Transcendental Numbers

Benjamin Church

December 3, 2022

Contents

1 Introduction

The rational numbers ($\mathbb{Q}$) are incomplete in two different ways. Firstly, $\mathbb{Q}$ is not algebraically closed because there exist polynomials with rational coeficients which have no roots in $\mathbb{Q}$. For example, $x^2 - 2 = 0$. Furthermore, $\mathbb{Q}$ is not complete because there are sequences of rational numbers which converge in the real numbers but not in the rational numbers. For example, let F_n be the n-th Fibonacci number then $\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \varphi$ where $\varphi = \frac{1+\sqrt{5}}{2} \notin \mathbb{Q}$. If we complete $\mathbb{Q}$ by adding in the limit of every sequence, we get the real numbers $\mathbb{R}$. If take the algebraic closure of $\mathbb{Q}$ by adding in the roots of every polynomial with coeficients in $\mathbb{Q}$ we get the algebraic numbers $\bar{\mathbb{Q}}$. The relationship between these two sets was of great historically importance. In particular, $\bar{\mathbb{Q}}$ contains complex numbers (for example i solves $x^2 + 1 = 0$) and $\mathbb{R}$ does not. The question arises, is $\mathbb{R}$ contained in $\bar{\mathbb{Q}}$. Equivalently, does there exist a non-algebraic real number. Such a number is called *transcendental* because the number "transcends" algebraic definition.

2 Algebraic Numbers and Cantor's Theorem

Definition: $\mathbb{Q}[X]$ is the set of polynomials with coeficients in $\mathbb{Q}$ and $\mathbb{Z}[X]$ is the set of polynomials with coeficients in Z.

Definition: A complex number $\alpha \in \mathbb{C}$ is *algebraic* if there exists a polynomial $f \in \mathbb{Q}[X]$ such that $f(\alpha) = 0$. Otherwise, α is *transcendental.*

Proposition. $\alpha \in \mathbb{C}$ is algebraic iff there exists a polynomial $f \in \mathbb{Z}[X]$ with *integer* coeficients such that $f(\alpha) = 0$.

Proof. Let $\alpha \in \mathbb{C}$ be a root of a polynomial $f \in \mathbb{Z}[X]$. Because $\mathbb{Z} \subset \mathbb{Q}$ then $\mathbb{Z}[X] \subset \mathbb{Q}[X]$ so $f \in \mathbb{Q}[X]$ so α is algebraic. Conversely, let $\alpha \in \mathbb{C}$ be algebraic. Then α is the root of some polynomial with rational coeficients,

$$\begin{aligned} f(\alpha) &= \frac{p_n}{q_n}\alpha^n + \cdots + \frac{p_1}{q_1}\alpha + \frac{p_0}{q_0} \\ &= p_n(q_{n-1}q_{n-2}\cdots q_0)\alpha^n + \cdots p_1(q_nq_{n-1}\cdots q_2q_0)\alpha + p_0(q_nq_{n-1}\cdots q_2q_1) \\ &= 0 \end{aligned}$$

Therefore, α is the root of a polynomial with coeficients in $\mathbb{Z}$. □

Definition: Let $\alpha \in \mathbb{C}$ be algebraic. The degree of α, denoted as $\deg \alpha$, is the minimum degree of a polynomial $f \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$.

Definition: A function $f : X \to Y$ is a *surjection* if for every $y \in Y$ there exists $x \in X$ such that $f(x) = y$.

Definition: A set X is *countable* if there is a surjection $f : \mathbb{N} \to X$. Otherwise, X is *uncountable.* Such a function is called a list of X.

Definition: The set $\bar{\mathbb{Q}} \subset \mathbb{C}$ is the set of algebraic numbers. That is, given a complex number $\alpha \in \mathbb{C}$ then $\alpha \in \bar{\mathbb{Q}}$ if any only if α is the root of some rational polynomial $p \in \mathbb{Q}[X]$.

