ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Introduction to Transcendental Numbers

Student Seminar Presentation

Romeo Schilling

October 28, 2021

Lecturer: Özlem Imamoglu

Department of Mathematics, ETH Zürich

Abstract

This report includes a very brief introduction to transcendental numbers, punctuated by some historical notes and some open problems. By no means is it meant to be an exhaustive survey, and in that regard it cannot reflect all the depth of the subject.

Of course, only a small part of the material summarized in this report will be discussed in the 45-minute talk: I will try to choose what can best be explained in the allotted time, avoiding too many technical details and barely mentioning the most general or accurate version of any presented result.

"Run to brilliance. Sprint to excellence. Soar to transcendence." — Matshona Dhliwayo

Contents

Chapter 1

Introduction

Although Leonhard Euler wrote that transcendental numbers "transcend the power of algebraic methods", any result about transcendental numbers is linked to those about algebraic numbers and quite often uses tools of algebra to be proven. Since a transcendental number is defined by what it is not, i.e. an algebraic number, there is this indeniable and interesting duality between those two concepts. For example, if one succeeds to prove a necessary, respectively a sufficient condition for a number to be algebraic, one will have directly gained a sufficient, respectively a necessary condition for a number to be transcendental.

1.1 Recap of Some Algebraic Concepts

All the following concepts have been discussed in our algebra courses. But we will repeat a few of them here.

1.1.1 Algebraic Numbers

Definition 1.1 *(Algebraic numbers) A complex number $\alpha \in \mathbb{C}$ is called an* algebraic number *if α is an algebraic element over the field $\mathbb{Q}$.*
In other words, a complex number $\alpha \in \mathbb{C}$ is an algebraic number if there exists (at least) one non-zero polynomial with rational coefficients $f = f(X) \in \mathbb{Q}[X]$ which has α as a root, i.e.

$$\exists\, n \in \mathbb{N}^{\geq 0} \text{ and } \exists\, a_0, a_1, a_2, \ldots, a_n \in \mathbb{Q} \text{ with } (a_0, a_1, \ldots, a_n) \neq (0, 0, \ldots, 0),$$
$$\text{such that } f(\alpha) = a_n\alpha^n + \ldots + a_1\alpha + a_0 = 0$$

Or, equivalently, a complex number $\alpha \in \mathbb{C}$ is an algebraic number if there exists (at least) one non-constant[1] *polynomial with rational coefficients $f = f(X) \in \mathbb{Q}[X]$*

[1] If $\alpha = 0$, take $f = f(X) = X$ which is a non-constant polynomial; otherwise, if $\alpha \neq 0$, then we certainly cannot have $n = 0$ or else $f(\alpha) = a_0 = 0 \Longrightarrow f \equiv 0$.

which has α as a root, i.e.

$$\exists\, n \in \mathbb{N}^{\geq 1} \text{ and } \exists\, a_0, a_1, a_2, \ldots, a_n \in \mathbb{Q} \text{ with } a_n \neq 0,$$
$$\text{such that } f(\alpha) = a_n\alpha^n + \ldots + a_1\alpha + a_0 = 0$$

The subset of $\mathbb{C}$ consisting of all algebraic numbers is usually denoted by

$$\mathbb{A} := \{\alpha \in \mathbb{C} \mid \alpha \text{ is an algebraic element over } \mathbb{Q}\}$$

and is in fact a subfield of $\mathbb{C}$.

Remark 1.2 *We can prove that $\mathbb{A}$ is an algebraic closure of $\mathbb{Q}$, which is why certain authors use the notation $\overline{\mathbb{Q}}$ instead of $\mathbb{A}$.*

Proposition 1.3 *(Minimal polynomial) For each $\alpha \in \mathbb{A}$, there exists a* unique *polynomial, denoted $irr_{\alpha,\mathbb{Q}} = irr_{\alpha,\mathbb{Q}}(X)$, which satisfies the following properties:*

(i) $irr_{\alpha,\mathbb{Q}} \in \mathbb{Q}[X]$*, i.e. its coefficients are rational*

(ii) $irr_{\alpha,\mathbb{Q}}$ *is monic, i.e. its leading coefficient is equal to 1*

(iii) $irr_{\alpha,\mathbb{Q}}(\alpha) = 0$ *, i.e. it has α as a root*

(iv) $irr_{\alpha,\mathbb{Q}}$ *has the lowest possible degree (which is necessarily greater or equal to 1) among all polynomials satisfying properties (i) to (iii).*

We call $irr_{\alpha,\mathbb{Q}}$ the minimal polynomial *of α over $\mathbb{Q}$.*

To characterize the minimal polynomial $irr_{\alpha,\mathbb{Q}}$ of an algebraic number α over $\mathbb{Q}$, it only needs to satisfy properties (i) to (iii) as well as the following property:

(iv)' $irr_{\alpha,\mathbb{Q}}$ *is irreducible in $\mathbb{Q}[X]$.*

Remark 1.4 *We can prove that for an algebraic number $\alpha \in \mathbb{A}$ and for any polynomial $f \in \mathbb{Q}[X]$ with rational coefficients, we have the equivalence:*

$$\alpha \text{ is a root of } f \iff irr_{\alpha,\mathbb{Q}} \text{ divides } f \text{ in } \mathbb{Q}[X]$$

Definition 1.5 *(Degree of an algebraic number) We say that $\alpha \in \mathbb{A}$ is of degree n (necessarily $n \geq 1$) if*

$$deg(irr_{\alpha,\mathbb{Q}}) = n,$$

i.e. if the degree of the minimal polynomial of α over $\mathbb{Q}$ is finite and equal to n.
We write: $deg(\alpha) = n$.

Remark 1.6 *One can prove that for $\alpha \in \mathbb{A}$:*

$$deg(irr_{\alpha,\mathbb{Q}}) = n \iff [\mathbb{Q}(\alpha) : \mathbb{Q}] = n,$$

i.e. the degree of the simple field extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is finite and equal to n.
In this case, the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ has for $\mathbb{Q}$-basis the set

$$\left\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\right\}$$

i.e. any $x \in \mathbb{Q}(\alpha)$ can be written as a unique linear combination of the elements $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ over $\mathbb{Q}$, that is:

$$x = \sum_{i=0}^{n-1} \lambda_i \alpha^i \text{ for some unique } \lambda_i \in \mathbb{Q} \ (i = 0, 1, \ldots, n-1)$$

Proposition 1.7 *Let $\alpha \in \mathbb{A}$ be complex algebraic number. Then we have:*

$$deg(\alpha) = 1 \Longleftrightarrow \alpha \in \mathbb{Q}$$

In particular, the degree of a real *algebraic number is strictly more than 1 if and only if α is an irrational number.*

