quad (11)\end{aligned}$$

where the coefficients c_N are chosen so that the intermediate term, $I_p(\alpha z)$, vanishes at $z = 1, 2, \ldots, d$.

Therefore we have for each $t, 1 \leq t \leq d$,

$$e^{t\alpha} \sum_{N=p}^{(d+1)p-1} N! c_N = M_p(t\alpha) + T_p(t\alpha),$$

while

$$e^0 \sum_{N=p}^{(d+1)p-1} N! c_N = M_p(0) + I_p(0).$$

This leads to

$$\underbrace{\Big|r_0\big(M_p(0)+I_p(0)\big)+r_1\big(M_p(\alpha)\big)+r_2\big(M_p(2\alpha)\big)+\cdots+r_d\big(M_p(d\alpha)\big)\Big|}_{\text{term that should lead to a nonzero integer}}$$
$$\leq \underbrace{\Big|r_1\big(T_p(\alpha)\big)+r_2\big(T_p(2\alpha)\big)+\cdots+r_d\big(T_p(d\alpha)\big)\Big|}_{\text{expression that should be small for } p \text{ large}}.$$

If we could somehow obtain an inequality of roughly the above form, and show the left-hand side is nonzero, we would still need to move from an inequality

$$0 < |\text{ algebraic number }| \leq \text{a small, positive quantity.}$$

to an inequality

$$0 < |\text{nonzero integer }| \leq \text{a small, positive quantity}$$

How to, in general, obtain a rational integer from an algebraic number, is perhaps the only new idea Lindemann had to introduce. We will come back to this outline of the proof of what is often called the Hermite-Lindemann Theorem after we investigate this point.

Algebraic Digression: Obtaining an integer from an algebraic number

Suppose that α is the zero of an irreducible, integral polynomial $P_\alpha(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_d \neq 0$. If we denote the d zeros of $P(x)$ by $\alpha_1(=\alpha), \alpha_2, \ldots, \alpha_d$ then we have the factorization:

$$P(x) = a_d \prod_{k=1,\ldots,d} \big(x-\alpha_k\big).$$

The algebraic numbers $\alpha_2, \ldots, \alpha_d$ are called the *conjugates* of α and the algebraic norm of α, defined by the product

$$Norm(\alpha) = \prod_{k=1,\ldots,d} \alpha_k$$

is equal to the ratio $(a_0)/(a_d)$. Thus for any nonzero algebraic number $\alpha, Norm(\alpha)$ is a rational number.

In the particular case that the minimal integral polynomial of α is *monic*, so that its leading coefficient equals 1 (in which case α is said to be an algebraic integer), we see that $Norm(\alpha)$ is a nonzero integer (namely the constant term of α's minimal, integral polynomial).

It is elementary, and central to transcendence theory, that for any algebraic number α there exists a rational integer δ so that $\delta\alpha$ is an algebraic integer. Any such δ is said to be a denominator for α and if the minimal, integral polynomial for α is the polynomial $P(x)$, as above, then $a_d\alpha$ is an algebraic integer. (It is a zero of the polynomial $Q(x) = x^d + a_{d-1}x^{d-1} + a_d a_{d-2}x^{d-2} + \cdots + a_d^{d-1}a_0$ since $Q(a_d\alpha) = a_d^{d-1}P(\alpha) = 0$.)

The Hermite-Lindemann's Theorem's proof (continued).

Assuming e^α is algebraic it is possible to obtain an inequality:

$$0 < |\text{ algebraic number }| \leq \text{a small, positive quantity.}$$

If we then multiply through by the denominator of the algebraic number in the above inequality we get:

$$\begin{aligned} 0 &< |\text{ denominator of the algebraic number} \times \text{algebraic number }| \\ &\leq |\text{ denominator of the algebraic number}| \times \text{a small, positive quantity.} \end{aligned}$$

Assuming we have a reasonable estimate for the absolute value of the denominator we have just multiplied by we then have

$$0 < |\text{ nonzero algebraic integer}| < \text{ a different, small, positive quantity.}$$

Taking the algebraic norm of the nonzero algebraic integer and estimating the *small, positive quantity* we are led, hopefully, to an inequality:

$$0 < |\text{nonzero integer}| < 1.$$

This final contradiction shows that our assumption that e^α is algebraic cannot hold, thus establishing the Hermite-Lindemann Theorem.

The proof of the Lindemann-Weierstrass also uses this approach, where the use of the conjugates of the assumed algebraic values is a bit more elaborate (and subtle). We omit any of these details but refer the interested reader to [Bu-Tu].

Exercises.

1. Let

$$P(z) = z^{p-1}(z-1)^p \cdots (z-d)^p = c_{p-1}z^{p-1} + c_p z^p + \cdots + c_{(d+1)p-1}z^{(d+1)p-1}.$$

Verify that the sum of Ps 1st through $(p-1)$st derivatives equals the sum:

$$\sum_{n=1}^{p-1} P^{(n)}(z) = \sum_{N=p-1}^{(d+1)p-1} \left(N! c_N \sum_{n=N-p+1}^{N-1} \frac{z^n}{n!} \right) .$$

2. Verify that the coefficients of P in problem 1, $c_{p-1}, \dots, c_{(d+1)p-1}$, satisfy

$$\max\{|c_{p-1}|, \dots, |c_{(d+1)p-1}|\} \le (2d)^{dp}.$$

3. Recall that for $t = 1, 2, \dots, d$,

$$T_p(t) = \sum_{N=p-1}^{(d+1)p-1} \left(N! c_N \sum_{n=N}^{\infty} \frac{t^n}{n!} \right);$$

Verify that for each of these values of t,

$$|T_p(t)| \le e^d d^{(d+2)p-1} \left((2d)^d\right)^p \; = c_1 \, (c_2)^p$$

where $c_1 = e^d/d$ and $c_2 = d^2 \left(2d^2\right)^d$.

4. a) Show that $\sqrt[3]{2}$ is an algebraic number and find its norm. Do the same for $i + \sqrt[3]{2}$.

b) Find the algebraic norm for each of the zeros of the polynomial $P(X) = 2X^4 + X - 8$. Does your calculation imply that any of these zeros are algebraic integers?

c) Suppose α is an algebraic number whose algebraic norm is a rational integer. Does it follow that α is an algebraic integer?