Theorem 2.1. $\bar{\mathbb{Q}}$ *is countable.*

Proof. Every polynomial has a finite number of roots so it suffices to show that we can list all polynomials with integer coeficients. The list goes as follows, list all polynomials with degree less than n and coeficients with absolute value less than n. There are a finite number of such polynomials so we will list every polynomial by incimentally increasing n. This is surjective becuase given a polynomial of degree n there are a finite number of polynomials with smaller degree and smaller coeficients so the function will reach this given polynomial in a finite number of steps. $\square$

Theorem 2.2 (Cantor)**.** $\mathbb{R}$ *is uncountable.*

Proof. This is a classic proof by contradiction. Suppose I had such a function $f : \mathbb{N} \to \mathbb{R}$. Now, I will construct some $r \in \mathbb{R}$ not in the image of f. For simplicty let us only take real numbers on the interval $[0, 1]$ this will suffice. Let r_i be the i-th digit of r in some base b. Define the number $s \in \mathbb{R}$ by its expansion base b as $s_i = f(i)_i + 1 \bmod b$. This is the i-th digit of the i-th number plus one reduced by b. I claim that there does not exist any $n \in \mathbb{N}$ such that $f(n) = s$. Suppose such and n exists. Then $s_n = f(n)_n + 1 \bmod b$ but $s = f(n)$ so $s_n = f_n$ which is a contradiction. Therefore, f cannot be a bijection. $\square$

corollary 2.3. *Transcendental numbers exist.*

Proof. If $\mathbb{R} \subset \bar{\mathbb{Q}}$ then because $\bar{\mathbb{Q}}$ is countable then $\mathbb{R}$ would be countable because any sujection onto $\bar{\mathbb{Q}}$ can be reduced to a surjection onto $\mathbb{R}$ by mapping every $x \in \bar{\mathbb{Q}}$ such that $x \notin \mathbb{R}$ to some fixed point of $\mathbb{R}$. However, $\mathbb{R}$ is uncountable so there must be some $r \in \mathbb{R}$ such that $r \notin \bar{\mathbb{Q}}$. $\square$

3 Diophantine Approximation

Definition: For $\alpha \in \mathbb{R}$, an n-*good* Diophantine approximation is $\frac{p}{q} \in \mathbb{Q}$ so that,

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n}$$

Definition: A number $\alpha \in \mathbb{R}$ is n-*approximable* if there exist infinitely many n-good Diophantine approximations.

Definition:

$$G_n(\alpha) = \left\{ \frac{p}{q} \in \mathbb{R} \mid 0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n} \right\}$$

the set of n-good approximations of α. α is n-approximable when $|G_n(\alpha)| = \infty$.

Lemma 3.1. *Let α be a root of $f \in \mathbb{Z}[X]$ with $\deg f = n$ then there exists $C \in \mathbb{R}^+$ such that for every $\frac{p}{q} \in \mathbb{Q}$ such that $\frac{p}{q} \neq \alpha$ we have,*

$$\left|\alpha - \frac{p}{q}\right| > \frac{C}{q^n}$$

Proof. Let $f(x) = a_n x^n + \cdots + a_0$ with coeficients $a_i \in \mathbb{Z}$. Take $f(\alpha) = 0$. There are at most n roots of f labled $\alpha_1, \alpha_n, \cdots, \alpha_k$ and α. Define,

$$r = \min\{|\alpha - \alpha_1|, |\alpha - \alpha_2|, \ldots, |\alpha - \alpha_k|\}$$

Therefore, f has no roots except α on the interval $(\alpha - r, \alpha + r)$. Define,

$$M = \max\{|f'(x)| \mid x \in (\alpha - r, \alpha + r)\}$$

and take any positive real number $C < \min\{r, \frac{1}{M}\}$. Now, take any $\frac{p}{q} \in \mathbb{Q}$ with $\frac{p}{q} \neq \alpha$. If $\left|\alpha - \frac{p}{q}\right| > C > \frac{C}{q^n}$ then we are done. Otherwise, $\left|\alpha - \frac{p}{q}\right| \leq C \leq r$ so $\frac{p}{q} \in (\alpha - r, \alpha + r)$ but $\alpha \neq \frac{p}{q}$ so $f(\frac{p}{q}) \neq 0$ because there are no other roots on this interval. Consider,

$$q^n f\left(\frac{p}{q}\right) = a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_0 q^n \in \mathbb{Z}$$

