Grade 11–12 Math Circles
November 3rd, 2021
Lesson 2: Algebraic and Transcendental Numbers

§1 Introduction

In Lesson 1, you learned about irrational numbers, and in this lesson we will focus on even more bizarre numbers — those that are called *transcendental*. Transcendental numbers are generalizations of irrational numbers. Proofs of transcendence are even harder than proofs of irrationality, and they rely on mysterious mathematical theories, such as the theory of *Linear Forms in Logarithms*. In this lesson, we will see what algebraic and transcendental numbers are, *construct* a transcendental number, and learn about famous theorems and open problems in Transcendental Number Theory.

§2 Polynomials and Their Rate of Growth

Before we introduce the notion of a *transcendental number*, we need to recall some of our knowledge on polynomials. Let d be some non-negative integer, and let $a_0, a_1, \ldots, a_d$ be real numbers. We refer to the function $f(x)$ of the form

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$$

as a *polynomial*. Here are some examples of polynomials:

- $f(x) = 0$ (we also refer to this function as the *zero polynomial*)
- $g(x) = x + 1$
- $h(x) = x^2 - 2$

In Figure 1, the graphs of $f(x)$, $g(x)$ and $h(x)$. Notice that, for large enough x, $g(x)$ grows faster than $f(x)$, while $h(x)$ grows faster than $g(x)$.

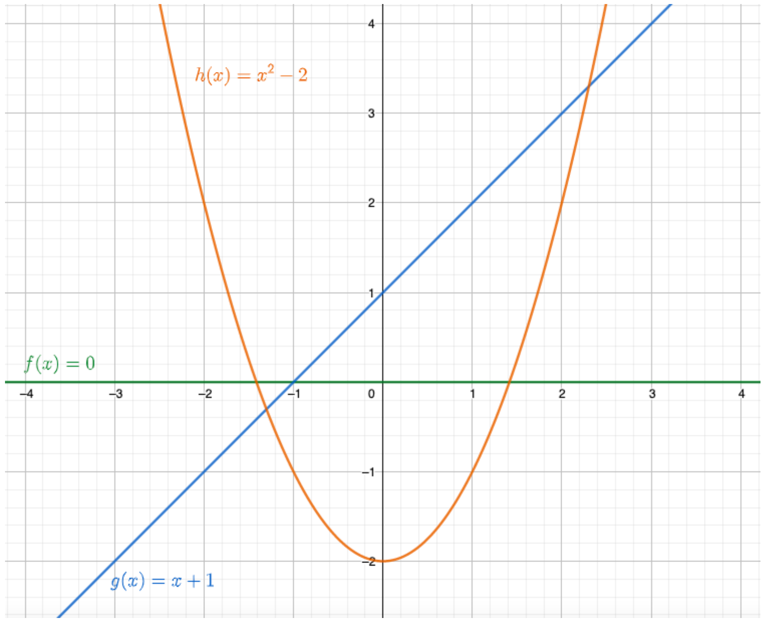

Figure 1: Graphs of $f(x) = 0$, $g(x) = x + 1$ and $h(x) = x^2 - 2$

Exercise 1

Determine which of the following functions are polynomials:

- $x^3 - x + 1$
- $\sqrt{x}$
- $x + \frac{1}{x}$
- π

Exercise 1 Solution

- The function $f(x) = x^3 - x + 1$ is a polynomial of the form

$$f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$$

  where $a_3 = 1$, $a_2 = 0$, $a_1 = -1$ and $a_0 = 1$.
- The function $\sqrt{x}$ is not a polynomial.
- The function $x + \frac{1}{x}$ is not a polynomial, since it has a term x^{-1}.

- The function $f(x) = \pi$ is a polynomial of the form

$$f(x) = a_0$$

where $a_0 = \pi$.

If for a *non-zero* polynomial $f(x) = a_d x^d + \cdots + a_1 x + a_0$ we have $a_d \neq 0$, then we say that a polynomial $f(x)$ has *degree* d, denoted $\deg f(x)$. If $f(x)$ is the zero polynomial, we are going to say that its degree is *undefined*. For example,

- The degree of $f(x) = 0$ is undefined;
- The degree of $g(x) = x + 1$ is equal to 1;
- The degree of $h(x) = x^2 - 2$ is equal to 2.

Exercise 2

Determine the degrees of each of the following polynomials:

- $f(x) = 1$
- $g(x) = 8x^3 - 6x - 1$
- $h(x) = 4x^2 - 2x - 1$

Exercise 2 Solution

- The degree of $f(x) = 1$ is equal to 0;
- The degree of $g(x) = 8x^3 - 6x - 1$ is equal to 3;
- The degree of $h(x) = 4x^2 - 2x - 1$ is equal to 2.

Another important parameter associated with a polynomial is its *height*. A *height* of a polynomial $f(x) = a_d x^d + \cdots + a_1 x + a_0$ is the non-negative number

$$H = \max(\ |a_0|,\ |a_1|,\ \ldots,\ |a_d|\ )$$

For example,

- The height of $f(x) = 0$ is $H = \max(\ |0|\ ) = 0$;

- The height of $g(x) = x - 1$ is $H = \max(\,|-1|,\ |1|\,) = 1$;
- The height of $h(x) = x^2 - 2$ is $H = \max(\,|-2|,\ |0|,\ |1|\,) = 2$.

