TOPICS IN ALGEBRA

2nd edition

I. N. HERSTEIN
15. (a) Prove that \( \sin 1^\circ \) is an algebraic number.
(b) From part (a) prove that \( \sin m^\circ \) is an algebraic number for integer \( m \).

### 5.2 The Transcendence of \( e \)

In defining algebraic and transcendental numbers we pointed out that it could be shown that transcendental numbers exist. One way of doing this would be the demonstration that some specific number is transcendental.

In 1851 Liouville gave a criterion that a complex number be transcendental; using this, he was able to write down a large collection of transcendental numbers. For instance, it follows from his work that the number \( 0.101001000000010 \ldots \) is transcendental; here the number of zeros between successive ones goes as \( 1!, 2!, \ldots, n!, \ldots \).

This certainly settled the question of existence. However, the hard problem of whether some given, familiar numbers were transcendental still persisted. The first success in this direction was by Hermite, who in 1873 proved that \( e \) is transcendental. His proof was greatly simplified by Hilbert, who gave an even shorter proof that we shall give here is a variation, due to Hurwitz, of Hilbert's proof.

The number \( \pi \) offered greater difficulties. These were finally overcome by Lindemann, who in 1882 produced a proof that \( e \) is transcendental. One immediate consequence of this is the fact that it is impossible to draw a straightedge and compass, to square the circle, so such a construction would lead to an algebraic number \( \theta \) such that \( \theta^2 = \pi \). But if \( \theta \) is algebraic, then so is \( \theta^2 \), in virtue of which \( \pi \) would be algebraic, in contradiction to Lindemann's result.

In 1934, working independently, Gelfond and Schneider proved that if \( a \) and \( b \) are algebraic numbers and if \( b \) is irrational, then \( a^b \) is transcendental. This answered in the affirmative the question raised by Hilbert whether \( 2^{\sqrt{2}} \) was transcendental.

For those interested in pursuing the subject of transcendental numbers further, we would strongly recommend the charming books by C. L. Siegel entitled *Transcendental Numbers*, and by I. Niven, *Irrational Numbers*.

To prove that \( e \) is irrational is easy; to prove that \( \pi \) is irrational is somewhat more difficult. For a very clever and neat proof of the latter, see the paper by Niven entitled "A simple proof that \( \pi \) is irrational," *Bulletin of the American Mathematical Society*, Vol. 53 (1947), page 509.

Now to the transcendence of \( e \). Aside from its intrinsic interest, it offers us a change of pace. Up to this point all our arguments have been of an algebraic nature; now, for a short while, we return to the more familiar calculus. The proof itself will use only elementary calculus; the real meat needed, therefore, will be the mean value theorem.

#### 5.2.1 The number \( e \) is transcendental

The proof we shall use the standard notation \( f^{(r)}(x) \) to denote the \( r \)th derivative of \( f(x) \) with respect to \( x \).

Since \( f(x) \) is a polynomial of degree \( r \) with real coefficients.

Next, we compute the fact that \( f^{(r+1)}(x) = 0 \) (since \( f(x) \) is of degree \( r \)).

The property of \( e \), namely that \( (e^x)' = e^x \), we obtain

\[
-f(\theta_k) = e^{-\theta_k}\frac{df}{dx}(\theta_k)k.
\]

The value theorem asserts that if \( g(x) \) is a continuously differentiable function on the closed interval \([x_1, x_2]\) then

\[
g(x_2) = g(x_1) + \frac{df}{dx}(\theta_k)(x_2 - x_1), \quad \text{where} \quad 0 < \theta < 1.
\]

This to our function \( e^{-\theta}F(x) \), which certainly satisfies all the conditions for the mean value theorem on the closed interval \( x_1 = 0 \) and \( x_2 = k \), where \( k \) is any positive integer. We then obtain

\[
F(k) - F(0) = -e^{-\theta_k}\frac{df}{dx}(\theta_k)k, \quad \text{where} \quad \theta_k \text{ depends on } k \text{ and } 0 < \theta_k < 1.
\]

Multiplying this relation through by \( -e^x \)

\[
F(1) - eF(0) = -e^{1-\theta_1}\frac{df}{dx}(\theta_1) = e_1,
\]

\[
F(2) - e^2F(0) = -2e^{2(1-\theta_2)}\frac{df}{dx}(\theta_2) = e_2,
\]

\[
F(n) - e^nF(0) = -ne^n\theta_1\frac{df}{dx}(\theta_n) = e_n.
\]

Now that \( e \) is an algebraic number; then it satisfies some relation

\[
c_1e + c_2e^2 + \cdots + c_ne^n = 0,
\]

where \( c_1, c_2, \ldots, c_n \) are integers and where \( c_0 > 0 \).

Evaluations (1) lead us multiply the first equation by \( c_1 \), the second by \( c_2 \), adding these up we get

\[
c_1F(1) + \cdots + c_ne^nF(n) = c_1e_1 + c_2e_2 + \cdots + c_ne_n.
\]

The relation (2), \( c_1e + c_2e^2 + \cdots + c_ne^n = 0 \), whence the relation simplifies to

\[
c_1F(1) + \cdots + c_ne^nF(n) = c_1e_1 + \cdots + c_ne_n.
\]
polynomial \( f(x) \). We now see what all this implies for a very easy polynomial, one first used by Hermite, namely,

\[
f(x) = \frac{1}{(p-1)!} x^{p-1} (1-x)^p (2-x)^p \cdots (n-x)^p.
\]

Here \( p \) can be any prime number chosen so that \( p > n \) and \( p \) divides this polynomial we shall take a very close look at \( F(0), F(1), \ldots \), and we shall carry out an estimate on the size of \( \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n \).