Proof One direction is obvious: if $\alpha \in \mathbb{Q}$, then $f = f(X) := X - \alpha$ satifies properties (i) to (iv) of Proposition 1.3, hence $irr_{\alpha,\mathbb{Q}} = f$, which implies that α has degree 1.
For the other direction, suppose that α has degree 1, which means that $irr_{\alpha,\mathbb{Q}} = aX + b$ for some $a, b \in \mathbb{Z}$ with $a \neq 0$. But $0 = irr_{\alpha,\mathbb{Q}}(\alpha) = a\alpha + b$ implies that $\alpha = \frac{-b}{a} \in \mathbb{Q}$. □

Definition 1.8 *(Algebraic conjugates of an algebraic number) For a complex algebraic number $\alpha \in \mathbb{A}$, we call the (complex) roots of the minimal polynomial of α over $\mathbb{Q}$ the* algebraic conjugates *of α.*

Remark 1.9 *Since $char(\mathbb{Q}) = 0$, any polynomial in $\mathbb{Q}[X]$ is necessarily separable (i.e. each of its irreducible factors in $\mathbb{Q}[X]$ has no repeated roots). Hence, for any $\alpha \in \mathbb{A}$ of degree n, its minimal polynomial $irr_{\alpha,\mathbb{Q}}$ has exactly n distinct (complex) roots, which means that α has exactly n* distinct *algebraic conjugates.*

Example 1.10 *The golden ratio $\varphi := \frac{1+\sqrt{5}}{2}$ is an algebraic number of degree 2, because its minimal polynomial can be proven to be*

$$irr_{\varphi,\mathbb{Q}} = irr_{\varphi,\mathbb{Q}}(X) = X^2 - X - 1$$

The number $\frac{1-\sqrt{5}}{2}$ is the other algebraic conjugate of φ.

Proposition 1.11 *We have the equivalence:*

$$\alpha \in \mathbb{A} \Longleftrightarrow \mathfrak{Re}(\alpha) \in \mathbb{A} \text{ and } \mathfrak{Im}(\alpha) \in \mathbb{A},$$

i.e. a number is algebraic if and only if its real and imaginary parts are algebraic numbers.

Proof One direction is obvious, because if $\mathfrak{Re}(\alpha) \in \mathbb{A}$ and $\mathfrak{Im}(\alpha) \in \mathbb{A}$, and since obviously $i \in \mathbb{A}$ (with minimal polynomial $irr_{i,\mathbb{Q}} = X^2 + 1$), then it follows that $\alpha = \mathfrak{Re}(\alpha) + i\,\mathfrak{Im}(\alpha)$ remains in the field $\mathbb{A}$, as a sum and product of elements of $\mathbb{A}$.

For the other direction, let α be an algebraic number, i.e. it is a root of a non-constant polynomial f with rational coefficients. But we know that any polynomial with real coefficients has the property that if it has a complex root, then it also has as root the complex conjugate of this complex root. Therefore, since $f \in \mathbb{Q}[X] \subseteq \mathbb{R}[X]$ and since $f(\alpha) = 0$, then $\overline{\alpha}$ is also a root of f, implying that $\overline{\alpha}$ is also an algebraic number. Therefore, since $\mathbb{A}$ is a field containing both $\alpha, \overline{\alpha}$ and i, it certainly contains the elements $\frac{\alpha+\overline{\alpha}}{2} = \mathfrak{Re}(\alpha)$ and $\frac{\alpha-\overline{\alpha}}{2i} = \mathfrak{Im}(\alpha)$, as desired.
In fact, for any algebraic number $\alpha \in \mathbb{A}$, we have:

$$irr_{\alpha,\mathbb{Q}} = irr_{\overline{\alpha},\mathbb{Q}}$$

Indeed, since $\alpha \in \mathbb{C}$ is a root of $irr_{\alpha,\mathbb{Q}} \in \mathbb{Q}[X] \subseteq \mathbb{R}[X]$, then $\overline{\alpha}$ is also a root of $irr_{\alpha,\mathbb{Q}}$. So, by Remark 1.4, since $irr_{\alpha,\mathbb{Q}}(\overline{\alpha}) = 0$, we have that $irr_{\overline{\alpha},\mathbb{Q}}$ divides $irr_{\alpha,\mathbb{Q}}$ in $\mathbb{Q}[X]$. Similarly, we deduce that $irr_{\alpha,\mathbb{Q}}$ divides $irr_{\overline{\alpha},\mathbb{Q}}$ in $\mathbb{Q}[X]$. Hence those two polynomials $irr_{\alpha,\mathbb{Q}}$ and $irr_{\overline{\alpha},\mathbb{Q}}$ are associated in $\mathbb{Q}[X]$, i.e. differ by only a unit of $\mathbb{Q}$ (because the set of units of $\mathbb{Q}[X]$ is just the set of constant and non-zero polynomials of $\mathbb{Q}[X]$, which is isomorphic to $\mathbb{Q}^\times$). Since $irr_{\alpha,\mathbb{Q}}$ and $irr_{\overline{\alpha},\mathbb{Q}}$ are both monic, they are equal. □

Remark 1.12 *From the proof of Proposition 1.11, we can highlight the fact that: if α is an algebraic number, then $\overline{\alpha}$ is also an algebraic number with the same minimal polynomial over $\mathbb{Q}$, namely $irr_{\alpha,\mathbb{Q}} = irr_{\overline{\alpha},\mathbb{Q}}$.*
Similarly, if α and β are algebraic numbers such that β is an algebraic conjugate of α, then they have the same minimal polynomial, namely $irr_{\alpha,\mathbb{Q}} = irr_{\beta,\mathbb{Q}}$.

Proposition 1.13 *If α is an algebraic number of degree $n \geq 1$, then $\mathfrak{Re}(\alpha)$ is algebraic number of degree m with $1 \leq m \leq n$.*

Proof It follows from Proposition 1.11, since $\alpha \in \mathbb{A}$, that the real number $\mathfrak{Re}(\alpha) \in \mathbb{A}$ is also an algebraic number with degree say $m \geq 1$.
Since α is of degree n, let $\alpha_1 := \alpha, \alpha_2, \ldots, \alpha_n$ be the n distinct algebraic conjugates of α (see Remark 1.9).
Consider the following polynomial of degree n:

$$g = g(X) := \prod_{i=1}^{n} [2X - (\alpha_i + \overline{\alpha_i})]$$

Since $\alpha_i + \overline{\alpha_i} = 2\,\mathfrak{Re}(\alpha_i) \in \mathbb{R}$, the polynomial g has real coefficients. We certainly have that $g(\mathfrak{Re}(\alpha)) = g(\mathfrak{Re}(\alpha_1)) = g(\frac{1}{2}(\alpha_1 + \overline{\alpha_1})) = 0$. If we can further verify that g is a polynomial in $\mathbb{Q}[X]$, then by Remark 1.4, the minimal polynomial of $\mathfrak{Re}(\alpha)$ over $\mathbb{Q}$ satisfies:

$$irr_{\mathfrak{Re}(\alpha),\mathbb{Q}} \text{ divides } g \text{ in } \mathbb{Q}[X].$$

Hence, we deduce, as desired, that $deg(irr_{\mathfrak{Re}(\alpha),\mathbb{Q}}) \leq deg(g)$, that is $m \leq n$, because $\mathfrak{Re}(\alpha)$ and g are respectively of degree m and n.