Exercise 3

Determine the heights of each of the following polynomials:

- $f(x) = 1$
- $g(x) = 8x^3 - 6x - 1$
- $h(x) = 4x^2 - 2x - 1$

Exercise 3 Solution

- The height of $f(x) = 1$ is $H = \max(\,|1|\,) = 1$;
- The height of $g(x) = 8x^3 - 6x - 1$ is $H = \max(\,|-1|,\ |-6|,\ |0|,\ |8|\,) = 8$;
- The height of $h(x) = 4x^2 - 2x - 1$ is $H = \max(\,|-1|,\ |-2|,\ |4|\,) = 4$.

The degree and the height are important, because they tells us how big can the function $|f(x)|$ be depending on the value of x. The following theorem makes this statement precise.

Theorem 1 (Rate of Growth of a Polynomial)

Let $f(x) = a_d x^d + \cdots + a_1 x + a_0$ be a polynomial of degreed d and height H. Then for every real number α,

$$|f(\alpha)| \leq H \cdot \left(\, |\alpha|^d \ +\ \cdots\ +\ |\alpha| + 1 \,\right)$$

Proof. Suppose that

$$f(x) = a_d x^d + \cdots + a_1 x + a_0$$

Notice how

$$|a_0| \leq H, \qquad |a_1| \leq H, \qquad \ldots, \qquad |a_d| \leq H$$

Thus,

$$|a_0| \leq H, \qquad |a_1 \alpha| \leq H \cdot |\alpha|, \qquad \ldots, \qquad \left|a_d \alpha^d\right| \leq H \cdot |\alpha|^d$$

Now, recall the triangle inequality, which tells us that $|v + w| \leq |v| + |w|$ for all real numbers v and w.

Therefore,

$$\begin{aligned} |f(\alpha)| &= |a_d\alpha^d \ + \ \cdots \ + \ a_1\alpha \ + \ a_0| \\ \text{Triangle inequality} \rightarrow &\leq |a_d\alpha^d| \ + \ \cdots \ + \ |a_1\alpha| \ + \ |a_0| \\ &\leq H \cdot |\alpha|^d \ + \ \cdots \ + \ H \cdot |\alpha| \ + \ H \\ &= H \cdot \left(\ |\alpha|^d \ + \ \cdots \ + \ |\alpha| + 1 \ \right) \end{aligned}$$

□

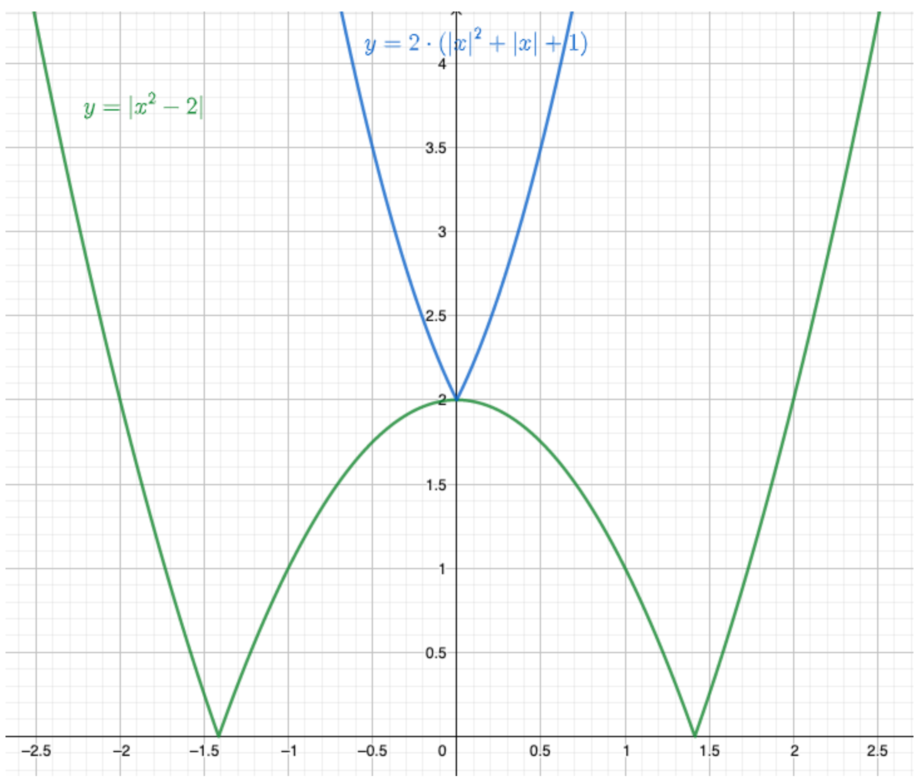

Figure 2: Graphs of $y = |x^2 - 2|$ and $y = 2 \cdot (|x|^2 + |x| + 1)$

Theorem 1 tells us that, for a polynomial $f(x)$ of degree d and height H, the absolute value of $f(x)$ is bounded above by the function $H \cdot \left(\ |x|^d \ + \ \cdots \ + \ |x| + 1 \ \right)$. In Figure 2 it is illustrated that, when $f(x) = x^2 - 2$, the graph of $y = |x^2 - 2|$ lies below the graph of $y = 2 \cdot (|x|^2 + |x| + 1)$. But how good is this bound? Are there examples of polynomials for which this bound is attainable? You will explore this question in the following exercise.

Exercise 4

For each non-negative integer d, find a polynomial $f(x)$ of degree d and height H such that

$$|f(\alpha)| = H \cdot \big(\ |\alpha|^d\ +\ \cdots\ +\ |\alpha| + 1\ \big)$$

for some real number α.