When expanded, \( f(x) \) is a polynomial of the form

\[
\frac{(n!)^p}{(p-1)!} x^{p-1} \frac{a_0 x^p}{(p-1)!} + \frac{a_1 x^{p+1}}{(p-1)!} + \cdots,
\]

where \( a_0, a_1, \ldots \), are integers.

When \( i \geq p \) we claim that \( f^{(i)}(x) \) is a polynomial, with integer coefficients all of which are multiples of \( p \). (Prove! See Sec. 5.3.)

Thus for any integer \( j \), \( f^{(i)}(j) \), for \( i \geq p \), is an integer and is a multiple of \( p \).

Now, from its very definition, \( f(x) \) has a root of multiplicity \( p \) at \( x = 0, 1, \ldots, n \). Thus for \( j = 1, 2, \ldots, n \), \( f(j) = 0 \), \( f^{(1)}(j) = 0 \), \ldots, \( f^{(p-1)}(j) = 0 \).

However, \( F(j) = f(j) + f^{(1)}(j) + \cdots + f^{(p-1)}(j) \) is a multiple of \( p \).

What about \( F(0) \)? Since \( f(x) \) has a root of multiplicity \( p \), \( f(0) = f^{(1)}(0) = \cdots = f^{(p-2)}(0) = 0 \) for \( i \geq p \), \( f^{(i)}(0) \) which is a multiple of \( p \). But \( f^{(p-1)}(0) = (n!)^p \) and since \( p \) is a prime number, \( p \nmid (n!)^p \) so that \( f^{(p-1)}(0) \) is an integer not divisible by \( p \).

Since \( F(0) = f(0) + f^{(1)}(0) + \cdots + f^{(p-1)}(0) + f^{(p-2)}(0) + \cdots + f^{(i)}(0) \), we conclude that \( F(0) \) is an integer not divisible by \( p \).

\( \varepsilon_0 > 0 \) and \( p > \varepsilon_0 \) and because \( p \nmid F(0) \) whereas \( p \mid F(n) \), we can assert that \( c_0 F(0) + c_1 F(1) + \cdots + c_n F(n) = \varepsilon_0 \).

However, by (3), \( c_0 F(0) + c_1 F(1) + \cdots + c_n F(n) = \varepsilon_0 \).

What can we say about \( \varepsilon_i \)? Let us recall that

\[
\varepsilon_i = \frac{e^{i (1-\theta_1)} (1 - i \theta_1)^p \cdots (n - i \theta_1)^p (i \theta_1)^p}{(p-1)!}
\]

where \( 0 < \theta_1 < 1 \). Thus

\[
|\varepsilon_i| \leq e^n n^p (n!)^p \frac{p}{(p-1)!}.
\]

As \( p \to \infty \),

\[
\frac{e^n n^p (n!)^p}{(p-1)!} \to 0.
\]

Whence we can find a prime number larger than both \( c_0 \) and \( n \) and large enough to force \( |c_0 \varepsilon_1 + \cdots + c_n \varepsilon_n| < 1 \). But \( c_0 \varepsilon_1 + \cdots + c_n \varepsilon_n = \varepsilon_0 \), so must be an integer; since it is smaller than 1 in absolute value, the only possible conclusion is that \( c_0 \varepsilon_1 + \cdots + c_n \varepsilon_n = 0 \). Consequently, \( c_0 F(0) + \cdots + c_n F(n) = 0 \); this however is sheer nonsense, since now that \( p \nmid (c_0 F(0) + \cdots + c_n F(n)) \), whereas \( p \mid 0 \). This contradiction from the assumption that \( \varepsilon \) is algebraic, proves that \( \varepsilon \) must be transcendental.


e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{m!} + \cdots,

Thus \( \varepsilon \) is irrational.

If \( f(x) \) is a polynomial with integer coefficients, prove that if \( p \) is a prime number, then for \( i \geq p \),

\[
\frac{d^i}{dx^i} \left( \frac{g(x)}{(p-1)!} \right)
\]

is a polynomial with integer coefficients each of which is divisible by \( p \).

For any real number, prove that \( (a^m/m!) \to 0 \) as \( m \to \infty \).

If \( a, b, n \) are integers, prove that \( e^{m/n} \) is transcendental.

**Roots of Polynomials**

In Sec. 5.3 we discussed elements in a given extension \( K \) of \( F \) which were roots of polynomials in \( F \), that is, elements which satisfied polynomials in \( F[x] \). We now introduce the problem around; given a polynomial \( p(x) \) in \( F[x] \) we wish to find a field \( K \) which is an extension of \( F \) in which \( p(x) \) has a root.

The field \( K \) available to us; in fact it is our prime objective to find it. Once it is constructed, we shall examine it more closely and determine its consequences we can derive.

If \( p(x) \in F[x] \), then an element \( a \) lying in some extension of \( F \) is called a root of \( p(x) \) if \( p(a) = 0 \).

With the familiar result known as the Remainder Theorem.

If \( p(x) \in F[x] \) and if \( K \) is an extension of \( F \), then for any element \( a = (x - b)q(x) + p(b) \) where \( q(x) \in K[x] \) and where \( \deg q(x) = \)