To prove that $g \in \mathbb{Q}[X]$, we need some Galois Theory. Let f be the minimal polynomial of α over $\mathbb{Q}$, and let E be the splitting field of this polynomial, i.e.

$$E = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$$

Since all α_i's are algebraic over $\mathbb{Q}$, we even have:

$$E = \mathbb{Q}[\alpha_1, \ldots, \alpha_n]$$

Recall that f is also the minimal polynomial of α_i and, by Remark 1.12, of $\overline{\alpha_i}$ for $i = 1, \ldots, n$, and so the field E certainly contains α_i and $\overline{\alpha_i}$ for $i = 1, \ldots, n$. We claim that the coefficients of g will remain unchanged under any permutation of the α_i's.
Indeed, for $n = 1$, this is trivial, because then α being of degre $n = 1$ is rational (by Proposition 1.7), hence we have in particular that $\overline{\alpha} = \alpha$, implying that:

$$g = g(X) = (2X - (\alpha + \overline{\alpha})) = (2X - 2\alpha),$$

which certainly remains unchanged under any permutation of the set $\{\alpha\}$.
For $n = 2$, we have:

$$g = g(X) = (2X - (\alpha_1 + \overline{\alpha_1})) \cdot (2X - (\alpha_2 + \overline{\alpha_2}))$$

Since both $\overline{\alpha_1}$ and $\overline{\alpha_2}$ are roots of f, we must have:

$$\overline{\alpha_1}, \overline{\alpha_2} \in \{\alpha_1, \alpha_2\}$$

We cannot have $\overline{\alpha_1} = \overline{\alpha_2}$, otherwise this would imply that $\alpha_1 = \alpha_2$, which is a contradiction, because all algebraic conjugates of α are distinct.
Case 1: $\overline{\alpha_1} = \alpha_1$ and $\overline{\alpha_2} = \alpha_2$, in which case:

$$g = (2X - 2\alpha_1) \cdot (2X - 2\alpha_2)$$

Case 2: $\overline{\alpha_1} = \alpha_2$ and $\overline{\alpha_2} = \alpha_1$, in which case:

$$g = (2X - (\alpha_1 + \alpha_2)) \cdot (2X - (\alpha_2 + \alpha_1))$$

In both cases, any permutation of the α_i's leaves g unchanged.
The proof of the general case $n \geq 3$ is similar.
Now consider the Galois group of f, i.e. the group of all field automorphisms of E leaving $\mathbb{Q}$ fixed:

$$Gal(f) := Gal(E/\mathbb{Q}) = \{\sigma \in Aut(E) \text{ such that } \sigma|_{\mathbb{Q}} = Id_{\mathbb{Q}}\}$$

We know that any element $\sigma \in Gal(f)$ permutes the roots of f, which are by definition the algebraic conjugates of α, and in fact any $\sigma \in Gal(f)$ is totally determined by its values at the algebraic conjugates of α. This result comes from the existence of a well-known injective group homomorphism Φ from

the Galois group $Gal(f)$ to the set of all permutations of the set of the roots of f, namely $\mathcal{R}_E(f) := \{\beta \in E \mid f(\beta) = 0\}$, given by:

$$\begin{array}{rccc} \Phi & : & Gal(f) & \hookrightarrow & \mathcal{S}_{\mathcal{R}_E(f)} \\ & & \sigma & \mapsto & \sigma\Big|_{\mathcal{R}_E(f)} \end{array}$$

Therefore, a permutation of the roots α_i's corresponds to the natural action of a field automorphim $\sigma \in Gal(f)$ restricted to the set $\mathcal{R}_E(f)$. To each such σ, corresponds a unique ring automorphism $\sigma^* : E[X] \to E[X]$ which sends X to X and sends any element x of E to $\sigma(x)$. Hence:

$$\sigma^*(g) = \prod_{i=1}^{n}[\sigma(2) \cdot \sigma(X) - (\sigma(\alpha_i) + \sigma(\overline{\alpha_i}))] = \prod_{i=1}^{n}[2X - (\sigma(\alpha_i) + \sigma(\overline{\alpha_i}))] = g$$

because, as we have seen, g remains unchanged under any permutation of the α_i's (which include all the $\overline{\alpha_i}$'s).
Since $\sigma^*(g) = g$, then, if we set

$$g = g(X) = b_nX^n + b_{n-1}X^{n-1} + \ldots + b_1X + b_0 \in \mathbb{R}[X],$$

we have that:

$$\sigma(b_n)X^n + \sigma(b_{n-1})X^{n-1} + \ldots + \sigma(b_0) = \sigma^*(g) = g = b_nX^n + \ldots + b_1X + b_0$$

Hence, by comparison of the coefficients, we see that all coefficients of g satisfy

$$\sigma(b_i) = b_i \quad (i = 0, 1, \ldots, n) \quad \text{for any element } \sigma \in Gal(f),$$

therefore all b_i's belong to the fixed field $E^{Gal(E/\mathbb{Q})}$ of $Gal(f) = Gal(E/\mathbb{Q})$. Since E is the splitting field of a polynomial in $\mathbb{Q}[X]$ and since $char(\mathbb{Q}) = 0$, we have that the field extension $E/\mathbb{Q}$ is Galois, which is equivalent to:

$$E^{Gal(E/\mathbb{Q})} = \mathbb{Q}$$

Hence all coefficients of g belong to the field $\mathbb{Q}$, which means that $g \in \mathbb{Q}[X]$, as desired. □

Remark 1.14 *Because $\mathbb{C}$ is the disjoint union of the following three sets*

$$\mathbb{C} = \mathbb{Q} \sqcup (\mathbb{R} \setminus \mathbb{Q}) \sqcup (\mathbb{C} \setminus \mathbb{R}),$$

and since rational numbers are simply algebraic numbers of degree 1, the subfield $\mathbb{A}$ of $\mathbb{C}$ is divided into three non-overlapping sets:

$$\mathbb{Q} \text{ and } (\mathbb{R} \setminus \mathbb{Q}) \cap \mathbb{A} \text{ and } (\mathbb{C} \setminus \mathbb{R}) \cap \mathbb{A}$$

Furthermore, all of those three subsets of $\mathbb{A}$ are non-empty. For example,