Exercise 4 Solution

Let d be a non-negative integer, and define

$$f(x) = x^d + \cdots + x + 1$$

Then

$$H = \max\big(\ |a_0|,\ |a_1|,\ \ldots,\ |a_d|\ \big) = \max\big(\ 1,\ 1,\ \ldots,\ 1\ \big) = 1$$

Then for $\alpha = 0$ we have

$$|f(0)| = 1 = H \cdot \big(\ |0|^d\ +\ \cdots\ +\ |0| + 1\ \big)$$

In fact, you can notice how the equality

$$|f(\alpha)| = H \cdot \big(\ |\alpha|^d\ +\ \cdots\ +\ |\alpha| + 1\ \big)$$

holds for *any* non-negative real number α.

§3 Polynomial Divisibility and Roots of Polynomials

In some way, polynomials are very similar to integers. For example, you can add, subtract and multiply polynomials, and the result will still be a polynomial. Polynomials also have an analogue of division with remainder.

Theorem 2 (Division With Remainder)
For all polynomials $f(x)$ and $g(x)$, with $g(x)$ not equal to the zero polynomial, there exist *unique* polynomials $q(x)$ (the *quotient*) and $r(x)$ (the *remainder*), such that

$$f(x) = q(x) \cdot g(x) + r(x)$$

and either $r(x)$ is the zero polynomial or $0 \leq \deg r(x) < \deg g(x)$.

Just like for integers, we can find quotient and remainder using *polynomial long division*. For example, we can find the quotient and remainder of $f(x) = x^3 + x^2 - 2x - 2$ when divided by $g(x) = x + 1$ as follows:

$$\begin{array}{r|l} & x^2 + 0x - 2 \\ \hline x+1 & x^3 + x^2 - 2x - 2 \\ & -x^3 - x^2 \\ \hline & 0x^2 - 2x \\ & 0x^2 + 0x \\ \hline & -2x - 2 \\ & 2x + 2 \\ \hline & 0 \end{array}$$

Based on these calculations, we find that $f(x) = q(x) \cdot g(x) + r(x)$, where

$$q(x) = x^2 - 2 \quad \text{and} \quad r(x) = 0$$

In Exercise 5 you can practice polynomial long division. For review, consider completing the module on Polynomial Equations and Inequalities in the CEMC Courseware.

Exercise 5
Find the quotient and remainder of $f(x) = x^2 - 2$ when divided by $g(x) = x - \frac{3}{2}$.

Exercise 5 Solution

We have

$$\begin{array}{r|l} & x + \frac{3}{2} \\ \cline{2-2} x - \frac{3}{2} & x^2 + 0x - 2 \\ & -\,x^2 + \frac{3}{2}x \\ \cline{2-2} & \frac{3}{2}x - 2 \\ & -\,\frac{3}{2}x + \frac{9}{4} \\ \cline{2-2} & \frac{1}{4} \end{array}$$

Based on these calculations, we find that $f(x) = q(x) \cdot g(x) + r(x)$, where

$$q(x) = x + \frac{3}{2} \quad \text{and} \quad r(x) = \frac{1}{4}$$

Notice how in Exercise 5, as well as in example preceding it, the remainder turned out to be a constant polynomial. Theorem 2 tells us that this is exactly what we should expect when the polynomial $g(x)$ that we are dividing by has degree 1, since in this case $r(x)$ is either the zero polynomial or its degree satisfies the inequality $0 \leq \deg r(x) < \deg g(x) = 1$, so $\deg r(x) = 0$. Theorem 3 shows that the situation becomes especially interesting when we divide a polynomial $f(x)$ by a polynomial $x - \alpha$, where α satisfies $f(\alpha) = 0$.

Theorem 3 (Factor Theorem)

Let $f(x)$ be a non-zero polynomial and let α be a real number such that $f(\alpha) = 0$. Then

$$f(x) = q(x) \cdot (x - \alpha)$$

for some polynomial $q(x)$.

Proof. Since $x - \alpha$ is not equal to the zero polynomial, it follows from Theorem 1 that there exist polynomials $q(x)$ and $r(x)$ such that

$$f(x) = q(x) \cdot (x - \alpha) + r(x)$$

and $r(x)$ is either the zero polynomial or $0 \leq \deg r(x) < \deg(x - \alpha)$. Since $\deg(x - \alpha) = 1$, we see that $r(x)$ must be a constant polynomial, i.e., there exists a real number r such that $r(x) = r$ for all real numbers x. Thus,

$$f(x) = q(x) \cdot (x - \alpha) + r$$

and since $f(\alpha) = 0$, we see that

$$r = f(\alpha) - q(\alpha) \cdot (\alpha - \alpha) = 0$$

which means that $f(x) = q(x) \cdot (x - \alpha)$. □

If $f(x)$ is a non-zero polynomial, we refer to a real number α such that $f(\alpha) = 0$ as a *root* of $f(x)$. Notice in the example above that, since $\alpha = -1$ is a root of $f(x) = x^3 + x^2 - 2x - 2$, the polynomial $f(x)$ can be written as $f(x) = q(x)(x - (-1))$, where $q(x) = x^2 - 2$.

