Algebraic and Transcendental Numbers

Given any distinct algebraic numbers $\alpha_1, \alpha_2, \ldots, \alpha_m$ the equation

$$\sum_{j=1}^{m} a_j e^{\alpha_j} = 0$$

is impossible in algebraic numbers $a_1, a_2, \ldots, a_m$ not all zero.

(F. Lindemann, 1822)

Probably the first crisis in Mathematics came with the discovery irrational or incommensurable numbers, such as $\sqrt{2}$. The early Greeks, in the fifth or sixth century B.C., were the first to realize that there are points on the number line which do not correspond to any rational number. In fact, it is now known that there are "more" irrationals than rationals. The concept of "more" as applied to infinite sets will be treated in another chapter.

The set of real numbers can also be divided into <u>algebraic</u> and <u>transcendental</u> numbers.

<u>Definition:</u> A number α is algebraic if α satisfies an equation of the form

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0$$

in which the coefficients a_i are rational numbers.

Notice that all rational numbers are algebraic, as well as numbers like $\sqrt{2}$.

<u>Definition:</u> A number is transcendental if it is not algebraic.

Thus, all transcendental numbers are irrational, but it was not known until 1844 whether any transcendental numbers actually existed! In that year Liouville constructed not only one, but an entire class of nonalgebraic real numbers, now known as Liouville numbers. About thirty years later, Cantor was able to prove that transcendental numbers exist and have the same cardinality as the real numbers (without exhibiting any transcendental numbers!). In 1873 C. Hermite proved that the number e is transcendental, and in 1882 F. Lindemann, basing his proof on Hermite's, was able to show that π is also transcendental. These are both great theorems, and the proof below of the transcendence of e is based on work of A. Hurwitz, published in 1893.

In order to prove the main result, the following preliminary lemma is convient.

<u>Lemma:</u> If $h(x) = \dfrac{f(x)g(x)}{n!}$ where $f(x) = x^n$ and $g(x)$ is a polynomial with integer coefficients, then $h^{(j)}(0)$, the jth derivative of h evaluated at $x = 0$, is an integer for $j = 0, 1, 2, \ldots$. Also, the integer $h^{(j)}(0)$ is divisible by $(n+1)$ for all j except possibly $j = n$, and in case $g(0) = 0$ the exception is not necessary.

Proof: (For those who are wondering what this lemma has to do with the transcendence of e, notice that it involves polynomials with integer coefficients, the kinds of things associated with algebraic numbers.) By calculating the first two or three derivatives of h and using induction it can be seen that

$$h^{(j)}(x) = \frac{1}{n!}\sum_{m=0}^{j}\binom{j}{m} f^{(m)}(x)g^{(j-m)}(x)$$

where $\binom{j}{m}$ represents the mth binomial coefficient of order j. Since $f(x) = x^n$ and since g can be expressed as $\displaystyle\sum_{i=0}^{k} c_i x^i$ with $c_0, c_1, \ldots, c_k$ intgers, it follows that

$$f^{(m)}(0) = \begin{cases} 0 & \text{if} \quad m \neq n \\ n! & \text{if} \quad m = n \end{cases} \quad \text{and } g^{(j-m)}(0) = \begin{cases} c_{j-m}(j-m)! & \text{if} \quad j-m \leq k \\ 0 & \text{if} \quad j-m > k \end{cases}.$$

Noting that k is the degree of g, there are 4 cases:

1. $\underline{j < n:}$ $f^{(m)}(0) = 0$ for $m = 0, 1, \ldots, j$, so $h^{(j)}(0) = 0$.
2. $\underline{j = n:}$ $h^{(n)}(0) = \frac{1}{n!}f^{(n)}(0)g(0) = c_0$.
3. $\underline{j = n+s,\ s = 1, 2, \cdots, k:}$ $h^{(j)}(0) = \frac{1}{n!}\binom{n+s}{n} n!\, g^{(s)}(0) = \frac{(n+s)!}{n!}\, c_s$.
4. $\underline{j > n+k}$: $h^{(j)}(0) = 0$.

Clearly, $h^{(j)}(0)$ is an integer in each case, and is divisble by $(n+1)$ in all except case 2. If $g(0) = c_0 = 0$, then the result in case 2 is also divisble by $(n+1)$. The proof of the lemma is complete.