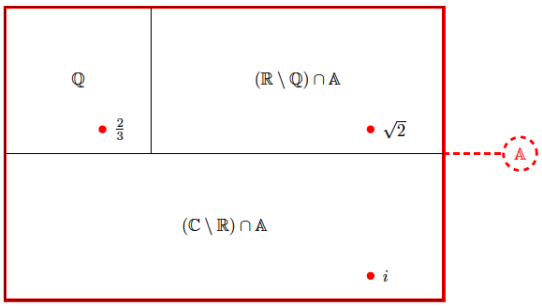

Figure 1.1: The complex algebraic numbers

- $2/3$ *belongs to* $\mathbb{Q}$ *with minimal polynomial* $irr_{2/3,\mathbb{Q}} = X - 2/3$;
- $\sqrt{2}$ *belongs to* $(\mathbb{R}\setminus\mathbb{Q})\cap\mathbb{A}$ *with minimal polynomial* $irr_{\sqrt{2},\mathbb{Q}} = X^2 - 2$;
- i *belongs to* $(\mathbb{C}\setminus\mathbb{R})\cap\mathbb{A}$ *with minimal polynomial* $irr_{i,\mathbb{Q}} = X^2 + 1$.

We now give a result about the cardinality of the set of algebraic numbers.

Proposition 1.15 *The field* $\mathbb{A}$ *of all algebraic numbers is countable.*

Proof We only give the outline of the proof. We first recall that any polynomial with coefficients in a given field has a finite number of roots which is at most its degree. Now, since the set $\mathbb{Q}$ of all rational numbers is countable, the set $\mathbb{Q}[X]$ of all polynomials with rational coefficients is also countable. Therefore, since the set $\mathbb{A}$ of all algebraic numbers is the set of all roots of a countable number of polynomials, each with a finite number of roots, we have the desired result. □

There is another property of algebraic numbers using polynomials with integral coefficients, instead of rational coefficients:

Proposition 1.16 *We have the equivalence:*

$$\alpha \in \mathbb{A} \iff \begin{array}{l} \exists \text{ a non-constant polynomial } g \in \mathbb{Z}[X] \\ \text{such that } g(\alpha) = 0 \text{ and with positive leading coefficient} \end{array}$$

Watch out, g is not necessarily monic!

Proof One direction is obvious, because any polynomial with integral coefficients is certainly a polynomial with rational coefficients.
For the other direction, let $\alpha \in \mathbb{A}$ be an algebraic number. That is, there exists a polynomial $f = f(X) = a_n X^n + \ldots + a_1 X + a_0$ with $n \in \mathbb{N}^{\geq 1}$ and $a_n, \ldots, a_1, a_0 \in \mathbb{Q}$ and $a_n \neq 0$ and such that $f(\alpha) = 0$. We set $a_i := p_i/q_i$

with $p_i, q_i \in \mathbb{Z}$ and $q_i > 0$, as well as $gcd(p_i, q_i) \sim 1$ for $i = 0, \ldots, n$, and we consider the new polynomial:

$$g = g(X) := \frac{lcm(q_0, q_1, \ldots, q_n)}{gcd(p_0, p_1, \ldots, p_n)} \cdot f(X)$$

(This construction comes from the "decomposition of f into its content and its corresponding $\mathbb{Z}$-primitive polynomial.")
We certainly have that $g \in \mathbb{Z}[X]$ with degree at least 1 and with non-zero leading coefficient, and that $g(\alpha) = 0$. If the leading coefficient of g is strictly negative, by considering the polynomial $(-g)$, we get the desired result. □

We can specify Proposition 1.16 by adding irreducibility and by specifying the degree of the polynomial in question.

Proposition 1.17 *We have the equivalence:*

$$\alpha \in \mathbb{A} \text{ of degree } n \iff \begin{array}{l} \exists \text{ a non-constant polynomial } g \in \mathbb{Z}[X] \text{ of degree } n \\ \text{such that } g(\alpha) = 0 \text{ and with positive leading coefficient} \\ \text{and which is irreducible in } \mathbb{Q}[X] \end{array}$$

Watch out, g is not necessarily monic!

Proof It suffices to redo the proof of Proposition 1.16 by taking f to be the minimal polynomial $irr_{\alpha,\mathbb{Q}}$ of α over $\mathbb{Q}$. Then g only differs from $irr_{\alpha,\mathbb{Q}}$ from a non-zero constant, hence g has the same degree as $irr_{\alpha,\mathbb{Q}}$ and is irreducible in $\mathbb{Q}[X]$ like $irr_{\alpha,\mathbb{Q}}$. □

Remark 1.18 *We note that the polynomial g in the proof of both Propositions 1.16 and 1.17 is a $\mathbb{Z}$-primitive polynomial. Hence, by Gauss's Lemma, the irreducibility of g in $\mathbb{Q}[X]$ is equivalent to the irreducibility of g in $\mathbb{Z}[X]$ (because we also have that $Quot(\mathbb{Z}) = \mathbb{Q}$)*

1.1.2 Algebraic Integers

We have stressed twice that the polynomial g in the last two propositions was not necessarily monic. By requiring that g be also monic, we get a new definition:

Definition 1.19 *(Algebraic integers) An algebraic number $\alpha \in \mathbb{A}$ is called an* algebraic integer *if it is the root of a monic non-constant polynomial $g \in \mathbb{Z}[X]$.*

By definition, all algebraic integers are algebraic numbers. But the converse is not true. There exist algebraic numbers which are not algebraic integers. One easy example is the following:

Example 1.20 *The irrational number $\sqrt{2}/3$ is not an algebraic integer, because even though it is a root of a non-constant polynomial with integral coefficients, namely $9X^2 - 2$, we cannot find a monic such polynomial which does the trick!*

Proof Assume $\alpha := \sqrt{2}/3$ is an algebraic integer. Then there exists a monic polynomial $g = g(X) = X^n + b_{n-1}X^{n-1} + \ldots + b_1X + b_0 \in \mathbb{Z}[X]$ which has α as root. So:

$$g(\alpha) = \left(\frac{\sqrt{2}}{3}\right)^n + b_{n-1}\left(\frac{\sqrt{2}}{3}\right)^{n-1} + \ldots + b_0 = 0$$

Hence, by multiplying both sides of this equation by 3^n, we obtain by setting $b_n = 1$:

$$\sum_{i=0}^{n} b_i(\sqrt{2})^i 3^{n-i} = (\sqrt{2})^n + b_{n-1}(\sqrt{2})^{n-1} \cdot 3 + \ldots + b_0 \cdot 3^n = 0$$

For $i = 0, \ldots, n$, we have that if i is odd, then $(\sqrt{2})^i$ is not an integer. So we can separate our equation into two smaller equations, and we obtain:

$$\sum_{\substack{i \text{ odd} \\ i=0,\ldots,n}} b_i(\sqrt{2})^i 3^{n-i} = 0 \quad \text{and} \quad \sum_{\substack{i \text{ even} \\ i=0,\ldots,n}} b_i(\sqrt{2})^i 3^{n-i} = 0$$