§4 Algebraic and Transcendental Numbers

Now that we reviewed properties of polynomials, we are ready to introduce the concept of an *algebraic number*, which will later help us to explain what a *transcendental number* is. Note that, if a number $\frac{m}{n}$ is rational, then it is a root of a non-zero polynomial $f(x) = nx - m$ of degree 1, which has rational coefficients:

$$f\left(\frac{m}{n}\right) = n \cdot \frac{m}{n} - m = m - m = 0$$

It turns out that it is possible to find a polynomial like that for other numbers, possibly of higher degree. Take, for example, the number $\sqrt{2}$ and the polynomial $g(x) = x^2 - 2$. Then,

$$g\left(\sqrt{2}\right) = \left(\sqrt{2}\right)^2 - 2 = 2 - 2 = 0$$

This motivates the following definition: we are going to say that a real number α is *algebraic* if there exists a *non-zero* polynomial $f(x)$, with *rational* coefficients, such that $f(\alpha) = 0$.

Exercise 6

Prove that each of the following real numbers α are algebraic by finding a *non-zero* polynomial $f(x)$, with *rational* coefficients, such that $f(\alpha) = 0$:

- $\cos(90°)$
- $\cos(30°)$
- $\cos(1°)$

Hint: To solve the last one, recall the definition of an n-th Chebyshev polynomial $T_n(x)$ from §3 of Lesson 1.

Exercise 6 Solution

- Since $\cos(90°) = 0$, we can take $f(x) = x$:

$$f(\cos 90°) = f(0) = 0$$

- Since $\cos(30°) = \frac{\sqrt{3}}{2}$, we can take $f(x) = 4x^2 - 3$:

$$f(\cos 30°) = f\left(\frac{\sqrt{3}}{2}\right) = 4\left(\frac{\sqrt{3}}{2}\right)^2 - 3 = 4 \cdot \frac{3}{4} - 3 = 0$$

- Recall how in §3 of Lesson 1, for each non-negative integer n, we've defined an *n-th Chebyshev polynomial* $T_n(x)$. According to Theorem 4, this polynomial has a special property that $T_n(\cos\alpha) = \cos(n\alpha)$ for every real number α. Furthermore, by definition, $T_n(x)$ has rational coefficients. Now, for $n = 90$, we must have

$$T_{90}(\cos(1°)) = \cos(90 \cdot 1°) = \cos(90°) = 0$$

The only thing that remains is to prove that $T_{90}(x)$ is not the zero polynomial. Notice that, if we can find *one* value x_0 for which $T_{90}(x_0) \neq 0$, we would be done. Taking $x_0 = \cos(2°)$,

$$T_{90}(\cos(2°)) = \cos(90 \cdot 2°) = \cos(180°) = -1 \neq 0$$

Therefore, $T_{90}(x)$ is non-zero.

So what are transcendental numbers? Well, we say that a number α is transcendental if it is **not** algebraic. That's it! To be more precise, a number α is transcendental if there does **not** exist a non-zero polynomial $f(x)$, with rational coefficients, such that $f(\alpha) = 0$.

Now, just like Ancient Greeks wondered whether or not every number is rational (the answer is "no", as you know from Lesson 1, §1, Theorem 1), we wonder whether every number out there is algebraic. The answer to this question is, once again, "no", but the proof of this fact is rather non-trivial. The first ever transcendental number was discovered in 1844 by a French mathematician Joseph Liouville, and in 6 we will learn about the criterion for transcendence that enabled Liouville to make his famous discovery.

§5 Minimal Polynomial of an Algebraic Number

In order to understand Liouville's criterion for transcendentality, we first need to understand algebraic numbers better. If we take an algebraic number α, then we know that there exists a non-zero polynomial $f(x)$, with rational coefficients, such that $f(\alpha) = 0$. The problem though is that there could be many polynomials with this property. Take, for example, $\alpha = \sqrt{2}$. Then each of the following non-zero polynomials with rational coefficients has α as its root:

- $\frac{1}{2}x^2 - 1$
- $x^3 - 2x$
- $x^2 - 2$
- $-x^2 + 2$
- $3x^2 - 6$

Among all these polynomials, is it possible to pick the one that is the most convenient to work with? It turns out that it *is* possible. In particular, notice how the polynomial $f(x) = x^2 - 2$ has *integer* coefficients, its leading coefficient is positive, and no other polynomial that has α as a root has a degree smaller than $\deg f(x)$. Further, its coefficients -2, 0 and 1 have no positive common divisors, apart from 1. It turns out that $x^2 - 2$ is the only polynomial with such unique properties, and we refer to it as the *minimal polynomial* of $\alpha = \sqrt{2}$.

Let us now introduce our last definition for this lesson. We say that $f(x) = a_d x^d + \cdots + a_1 x + a_0$ is the *minimal polynomial* of an algebraic number α if

1. $f(\alpha) = 0$;

2. $f(x)$ has *integer* coefficients;
3. $a_d > 0$;
4. The only positive common divisor k of the coefficients $a_0, a_1, \ldots, a_d$ is $k = 1$; and
5. The degree of $f(x)$ is the smallest among all non-zero polynomials $q(x)$, with rational coefficients, such that $q(\alpha) = 0$.

In Theorem 4, which we leave without proof, we state the defining property of a minimal polynomial.

Theorem 4 (Minimal Polynomial Is Unique)

The minimal polynomial of an algebraic number α is unique.

Theorem 5

The minimal polynomial of $\sqrt{2}$ is $f(x) = x^2 - 2$.