However, $q^n f(\frac{p}{q}) \neq 0$ so $|q^n f(\frac{p}{q})| \geq 1$ because it is a nonzero positive integer. Thus, $|f(\frac{p}{q})| \geq \frac{1}{q^n}$. By the mean value theorem, there exists $\xi \in (\alpha, \frac{p}{q}) \subset (\alpha - r, \alpha + r)$ such that,

$$f'(\xi) = \frac{f(\frac{p}{q}) - f(\alpha)}{\frac{p}{q} - \alpha}$$

Therefore,

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

However, $|f'(\xi)| \leq M$ and $|f(\frac{p}{q})| \geq \frac{1}{q^n}$ so,

$$\left|\alpha - \frac{p}{q}\right| = \left|\frac{f(\frac{p}{q})}{f'(\xi)}\right| \geq \frac{1}{M q^n} > \frac{C}{q^n}$$

□

corollary 3.2. *Let α be algebraic with degree n, then for any $k > n$, α is not k-approximable.*

Proof. Suppose that $k > n$ and α is k-approximable then $G_k(\alpha)$ is infinite and thus must contain $\frac{p}{q}$ with arbitrarily large q. Therefore, given any $C \in \mathbb{R}^+$ we can choose $\frac{p}{q} \in G_k(\alpha)$ such that $q^{k-n} > C$ which is possible because $k - n > 0$. Then, because $\frac{p}{q} \in G_k(\alpha)$,

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^k} = \frac{C}{q^n} \cdot \frac{C}{q^{n-k}} < \frac{C}{q^n}$$

Since $\frac{p}{q} \neq \alpha$, this contradicts the previous lemma because α is a root to some $f \in Z[X]$ with $\deg f = n$. However, there could not exist any $C \in \mathbb{R}^+$ such that,

$$\left|\alpha - \frac{p}{q}\right| > \frac{C}{q^n}$$

for every $\frac{p}{q} \in \mathbb{Q}$ with $\frac{p}{q} \neq \alpha$. Thus, α is not n-approximable. □

4 Irrationality Measure

We can use the previous definitions and results to define a measure of how irrational a number is. Essentially, the irrationality measure tells us how well a number can be approximated by rational numbers. Perhaps unintuitively, the more irrational the number, the *better* it can be approximated by rationals.

Definition: The *irrationality measure* is $\mu(\alpha) = \sup\{n \in \mathbb{R}^+ \mid |G_n(\alpha)| = \infty\}$

Proposition. Let α be algebraic of degree n, then $\mu(\alpha) \leq n$.

Proof. Suppose that $\mu(\alpha) > n$. Then there would exist some $k > n$ such that $|G_k(\alpha)| = \infty$ else the supremum would be n. However, $\mu(\alpha)$ is algebraic of order n and $k > n$ so α is not k-approximable. Therefore, $\mu(\alpha) \leq n$. □

Proposition. If $\alpha \in \mathbb{Q}$ then $\mu(\alpha) = 1$

Proof. Take $\epsilon < 1$ and $\alpha = \frac{p}{q}$. Then, for any $n \in \mathbb{N}$ consider $p_n = np + 1$ and $q_n = nq$. Now, $\alpha - \frac{p_n}{q_n} = \frac{np - p_n}{nq} = \frac{1}{nq} = \frac{1}{q_n}$. Also, $q_n^\epsilon < q_n$. Therefore,

$$0 < \left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n} < \frac{1}{q_n^\epsilon}$$

Also, $\frac{p_n}{q_n} = \frac{p}{q} + \frac{1}{nq}$ so these solutions are all distinct. Thus, there are infinitely many ϵ-good approximations of α so $\mu(\alpha) \geq \epsilon$ for every $\epsilon < 1$ so $\mu(\alpha) \geq 1$. Futhermore, $\alpha = \frac{p}{q}$ solves $f(x) = qx - p$ which has degree 1 so $\mu(\alpha) \leq 1$. Therefore, $\mu(\alpha) = 1$. □

Theorem 4.1 (Roth, 1955)**.** *If α is algebraic then $\mu(\alpha) = 2$.*

Klaus Roth was awarded the Fields Medal for the proof of this theorem. Needless to say, we will not prove it here.