By factorizing by $\sqrt{2}$, the first equation becomes:

$$\sum_{\substack{i \text{ odd} \\ i=0,\ldots,n}} b_i(\sqrt{2})^i 3^{n-i} = 0 \iff \sqrt{2} \cdot \sum_{\substack{i \text{ odd} \\ i=0,\ldots,n}} b_i\, 2^{\frac{i-1}{2}}\, 3^{n-i} = 0$$

Since 3 divides 0 in $\mathbb{Z}$, each sum above (the one for i even and the one for i odd) must be divisible by 3. In particular, because each summand containing $b_i, i \neq n$, has a factor of 3, the number 3 must divide the summand containing $b_n = 1$. This tells us that 3 divides $2^{\frac{n-1}{2}}$ in $\mathbb{Z}$ if n is odd, and 3 divides $2^{\frac{n}{2}}$ in $\mathbb{Z}$ if n is even. In either case, this is false and hence we can conclude that $\alpha := \sqrt{2}/3$ is not an algebraic integer. □

We have to stress out that algebraic integers are not always (ordinary) integers. For example, i or $\sqrt{2}$ are algebraic integers which are not ordinary integers. Indeed, we have $g_1(i) = 0$ and $g_2(\sqrt{2}) = 0$ with $g_1 = g_1(X) = X^2 + 1$ and $g_2 = g_2(X) = X^2 - 2$ being two non-constant, monic polynomials with integral coefficients.

In fact, we can specify the nature of *real* algebraic integers.

Proposition 1.21 *A real algebraic integer is either an (ordinary) integer or an irrational number. In other words, any non-integral root of a monic non-constant polynomial with integral coefficients is necessarily irrational.*

Proof Let α be a real algebraic integer, i.e. $\alpha \in \mathbb{R}$ is a root of a non-constant monic polynom $g \in \mathbb{Z}[X]$. Suppose that $\alpha \notin \mathbb{R} \setminus \mathbb{Q}$, i.e. , since $\alpha \in \mathbb{R}$, suppose that α is rational (we have indeed restricted ourselves to *real* algebraic integers

in this proposition). Let us show that $\alpha \in \mathbb{Z}$. Using a result from algebra, since $Quot(\mathbb{Z}) = \mathbb{Q}$ and since any monic polynom $g \in \mathbb{Z}[X]$ is necessarily $\mathbb{Z}$-primitive, then we know that if $\alpha = p/q \in \mathbb{Q}$ (with $p, q \in \mathbb{Z}$, $q > 0$ and $gcd(p, q) \sim 1$) is a rational root of g, then p divides the constant coefficient of g and q divides the leading coefficient of g. Since g is monic, we get that q divides 1 in $\mathbb{Z}$, which implies that $q = \pm 1$. Since $q > 0$, we have $q = 1$, and therefore $\alpha = p \in \mathbb{Z}$, as desired. □

Remark 1.22 *As a fun fact, we can prove that the algebraic integers form a ring, whereas the algebraic numbers form a field.*

There is a small property which links algebraic numbers to algebraic integers:

Proposition 1.23 *If α is an algebraic number, then there exists an integer $c \in \mathbb{Z}$ such that $c \cdot \alpha$ is an algebraic integer.*

Proof Since $\alpha \in \mathbb{A}$, there exists a non-constant polynomial $g \in \mathbb{Z}[X]$ such that

$$g(\alpha) = a_n \alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$$

with $n \geq 1$ and $a_n > 0$ (we only need the fact that $a_n \neq 0$).
We define

$$\tilde{g} = \tilde{g}(X) := a_n^{n-1} \cdot g\left(\frac{X}{a_n}\right)$$

More precisely, we have:

$$\tilde{g} = a_n^{n-1} \cdot a_n \cdot \left(\frac{X}{a_n}\right)^n + a_n^{n-1} \cdot a_{n-1} \cdot \left(\frac{X}{a_n}\right)^{n-1} + \ldots + a_n^{n-1} \cdot a_1 \cdot \left(\frac{X}{a_n}\right) + a_n^{n-1} \cdot a_0$$

This polynomial has certainly integral coefficients and is monic. Furthermore, we have:

$$\tilde{g}(a_n\alpha) = a_n^{n-1} g\left(\frac{a_n\alpha}{a_n}\right) = a_n^{n-1} \cdot g(\alpha) = a_n^{n-1} \cdot 0 = 0$$

Hence $a_n\alpha$ is an algebraic integer, which proves the proposition by taking $c := a_n$. □

In fact, there is also a relation between algebraic numbers and algebraic integers using the minimal polynomial:

Proposition 1.24 *For any algebraic number $\alpha \in \mathbb{A}$, we have the equivalence:*

$$\alpha \text{ is an algebraic integer } \iff irr_{\alpha,\mathbb{Q}} \in \mathbb{Z}[X]$$

Proof One direction is obvious, because the minimal polynomial of any algebraic number is always monic.
For the other direction, let α be an algebraic integer, i.e. there exists a monic

non-constant polynomial $g \in \mathbb{Z}[X]$ such that $g(\alpha) = 0$. Let also $irr_{\alpha,\mathbb{Q}}$ be the minimal polynomial of the given algebraic number α over $\mathbb{Q}$. By Remark 1.4, since $g \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X]$ with $g(\alpha) = 0$, we have that:

$$irr_{\alpha,\mathbb{Q}} \text{ divides } g \text{ and } \mathbb{Q}[X],$$

i.e. $g(X) = irr_{\alpha,\mathbb{Q}}(X) \cdot h(X)$ for some polynomial $h \in \mathbb{Q}[X]$. By "decomposing" the two polynomials $irr_{\alpha,\mathbb{Q}}$ and h into their contents and their $\mathbb{Z}$-primitive parts, we get:

$$irr_{\alpha,\mathbb{Q}}(X) = \frac{a}{b} \cdot \varphi^*(X) \text{ and } h(X) = \frac{c}{d} \cdot \psi^*(X)$$

for some integers $a, b, c, d \in \mathbb{Z}$ with $b, d > 0$ and some $\mathbb{Z}$-primitive polynomials $\varphi^*, \psi^* \in \mathbb{Z}[X]$. So we obtain from $g = irr_{\alpha,\mathbb{Q}} \cdot h$ that:

$$bd \cdot g = ac \cdot \varphi^*\psi^*$$

Because φ^* and ψ^* are $\mathbb{Z}$-primitive, then by Gauss' s Lemma, the product $\varphi^*\psi^*$ is also $\mathbb{Z}$-primitive. But g is also $\mathbb{Z}$-primitive (since g is monic), hence by unicity of the decomposition of polynomials into their content and primitive part up to association (i.e. up to units), we get:

$$bd \sim ac \text{ in } \mathbb{Z},$$

i.e. bd and ac are associated in $\mathbb{Z}$. Now, because $Z^\times = \{\pm 1\}$, we get $bd = \pm ac$, which implies that $g = g(X) = (\pm 1) \cdot \varphi^*\psi^*$. So the leading coefficient of both φ^* and ψ^* is ± 1 (since g is monic).
Therefore, by comparing now the leading coefficients in $irr_{\alpha,\mathbb{Q}} = \frac{a}{b} \cdot \varphi^*$, we get that:

$$1 = \frac{a}{b} \cdot (\pm 1) \Longrightarrow \frac{a}{b} = \pm 1 \Longrightarrow irr_{\alpha,\mathbb{Q}} = \pm\varphi^*$$