Proof. Let us verify that $f(x) = x^2 - 2$ satisfies each of the five properties of the minimal polynomial of $\alpha = \sqrt{2}$:

1. We have $f(\alpha) = \left(\sqrt{2}\right)^2 - 2 = 2 - 2 = 0$.
2. The coefficients of $f(x)$ are -2, 0 and 1, which are all integers.
3. The leading coefficient of $f(x)$ is equal to 1 and it is positive.
4. The only positive common divisor of -2, 0 and 1 is 1.
5. Suppose that $f(x) = x^2 - 2$ does *not* have the smallest degree, and so there exists a non-zero polynomial $q(x)$, with rational coefficients, such that $q(\alpha) = 0$ and $\deg q(x) < \deg f(x)$. Then the degree of $q(x)$ has to be equal to 1, and so $g(x) = ax + b$ for some $a, b \in \mathbb{Q}$, with $a \neq 0$. Now, since $g(\alpha) = 0$, we see that $a \cdot \sqrt{2} + b = 0$, which is equivalent to $\sqrt{2} = -\frac{b}{a}$. Since the number $-\frac{b}{a}$ is rational and $\sqrt{2}$ is irrational, we reach a contradiction. Thus, $f(x)$ has the smallest degree.

Since $f(x)$ satisfies all the properties of the minimal polynomial of $\sqrt{2}$, it follows from Theorem 4 that $f(x) = x^2 - 2$ is the minimal polynomial of $\sqrt{2}$. □

Exercise 7

Let $\frac{m}{n}$ be a rational number, with $m \in \mathbb{Z}$ and $n \in \mathbb{N}$, written in lowest terms. Prove that the minimal polynomial of $\frac{m}{n}$ is $f(x) = nx - m$.

Exercise 7 Solution

Let us verify that $f(x) = nx - m$ satisfies each of the five properties of the minimal polynomial of $\alpha = \frac{m}{n}$:

1. We have $f(\alpha) = n \cdot \frac{m}{n} - m = m - m = 0$.
2. The coefficients of $f(x)$ are $-m$ and n, which are both integers.
3. The leading coefficient of $f(x)$ is equal to n and it is positive, because $n \in \mathbb{N}$.
4. Suppose that $k \geq 2$ is a common divisor of $-m$ and n, so that $-m = ks$ and $n = kt$ for some integers s and t. Then, $\frac{m}{n} = -\frac{ks}{kt} = -\frac{s}{t}$, which contradicts the fact that $\frac{m}{n}$ is written in lowest terms. Thus, $k = 1$ is the only positive common divisor of $-m$ and n.
5. Since $f(x) = nx - m$ has degree 1, and the minimal polynomial cannot be a constant polynomial, we see that $f(x)$ has the smallest degree possible.

Since $f(x)$ satisfies all the properties of the minimal polynomial of $\frac{m}{n}$, it follows from Theorem 4 that $f(x) = nx - m$ is the minimal polynomial of $\frac{m}{n}$.

Exercise 8

Determine, with proof, the minimal polynomial of $\cos(30°)$.

Exercise 8 Solution

Let us verify that $f(x) = 4x^2 - 3$ satisfies each of the five properties of the minimal polynomial of $\alpha = \cos(30°) = \frac{\sqrt{3}}{2}$:

1. We have $f(\alpha) = 4\left(\frac{\sqrt{3}}{2}\right)^2 - 3 = 4 \cdot \frac{3}{4} - 3 = 0$.
2. The coefficients of $f(x)$ are -3, 0 and 4, which are all integers.
3. The leading coefficient of $f(x)$ is equal to 4 and it is positive.
4. The only positive common divisor of -3, 0 and 4 is 1.

5. Suppose that $f(x) = 4x^2 - 3$ does *not* have the smallest degree, and so there exists a non-zero polynomial $q(x)$, with integer coefficients, such that $q(\alpha) = 0$ and $\deg q(x) < \deg f(x)$. Then the degree of $q(x)$ has to be equal to 1, and so $q(x) = ax + b$ for some $a, b \in \mathbb{Q}$, with $a \neq 0$. Now, since $q(\alpha) = 0$, we see that $a \cdot \frac{\sqrt{3}}{2} + b = 0$, which is equivalent to $\sqrt{3} = -\frac{2b}{a}$. Since the number $-\frac{2b}{a}$ is rational and $\sqrt{3}$ is irrational, we reach a contradiction. Thus, $f(x)$ has the smallest degree.

Since $f(x)$ satisfies all the properties of the minimal polynomial of $\cos(30°)$, it follows from Theorem 4 that $f(x) = 4x^2 - 3$ is the minimal polynomial of $\cos(30°)$.

§6 Approximation of Algebraic Numbers By Rationals

Finally, we are able to state a very important result, which gives us a property that characterizes all algebraic numbers.

Theorem 6

Let α be an algebraic number with the minimal polynomial $f(x)$ of degree d. There exists a positive number C, which depends only on α, such thats for every rational number $\frac{p}{q} \neq \alpha$, with $p \in \mathbb{Z}$ and $q \in \mathbb{N}$, the inequality

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{C}{q^d}$$

is satisfied. Furthermore, we can take

$$C = \frac{1}{H \cdot \Big((1+|\alpha|)^{d-1} + \cdots + (1+|\alpha|) + 1 \Big)}$$

where H is the height of the polynomial $g(x)$ such that $f(x) = (x - \alpha)g(x)$.

Theorem 6 tells us that, no matter what you do, any algebraic α cannot be approximated by a rational number $p/q \neq \alpha$ "too well". In other words, if $\alpha \neq p/q$, there is always a limitation to how close p/q can be to α: the distance between these two numbers can never be smaller than Cq^{-d}.