Example 4.1. The best known upper bound on the irrationality measure of π was given in 2008 by Salikhov as $\mu(\pi) \leq 7.6063$

Example 4.2. Borwein and Borwein proved in 1987 that $\mu(e) = 2$.

5 Liouville Numbers

Definition: L is a *Liouville number* if for every $n \in \mathbb{Z}^+$ there exists $\frac{p}{q} \in \mathbb{Q}$ such that,

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n}$$

Proposition. L is Liouville if and only if $\mu(L) = \infty$

Proof. Let $\mu(L) = \infty$. then for any $n \in \mathbb{Z}^+$ there must be a $k > n$ such that L is k-approximable because $\mu(L) > n$. Therefore, there is a solution $\frac{p}{q} \in \mathbb{Q}$ (in fact infinitely many) to the inequality,

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^k} < \frac{1}{q^n}$$

so L is Liouville. Conversely, suppose that L is Liouville. Then take any k and choose $n > k$ with $n \in \mathbb{Z}^+$. Because L is Liouville, for each n there must be a solution $\frac{p_n}{q_n} \in \mathbb{Q}$ to,

$$0 < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{p_n^n} < \frac{1}{p_n^k}$$

Therefore, each $\frac{p_n}{q_n} \in G_k(L)$. I claim that this is an infinite number of distinct solutions. Otherwise, there would be a single value $\frac{p'}{q'}$ which appears infinitely many times. Thus,

$$0 < \left|\alpha - \frac{p'}{q'}\right| < \frac{1}{(q')^n}$$

for infinitely many values of $n \in \mathbb{Z}^+$ which is impossible because,

$$\left|\alpha - \frac{p'}{q'}\right| \neq 0$$

but $\frac{1}{(q')^n} \to 0$. Therefore, $|G_k(L)|$ is infinite for every $k \in \mathbb{R}^+$. Thus, $\mu(L) \geq k$ for all $k \in \mathbb{R}^+$ so $\mu(L) = \infty$. □

Theorem 5.1. *Liouville numbers are trancendental.*

Proof. Let L be algebraic then there exists some $f \in Z[X]$ such that $f(L) = 0$. However, then $\mu(L) \leq \deg f$ which is finite so $\mu(L) < \infty$ and thus L is not Liouville. Thus, if L is Liouville, then L is not algebraic so L is trancendental. □

Theorem 5.2. *Take $b \in \mathbb{Z}$ with $b \geq 2$ and $a_k \in \{0, 1, 2, \cdots, b-1\}$ for every $k \in \mathbb{N}$, then, the number,*

$$L = \sum_{k=1}^{\infty} \frac{a_k}{b^{k!}}$$

is Liouville number and thus trancendental. In particular, we have uncountably many explict examples of trancendental numbers.

Proof. Let $q_n = b^{n!}$ and $p_n = q_n \sum_{k=1}^{n} \frac{a_k}{b^{k!}}$ then,

$$0 < \left|\alpha - \frac{p}{q}\right| = \sum_{k=n+1}^{\infty} \frac{a_k}{b^{k!}} < \sum_{k'=(n+1)!}^{\infty} \frac{a_k}{b^{k'}} \leq \sum_{k'=(n+1)!}^{\infty} \frac{b-1}{b^{k'}} = \frac{b-1}{b^{(n+1)!}} \sum_{k=0}^{\infty} \frac{1}{b^k}$$
$$= \frac{b-1}{b^{(n+1)!}} \frac{b}{b-1} = \frac{b}{b^{(n+1)!}} \leq \frac{b^{n!}}{b^{(n+1)!}}$$

Now, $(n+1)! - n! = (n+1) \cdot n! - n! = n \cdot n!$ and thus,

$$0 < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{b^{n!}}{b^{(n+1)!}} = \frac{1}{b^{n \cdot n!}} = \frac{1}{(b^{n!})^n} = \frac{1}{q_n^n}$$

Therefore, the inequality,

$$0 < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^n}$$

has a solution for every integer n. For any k we can take an integer $n > k$ such that,

$$0 < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^n} < \frac{1}{q_n^k}$$

has a solution. □