Since $\varphi^* \in \mathbb{Z}[X]$, we deduce that $irr_{\alpha,\mathbb{Q}} \in \mathbb{Z}[X]$, as desired. □

We should not talk of the minimal polynomial over $\mathbb{Z}$, because $\mathbb{Z}$ is not a field, but some authors do it in correlation with the last proposition. They define the minimal polynomial of an algebraic number over $\mathbb{Z}$ as a monic polynomial with integral coefficients having α as root and being irreducible in $\mathbb{Z}[X]$, which is equivalent via Gauss's Lemma to being irreducible in $\mathbb{Q}[X]$. But we prefer not to do that, because with this definition of minimal polynomial over $\mathbb{Z}$, its existence is not guaranteed anymore.

Up until now we have only considered roots of polynomials either with rational coefficients or integral coefficients.

Proposition 1.25 *If $\alpha \in \mathbb{C}$ is a root of a polynomial $h = h(X) \in \mathbb{A}[X]$ with algebraic coefficients, then α must be an algebraic number.*

Proof We only outline the proof which uses some linear algebra. Let $E := \mathbb{Q}(a_n, a_{n-1}, \ldots, a_1, a_0)$ be the smallest field containing $\mathbb{Q}$ and all the coefficients of $h = h(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$. Since all coefficients of h are algebraic elements over $\mathbb{Q}$, then the field extension $E/\mathbb{Q}$ is a finite extension. Since the vector space formed by the powers of α is finite-dimensional over E, it is also finite-dimensional over $\mathbb{Q}$. That is, some linear combination of the powers of α with rational coefficients vanishes, so α is a root of a polynomial with rational coefficients. □

1.1.3 Transcendental Numbers

Having thoroughly recalled all we need about algebraic numbers, we can now turn to transcendental numbers.

Definition 1.26 *(Transcendental numbers) A complex number $\alpha \in \mathbb{C}$ is called a* transcendental number *if it is not an algebraic number, i.e. if there does not exist any non-constant polynomial with rational coefficients which has α as a root.*
The quality of a number being transcendental is called transcendence.

The fundamental theorem of algebra tells us that if $f \in \mathbb{C}[X]$ is a non-constant polynomial with complex coefficients, then there exists a complex number $\alpha \in \mathbb{C}$ such that $f(\alpha) = 0$. So in particular, for any non-constant polynomial $f \in \mathbb{Q}[X]$ with rational coefficients, we have the existence of a complex number $\alpha \in \mathbb{C}$ such that $f(\alpha) = 0$.
The subject of transcendental numbers focuses on the reverse question:
Given a complex number $\alpha \in \mathbb{C}$, does there exist a polynomial $f \in \mathbb{Q}[X]$ with rational coefficients such that $f(\alpha) = 0$? Simply by definition, the answer is yes if and only if α is an algebraic number. In other words, the answer is no if and only if α is a transcendental number.

We note that every *real* transcendental number must be irrational, since a rational number is, by Proposition 1.7, an algebraic number of degree 1. The converse is obviously not true: not all irrational numbers are real transcendental numbers. For example, $\sqrt{2}$ and $\varphi := \frac{1+\sqrt{5}}{2}$ are both irrational numbers which are not real transcendental, because they are both algebraic numbers of degree 2.

Hence, making use of Proposition 1.7, we can say that the set of real numbers $\mathbb{R}$ consists of three non-overlapping sets:

1. The set $\mathbb{Q}$ of all rational numbers, which is simply the set of algebraic numbers of degree 1
2. The set $(\mathbb{R} \setminus \mathbb{Q}) \cap \mathbb{A}$ of all algebraic irrational numbers, which is in fact the set of real algebraic numbers of degree ≥ 2
3. The set of all real transcendental numbers, which is just the complement of the set of real algebraic numbers with respect to $\mathbb{R}$

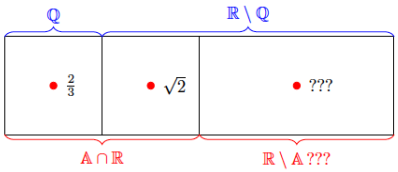

Figure 1.2: The real numbers

We have seen examples of elements in the first two sets, but a priori, we do not know yet whether the set of real transcendental numbers is empty or not (it is not!)
One can even wonder if the set of non-real transcendental numbers is empty or not. To partially answer this question, we recall Proposition 1.11, which says that a complex number is an algebraic number if and only if its real and imaginary parts are both algebraic numbers. By taking the contraposite, we obtain:

Proposition 1.27 *Let $\alpha = a + ib \in \mathbb{C}$ with $a, b \in \mathbb{R}$ be a given complex number. Then we have the equivalence:*

$$\alpha \text{ is a transcendental number} \iff \begin{array}{c} \mathfrak{Re}(\alpha) = a \text{ is a transcendental number} \\ \text{OR} \\ \mathfrak{Im}(\alpha) = b \text{ is a transcendental number} \end{array}$$

As a consequence, if α is real transcendental number, then $\alpha + i$ and $i\alpha$ are both complex non-real transcendental numbers, because in the first case, $\mathfrak{Re}(\alpha + i) = \alpha$ is transcendental and in the second case, $\mathfrak{Im}(i\alpha) = \alpha$ is transcendental. Similarly, the number $\alpha + i\alpha$ is also a non-real transcendental number, because, here, even both real and imaginary parts are transcendental.
In other words, the existence of non-real transcendental numbers is a consequence of the existence of real transcendental numbers. Because of this, some authors only focus on the study of real transcendental numbers.