Notice how similar the above theorem is to the result proved in §5 of Lesson 1. The latter follows by simply taking $d = 1$ in Theorem 6 above.

Let us now turn out attention to the proof of Theorem 6. To do so, we need to establish two supplementary results. In mathematics, such results are called *lemmas*.

Lemma 1

Let α be an algebraic number with the minimal polynomial $f(x)$ of degree $d \geq 1$. Then for every rational number $\frac{p}{q} \neq \alpha$, with $p \in \mathbb{Z}$ and $q \in \mathbb{N}$, it is the case that

$$f\left(\frac{p}{q}\right) \neq 0$$

Proof. Let α be an algebraic number, with minimal polynomial $f(x)$ of degree $d \geq 1$. Let $\frac{p}{q} \neq \alpha$ be a rational number, with $p \in \mathbb{Z}$ and $q \in \mathbb{N}$. We claim that $f\left(\frac{p}{q}\right)$ is not equal to zero. To prove this, assume, for a contradiction, that $f\left(\frac{p}{q}\right) = 0$. Then it follows from Theorem 3 that is possible to write $f(x)$ as $f(x) = q(x) \cdot \left(x - \frac{p}{q}\right)$ for some non-zero polynomial $q(x)$ of degree $d-1$. Furthermore, since both $f(x)$ and $x - \frac{p}{q}$ have rational coefficients, the quotient polynomial $q(x)$ must also have rational coefficients (make sure you understand why). But then

$$0 = f(\alpha) = q(x) \cdot \left(\alpha - \frac{p}{q}\right)$$

and since $\alpha - \frac{p}{q} \neq 0$, it must be the case that $q(\alpha) = 0$. Since $q(x)$ is a non-zero polynomial, with rational coefficients, such that $q(\alpha) = 0$, it must be the case that the degree of $q(x)$ cannot be smaller that the degree of the minimal polynomial of α, i.e., $\deg g(x) \geq \deg f(x)$. However, we know that

$$\deg g(x) \; = \; d-1 \; < \; d \; = \; \deg f(x)$$

so we reach a contradiction. Therefore, $f\left(\frac{p}{q}\right) \neq 0$. $\square$

Lemma 2

Let α be an algebraic number with minimal polynomial $f(x)$ of degree $d \geq 1$. Then for every rational number $\frac{p}{q} \neq \alpha$, with $p \in \mathbb{Z}$ and $q \in \mathbb{N}$, it is the case that

$$\left| f\left(\frac{p}{q}\right) \right| \geq \frac{1}{q^n}$$

Proof. Let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ and observe that

$$\begin{aligned} f\left(\frac{p}{q}\right) &= a_d\left(\frac{p}{q}\right)^d + a_{d-1}\left(\frac{p}{q}\right)^{d-1} + \cdots + a_1\cdot\frac{p}{q} + a_0 \\ &= a_d\cdot\frac{p^d}{q^d} + a_{d-1}\cdot\frac{p^{d-1}}{q^{d-1}} + \cdots + a_1\cdot\frac{p}{q} + a_0 \\ &= a_d\cdot\frac{p^d}{q^d} + a_{d-1}\cdot\frac{p^{d-1}q}{q^d} + \cdots + a_1\cdot\frac{pq^{d-1}}{q^d} + a_0\cdot\frac{q^d}{q^d} \\ &= \frac{a_d p^d + a_{d-1}p^{d-1}q + \cdots + a_1 pq^{d-1} + a_0 q^d}{q^d} \\ &= \frac{A}{q^d} \end{aligned}$$

where

$$A = a_d p^d + a_{d-1}p^{d-1}q + \cdots + a_1 pq^{d-1} + a_0 q^d$$

Since p and q are integers, and the coefficients of the minimal polynomial of $f(x)$ are integers, we see that A is an integer. We claim that A is not equal to zero. For suppose not. Then

$$\begin{aligned} 0 &= A \\ &= a_d p^d + a_{d-1}p^{d-1}q + \cdots + a_1 pq^{d-1} + a_0 q^d \\ &= q^d\left(a_d\cdot\frac{p^d}{q^d} + a_{d-1}\cdot\frac{p^{d-1}q}{q^d} + \cdots + a_1\cdot\frac{pq^{d-1}}{q^d} + a_0\cdot\frac{q^d}{q^d}\right) \\ &= q^d f\left(\frac{p}{q}\right) \end{aligned}$$

Since $q^d \neq 0$, it must be the case that $f\left(\frac{p}{q}\right) = 0$, which contradicts our result established in Lemma 1. Therefore, $A \neq 0$, and since A is an integer, we conclude that $|A| \geq 1$. Therefore,

$$\left|f\left(\frac{p}{q}\right)\right| = \frac{|A|}{q^d} \geq \frac{1}{q^d}$$

□

Proof of Theorem 6. Let α be an algebraic number with minimal polynomial $f(x)$ of degree d. Let $\frac{p}{q}$ be a rational number, with $q \in \mathbb{N}$, such that $\alpha \neq \frac{p}{q}$. Notice that if $\left|\alpha - \frac{p}{q}\right| > 1$, then

$$\left|\alpha - \frac{p}{q}\right| > 1 \geq \frac{1}{q^d}$$

So in this situation we can choose $C = 1$. Hence our theorem is true in this case, and so we may assume that $\left|\alpha - \frac{p}{q}\right| \leq 1$, or in other words

$$-1 \ \leq \ \frac{p}{q} - \alpha \ \leq \ 1$$

$$-1 + \alpha \ \leq \ \frac{p}{q} \ \leq \ 1 + \alpha$$

Thus,

$$\left|\frac{p}{q}\right| \leq \max\left(\ |-1+\alpha|, \ |1+\alpha| \ \right) \leq 1 + |\alpha|$$

Let us remember this inequality, as it will become very useful for us later.