Theorem : The number e satisfies no relation of the form

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

with integer coefficients not all 0.

Proof: The idea of the proof will be to assume that e does satisfy such a relation, and arrive at a logical impossibility, or contradiction. In this case, the contradiction will be that a certain number is a non-zero integer, but also has absolute value less than 1.

There is no loss of generality in assuming that a_m is nonzero.

For an odd prime p (to be specified later) define the polynomial

$$h(x) = \frac{x^{p-1}(x-1)^p(x-2)^p\cdots(x-m)^p}{(p-1)!}$$

which has degree $mp+p-1$ and notice that the lemma is applicable to not only $h(x)$, but also to $h(x+1)$, $h(x+2)$, ..., and $h(x+m)$. Also define

$$H(x) = h(x) + h'(x) + h''(x) + \cdots + h^{(mp+p-1)}(x)$$

and notice that $h^{(mp+p-1)} = (mp+p-1)!/(p-1)!$, a constant. Now

$$(e^{-x}H(x))' = e^{-x}H'(x) - e^{-x}H(x) = e^{-x}(H'(x) - H(x)) = -e^{-x}h(x)$$

so that

$$a_i \int_0^i e^{-x}h(x)dx = -a_i \int_0^i (e^{-x}H(x))' dx = -a_i[e^{-i}H(i) - H(0)].$$

Now multiply by e^i and sum from i=0 to m :

$$\sum_{i=0}^m a_i e^i \int_0^i e^{-x}h(x)dx = H(0)\sum_{i=0}^m a_i e^i - \sum_{i=0}^m a_i H(i).$$

Now, assuming that e does satisfy the equation in the theorem, the first term on the right is 0, and using the definition of H, the above equation becomes:

$$\sum_{i=0}^m a_i e^i \int_0^i e^{-x}h(x)dx = -\sum_{i=0}^m \sum_{j=0}^{mp+p-1} a_i h^{(j)}(i). \qquad (*)$$

Looking first at the right side, the lemma can be applied to $h(x)$, $h(x+1)$, $h(x+2)$,..., and $h(x+m)$ to get, (for $j = 0, 1, \ldots, mp+p-1$) $h^{(j)}(0)$, $h^{(j)}(1)$, ..., $h^{(j)}(m)$ are all integers and are all divisble by p except possibly $h^{(p-1)}(0)$. However,

$$h^{(p-1)}(0) = (-1)^p(-2)^p \cdots (-m)^p$$

and if p is chosen so that $p > m$ and also $p > |a_0|$ then

1. $h^{(p-1)}(0)$ is not divisible by p, and
2. every term in the double sum above is a multiple of p except the term $-a_0 h^{(p-1)}(0)$.

Therefore the right side of (*) represents a <u>nonzero</u> integer. Turning to the left side now,

$$\begin{aligned}
\left|\sum_{i=0}^m a_i e^i \int_0^i e^{-x}h(x)dx\right| &\leq \sum_{i=0}^m \left|a_i e^i \int_0^i e^{-x}h(x)dx\right| \\
&\leq \sum_{i=0}^m |a_i|\, e^i\, (i)\, (1)\, \frac{m^{mp+p-1}}{(p-1)!} \\
&\leq \sum_{i=0}^m |a_i|\, m\, e^m \frac{m^{mp+p-1}}{(p-1)!} \\
&\leq \sum_{i=0}^m |a_i|\, e^m \frac{(m^{m+2})^{(p-1)}}{(p-1)!}
\end{aligned}$$

where it is necessary to require $p > m + 2$ for the last inequality. The expression $\dfrac{(m^{m+2})^{(p-1)}}{(p-1)!}$ above is the p-th term in the series for $e^{m^{m+2}}$, which is a convergent series of constants, and so the p-th term can be made arbitrarily small by choosing p large enough. This means that the left side of (*) can be made smaller than 1 in absolute value, contradicting that the right side is a nonzero integer. This completes the proof.

Lindemann's theorem, stated at the beginning of this section, replaces the integer exponents 0, 1, $\ldots$, m by algebraic numbers $\alpha_1, \ldots, \alpha_m$. The transcendence of π then follows from observing that, if π were algebraic, then $i\pi$ would also be algebraic and the equation

$$e^{i\pi} + 1 = 0$$

would be impossible. However, this formula is one of the best-known in mathematics and is certainly true, so π must be transcendental.