Another consequence of Proposition 1.25 in the light of transcendental numbers is the following:

Proposition 1.28 *If α_1 and α_2 are both transcendental numbers, then either $\alpha_1 + \alpha_2$ or $\alpha_1 \cdot \alpha_2$ is a transcendental number.*

Proof Assume the contrary, i.e. $\alpha_1 + \alpha_2$ and $\alpha_1 \cdot \alpha_2$ are both algebraic numbers. Then the polynomial

$$h = h(X) = (X - \alpha_1)(X - \alpha_2) = X^2 - (\alpha_1 + \alpha_2)X + \alpha_1\alpha_2 \in \mathbb{A}[X]$$

would have algebraic coefficients. Hence, by Proposition 1.25, the roots of h, which are α_1 and α_2, would both be algebraic numbers, which is a contradiction. □

That being said, the big question (which we have already mentioned) is:

Do real transcendental numbers exist?

If yes, can one give explicit examples of real transcendental numbers? And even more difficult: given a specific (necessarily irrational) real number, like e or π, how can you determine whether this number is transcendental or not? We will answer to all these questions in this report, but we start by giving a brief historical outlook on the subject of the transcendental numbers.

1.2 Some Historical Notes

The name "transcendental" comes from the Latin transcendĕre, which means 'to climb over or beyond, to surmount', and was first used in the context of a function not being algebraic by Leibniz in his 1682 paper, in which he proved that $\sin x$ is not an algebraic function of x.

Euler, in the 18^{th} century, was probably the first person to define transcendental numbers in the modern sense, when he asserted in 1748 that the number $log_a b$ was not algebraic for rational numbers a and b provided b is not of the form $b = a^c$ for some rational c. Euler's claim was not proved by the way until the 20^{th} century!

As already mentioned, a real transcendental number must be irrational. By 1744, Euler had already established the irrationality of e, and, by 1761, Lambert had confirmed the irrationality of π. But both of these mathematicians could not give a proof of the transcendence of those two numbers. Lambert proposed a tentative sketch of a proof of π's transcendence in his 1768 paper, but it was far from being convincing.

The existence of transcendental numbers was already suspected by the end of the 18^{th} century, but it was the French mathematician Liouville in 1844 who exhibited the first class of transcendental numbers (now called Liouville numbers in his honour) as a consequence of an approximation theorem that he proved. The contribution of Liouville is significant because before 1844 we did not know for sure of the existence of transcendental numbers. This is why we now consider 1844 to be the launch of the subject of transcendental numbers.

We had to wait 29 more years for Hermite to finally give the first proof of the transcendence of e in 1873, followed nine years later by Lindemann who gave the first proof of the transcendence of π in 1882, by cleverly modifying

Hermite's proof and by making use of the famous Euler equation linking the old constant π to the modern constant e, namely $e^{i\pi} + 1 = 0$. The proofs of the transcendence of e and π were considered among the greatest achievements of 19^{th} century mathematics. The transcendence of π especially is a fact of great historical, as well as intrinsic, interest.

Indeed, one of the classical problems of Greek mathematics was to construct, with compass and straightedge alone, a square whose area is that of a circle of radius 1. This requires the construction of a line segment whose length is $\sqrt{\pi}$, which can be accomplished if a line segment of length π is constructible. The Greeks were totally unable to decide whether such a line segment could be constructed, and even the full resources of modern mathematics were unable to settle this question until 1882, when π was proven to be transcendental by Lindemann. Since the length of any line segment that can be constructed with straightedge and compass can be written in terms of $+, \times, -, \div$, and $\sqrt{}$, and is therefore algebraic, this proves that a line segment of length π cannot be constructed.

A totally different approach to the existence of transcendental numbers was taken by Cantor who proved with his famous diagonal's argument (which dates back to 1874) that the real numbers are uncountable. Since the real numbers are the union of the real algebraic numbers and the real transcendental numbers, both of these sets cannot be countable. This implies that the real transcendental numbers must be uncountable, since the real algebraic numbers are countable (see Proposition 1.15). Cantor thus showed in a non-constructive manner that almost all real numbers are transcendental, without giving any explicit examples.

From the end of the 19^{th} century up until the 1930's, not much new impetus has been given to the subject of transcendental numbers: we can only mention a dozen of new and simpler proofs of the transcendence of e and π which rely more and more on the property of the exponential function, and therefore less succeptible of being generalized.

But in 1934 new impulse was given to the subject, when Hilbert's 7^{th} problem (posed in 1900) was solved, namely:

Is a^b always a transcendental number,
for any algebraic number $a \notin \{0, 1\}$
and any irrational algebraic number b?

The question was answered in the affirmative by Gelfond in 1934, following the ideas of Gelfond and Siegel, and refined by Schneider in 1935, as well as extended by Baker in 1966. A neat application of Hilbert's 7^{th} problem implies for example that the number $2^{\sqrt{2}}$ is transcendental.

Among the important results of the remaining of the 20th century, we can cite the classification of transcendental numbers by Mahler (1932) and later by Koksma (1939); Schneider's theorem on elliptic functions and Abelian integrals (1941) and the Thue-Siegel-Roth Theorem on the approximation of algebraic numbers by rationals (1955), which generalizes Liouville's original approximation theorem.

Open problems in the subject of transcendental numbers are very interesting and surprisingly easy to state: they form a list of given numbers which have yet to be proven to be either transcendental or algebraic.
For example, most sums, products, powers, etc. of the number π and the number e, e.g. $e\pi$, $e+\pi$, $\pi-e$, π/e, π^{π}, e^{e}, π^{e} , $\pi^{\sqrt{2}}$, e^{π^2}, are not known to be rational, algebraic, irrational or transcendental. A notable exception is $e^{\pi\sqrt{n}}$ (for any positive integer n) which has been proven transcendental. By the way, even though both $e\pi$ and $e+\pi$ are of unknown status, we certainly have by Proposition 1.28 that either $e\pi$ or $e+\pi$ is transcendental. We also do not know whether e and π are algebrically dependent or not.

Another open problem concerns the Euler's constant γ defined as the limiting difference between the harmonic series and the natural logarithm, namely:

$$\gamma = \lim_{n\to\infty}\left(-\log n + \sum_{k=1}^{n}\frac{1}{k}\right) = \int_1^{\infty}\left(-\frac{1}{x}+\frac{1}{\lfloor x\rfloor}\right)dx.$$

Here, $\lfloor x\rfloor$ represents the floor function. The number γ has not been proved algebraic or transcendental. In fact, it is not even known whether γ is irrational. Of course, some progress have been made, but a definite answer has still not been given.

In the same vein, the Riemann zeta function at odd integers strictly greater than 3, namely $\zeta(5), \zeta(7), \ldots$, has not even been proven to be irrational.

The subject of transcendental numbers is a branch of number theory that investigates transcendental numbers, in both qualitative and quantitative ways. As yet, there seems to be no aspect to the study of transcendental numbers which could be described as a general theory. However, there are some methods which are quite powerful and useful in other domain of mathematics. For example, many approximation theorems used in the study of transcendental numbers come in handy in the study of diophantine equations.