Since $f(\alpha) = 0$, it follows from Theorem 3 that $f(x) = (x - \alpha)g(x)$ for some polynomial

$$g(x) = b_{d-1}x^{d-1} + \cdots + b_1 x + b_0$$

Therefore,

$$\left|f\left(\frac{p}{q}\right)\right| = \left|\alpha - \frac{p}{q}\right| \cdot \left|g\left(\frac{p}{q}\right)\right|$$

By Theorem 1, if we let

$$H = \max\left(\ |b_0|, \ |b_1|, \ \ldots, \ |b_{d-1}| \ \right)$$

then

$$\begin{aligned} \left|f\left(\frac{p}{q}\right)\right| &= \left|\alpha - \frac{p}{q}\right| \cdot \left|g\left(\frac{p}{q}\right)\right| \\ \text{Theorem 1} \rightarrow &\leq \left|\alpha - \frac{p}{q}\right| \cdot H \cdot \left(\left|\frac{p}{q}\right|^{d-1} + \cdots + \left|\frac{p}{q}\right| + \ 1 \right) \\ &\leq \left|\alpha - \frac{p}{q}\right| \cdot H \cdot \left(\ (1+|\alpha|)^{d-1} \ + \cdots + \ (1+|\alpha|) + \ 1 \right) \end{aligned}$$

where the last inequality follows from the fact that $\left|\frac{p}{q}\right| \leq 1 + |\alpha|$. If we now let

$$C = \frac{1}{H \cdot \left(\ (1+|\alpha|)^{d-1} \ + \cdots + \ (1+|\alpha|) + \ 1 \ \right)}$$

then it follows from Lemma 2 that

$$\frac{1}{q^d} \ \leq \ \left| f\left(\frac{p}{q}\right) \right| \ \leq \ \left| \alpha - \frac{p}{q} \right| \cdot \frac{1}{C}$$

which means that

$$\left| \alpha - \frac{p}{q} \right| \ \geq \ \frac{C}{q^d}$$

□

Let us apply Theorem 6 to find a positive real number C such that, for every rational number $\frac{p}{q}$ with $p \in \mathbb{Z}$ and $q \in \mathbb{N}$,

$$\left| \sqrt{2} - \frac{p}{q} \right| \geq \frac{C}{q^2}$$

Recall that the minimal polynomial of $\sqrt{2}$ is $f(x) = x^2 - 2$. Notice that

$$f(x) = (x - \sqrt{2})(x + \sqrt{2})$$

If we now let $g(x) = x + \sqrt{2}$, then the height of $g(x)$ is equal to

$$H = \max(\ |1|, \ |\sqrt{2}| \ ) = \sqrt{2}$$

At this point, we apply Theorem 6 to conclude that

$$\left| \sqrt{2} - \frac{p}{q} \right| \geq \frac{C}{q^2}$$

where

$$C = \frac{1}{H \cdot (\ (1+\sqrt{2}) + \ 1 \ )} = \frac{1}{2 + 2\sqrt{2}}$$

Thus, no matter what rational number p/q we choose, the distance between p/q and $\sqrt{2}$ will never be smaller than $\frac{1}{2+2\sqrt{2}} \ q^{-2}$.

Exercise 9

Find a positive real number C such that, for every rational number $\frac{p}{q}$ with $p \in \mathbb{Z}$ and $q \in \mathbb{N}$,

$$\left|\cos(36^\circ) - \frac{p}{q}\right| \geq \frac{C}{q^2}$$

Hint: Note that $\cos(36^\circ) = \frac{1+\sqrt{5}}{4}$.

Exercise 9 Solution

Let us find the minimal polynomial of $\alpha = \frac{1+\sqrt{5}}{4}$. Notice that $4\alpha - 1 = \sqrt{5}$, and if we square both sides, we get $(4\alpha - 1)^2 = 5$, which is equivalent to

$$16\alpha^2 - 8\alpha + 1 = 5$$

Rearranging the terms, we get

$$16\alpha^2 - 8\alpha - 4 = 0$$

Now we are almost done, except that we can make one additional simplification by dividing both sides by 4:

$$4\alpha^2 - 2\alpha - 1 = 0$$

Thus, we see that the minimal polynomial of $\cos(36^\circ)$ is $f(x) = 4x^2 - 2x - 1$. Notice that

$$f(x) = \left(x - \frac{1+\sqrt{5}}{4}\right)\left(4x + \sqrt{5} - 1\right)$$

If we now let $g(x) = 4x + \sqrt{5} - 1$, then the height of $g(x)$ is equal to

$$H = \max(\ |\sqrt{5} - 1|,\ |4|\ \ ) = 4$$

At this point, we apply Theorem 6 to conclude that

$$\left|\cos(36^\circ) - \frac{p}{q}\right| \geq \frac{C}{q^2}$$

where

$$C = \frac{1}{H \cdot (\ (1+\cos(36^\circ)) + \ 1\ )} = \frac{1}{4 \cdot \left(\ 2 + (1+\sqrt{5})/4\ \right)} = \frac{1}{9+\sqrt{5}}$$

§7 An Interesting Criterion for Transcendence

Finally, we are ready to learn about the criterion for transcendence that Liouville discovered. In Theorem 6, we proved that every algebraic number cannot be approximated "too well" by rationals. Thus, if we are able to find a real number r that can be approximated by the rationals very well, then we should be able to prove the existence of transcendental numbers.

Criterion for Transcendence

Let r be a real number. If for every positive integer d and every positive real number C there exists a rational number $\frac{p}{q}$, with $p \in \mathbb{Z}$ and $q \in \mathbb{N}$, such that

$$0 < \left| r - \frac{p}{q} \right| < \frac{C}{q^d}$$

then r is transcendental.

Notice how similar this criterion is to the criterion for irrationality described in §5 of Lesson 1. In 1844, a number L satisfying the above criterion for transcendentality was discovered by Joseph Liouville. Here it is:

$$L = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}} + \frac{1}{10^{4!}} + \frac{1}{10^{5!}} + \cdots$$

Here $n! = 1 \cdot 2 \cdot 3 \cdots n$ denotes the *factorial* function. Notice that

$$L \approx 0.\mathbf{11}000\mathbf{1}00000000000000000\mathbf{1}00000000000000\ldots$$

and that the 1's in the decimal representation of L occur in slots #1, #2, #6, #24, #120, and so on. This is because

$$1! = 1, \qquad 2! = 2, \qquad 3! = 1 \cdot 2 \cdot 3 = 6, \qquad 4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24, \qquad 5! = 120, \qquad \ldots$$

If we denote

$$L_1 = \frac{1}{10^{1!}}, \qquad L_2 = \frac{1}{10^{1!}} + \frac{1}{10^{2!}}, \qquad L_3 = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}}, \qquad \ldots$$

then the numbers $L_1, L_2, L_3, \ldots$ are all rational and they approximate L so well that L satisfies the criterion for trasncendence.

Figure 3: Joseph Liouville (1809–1882)

Since Liouville, a lot advances have been made in Transcedental Number Theory. For example, Cantor proved that, in fact, there's many more transcendental numbers than algebraic numbers. More precisely, he showed that it is impossible to *count* transcendental numbers, meaning that we cannot align them in a sequence (1st, 2nd, 3rd, and so on) and this way count all of them. Perhaps surprisingly, this *is* possible to do for algebraic numbers.

In the last quarter of the 19th century, Lindemann-Weierstrass Theorem was established, which enabled mathematicians to show that the numbers $\pi \approx 3.14$ and $e \approx 2.72$ are transcendental.

Exercise 10

Use the fact that π is transcendental to prove that π^n is transcendental for every positive integer n.

Exercise 10 Solution

Let n be a positive integer. Assume, for a contradiction, that there exists a non-zero polynomial $f(x)$, with rational coefficients, such that $f(\pi^n) = 0$. Let $g(x) = f(x^n)$. Then $g(x)$ is also a non-zero polynomial with rational coefficients. Furthermore,

$$g(\pi) = f(\pi^n) = 0$$

Since there exists a non-zero polynomial $g(x)$, with rational coefficients, such that $g(\pi) = 0$, it must be the case that π is algebraic. Thus, we reach a contradiction, and so π^n is a transcendental number.

Another important theorem in the field, called the Gelfond-Schneider Theorem, was proved independently in 1934 by a Soviet mathematician Aleksandr Gelfond and a German mathematician Theodor Schneider. Below is a variant of their result.

Theorem 7 (A Variant of Gelfond-Schneider Theorem)

If $v > 0$ and w are real algebraic numbers, with $v \neq 1$ and w irrational, then v^w is a transcendental number.

With this theorem, it became possible to prove that the numbers $\sqrt{2}^{\sqrt{2}} \approx 1.63$ and $e^{\pi} \approx 23.14$ are transcendental. You can also use it to prove that certain values of the logarithms $\log_a b$ are transcendental.

Exercise 11

Let $a \geq 2$ and $b \geq 2$ be integers such that $b \neq \sqrt[n]{a^m}$ for all $m, n \in \mathbb{N}$. Use Theorem 7 to prove that $\log_a b$ is transcendental.

Hint: Apply the result from Lesson 1, §3, Exercise 5.

Exercise 11 Solution

Let $a \geq 2$ and $b \geq 2$ be integers such that $b \neq \sqrt[n]{a^m}$ for all $m, n \in \mathbb{N}$. Then it follows from Exercise 3 of §3 Lesson 1 that $w = \log_a b$ is irrational. Further, if we let $v = a$, then $v > 0$, $v \neq 1$ and v is algebraic, because every integer is an algebraic number. Now, assume, for a contradiction, that $w = \log_a b$ is algebraic. Then it follows from Theorem 7 that $v^w = a^{\log_a b} = b$ is transcendental, which is false, because b is an integer. Thus, $w = \log_a b$ is not algebraic, meaning that it must be transcendental.

Despite all of these advances, there are still many questions in Transcendental Number Theory that remain open. For example, in Lesson 1 you've learned about Apéry's constant

$$A = 1 + \frac{1}{2^3} + \frac{1}{3^3} + \frac{1}{4^3} + \cdots \approx 1.202$$

While we do know that A is irrational, we still don't know if it is transcendental or not. It is known, however, that the number $1 + 2^{-s} + 3^{-s} + 4^{-s} + \cdots$ is transcendental for *every* even integer $s \geq 2$.