Chapter 2

Transcendence Criteria

Usually the numbers for which we do not know of their transcendence arise from analysis and are given by infinite processes, involving limits, infinite series, infinite products or integrals. So it is very difficult in general to determine whether those numbers are even irrational, let alone transcendental, or not.

Since being irrational is a necessary condition for a real number to be transcendental, we start by looking at some irrationality criteria, hoping that one of them can be modified into a transcendence criterion.

There exists a well-known criterion to determine whether a real and (for simplification) non-negative number x is irrational or not, using its expansion in an integer basis $b \in \mathbb{N}^{\geq 2}$ (e.g. in binary or decimal expansion), namely:

$$x = \lfloor x \rfloor + \sum_{j \geq 1} \frac{d_j}{b^j} =: [s \cdot d_1 d_2 d_3 \ldots]_b$$

for some integers s and $0 \leq d_n \leq b-1$ for $n = 1, 2, \ldots$, where $\lfloor x \rfloor$ denotes the floor of x (which is equal to the integral part of x, since $x \geq 0$).

Indeed, we have the equivalence: x is rational if and only if x has an eventually periodic (including finite) expansion in some (or equivalently in every) integer basis. In other words, x is rational if and only if x is of the form

$$[s \cdot d_1 d_2 d_3 \ldots d_r d_{r+1} d_{r+2} \ldots d_{r+p} d_{r+1} d_{r+2} \ldots d_{r+p} d_{r+1} d_{r+2} \ldots d_{r+p} d_{r+1} \ldots]_b$$

for some (or equivalently for every) integer $b \geq 2$.

For example, the real numbers $\sqrt{2}$ and the golden ratio $\varphi := \frac{1+\sqrt{5}}{2}$ are both irrational, because their decimal expansion are respectively $\sqrt{2} = 1.4142135623730950488\ldots$ and $\varphi = 1.618033988749894\ldots$ and are infinite aperiodic.

There is also another well-known criterion for irrationality using the continued fraction expansion. Any real and (for simplification) non-negative x can be uniquely written as a simple continued fraction of the form

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \ddots}}}} =: [a_0; a_1, a_2, a_3, \ldots]$$

for some integers $a_0, a_1, a_2, \ldots$

We have the equivalence: x is irrational if and only if x has an infinite simple continued fraction expansion.
For example, the real numbers $\sqrt{2}$ and the golden ratio $\varphi := \frac{1+\sqrt{5}}{2}$ are both irrational, because their simple continued fraction expansion are respectively $\sqrt{2} = [1; 2, 2, 2, \ldots]$ and $\varphi = [1; 1, 1, 1, \ldots]$ and are not finite.

Unfortunately, we do not know the expansion of most constants arising from analysis , either in an integer basis or in simple continued fractions. So these two irrationality criteria are of no use. We thus need to find another criterion for irrationality, which is, as already mentioned, a necessary condition for a number to be transcendental.

2.1 Irrationality Criterion

The most efficient criterion for irrationality, or equivalently for rationality, involves rational approximation.

Since $\mathbb{Q}$ is dense in $\mathbb{R}$, then of course for any real number $\theta \in \mathbb{R}$ and any $\varepsilon > 0$, there exists a rational number $p/q \in \mathbb{Q}$ with $p, q \in \mathbb{Z}$, and $q > 0$, as well as $gcd(p, q) \sim 1$, for which

$$|\theta - \frac{p}{q}| < \varepsilon \tag{2.1}$$

The problem is that, as we try to make $\frac{p}{q}$ closer and closer to θ, we may have to use larger and larger integers p and q. So, the reasonable question to ask here is how well can we approximate θ by rationals without too large denominators.

Trivially, every real number θ can be approximated by a rational number $\frac{p}{q}$ with a given denominator $q \geq 1$ with an error not exceeding $\frac{1}{2q}$.

Let indeed $q \in \mathbb{Z}^{>0}$ be any positive integer. Note that the closed interval $\left[q\theta - \frac{1}{2}, q\theta + \frac{1}{2}\right]$ has length 1 and, therefore, contains at least one integer. Choosing p to be that integer, we immediately get the result:

$$|q\theta - p| \leq \frac{1}{2} \Longrightarrow |\theta - \frac{p}{q}| \leq \frac{1}{2q}$$

This estimate

$$|\theta - \frac{p}{q}| \leq \frac{1}{2q} \tag{2.2}$$

certainly implies (2.1). Indeed, for any $\varepsilon > 0$, just take $q \in \mathbb{Z}^{>0}$ large enough so that $\frac{1}{2q} < \varepsilon$ and you get:

$$|\theta - \frac{p}{q}| \leq \frac{1}{2q} < \varepsilon$$

Considering rational approximations p/q of real numbers with an error of order $\frac{1}{q}$ is the key to find a criterion which will distinguish rational from irrational numbers.

The idea is the following: if you have a rational number, then it has a very bad approximation by any other rational numbers, in the following sense: Let $\theta = a/b \in \mathbb{Q}$ with $a, b \in \mathbb{Z}, b > 0$ and $gcd(a, b) \sim 1$ be any rational number. Then for all *other* rational numbers $\frac{p}{q} \neq \theta$ (with $p, q \in \mathbb{Z}, q > 0$ and $gcd(p, q) \sim 1$), we claim that the distance between θ and p/q is not too small. Indeed, we have:

$$|\theta - \frac{p}{q}| = \frac{|aq - pb|}{qb}$$

Now, since $\frac{p}{q} \neq \theta = \frac{a}{b}$, we have, using the fact that the product of means equals the product of the extremes, that $aq \neq bp$, hence $aq - bp \neq 0$. So, since this number is a non-zero integer, we have that $|aq - bp| \geq 1$. So we obtain:

$$|\theta - \frac{p}{q}| \geq \frac{1}{bq} = \frac{1}{b} \cdot \frac{1}{q} > \frac{1}{2b} \cdot \frac{1}{q}$$

By taking $c := \frac{1}{2b} > 0$ (which is a positive constant only depending on $\theta = a/b$), we get that:

$$|\theta - \frac{p}{q}| > \frac{1}{2b} \cdot \frac{1}{q} = \frac{c}{q} \tag{2.3}$$

On the other hand, we will show that irrational numbers are well approximable by rationals.

Another interesting question is whether or not we can get a smaller error of approximation than $\frac{1}{q}$. Surprisingly enough, it is possible, if not for all q, then, at least for some of them.

This way of distinguishing rational from irrational numbers using rational approximations by specifying the order of the approximation error is formalised in the next proposition:

Proposition 2.1 *(Criterion for irrationality / rationality) Let $\theta \in \mathbb{R}$ be a real number. Then the following conditions are equivalent:*

(i) $\theta \notin \mathbb{Q}$

(ii) For any $\varepsilon > 0$ there exists a rational number $p/q \in \mathbb{Q}$ (with $p, q \in \mathbb{Z}, q > 0$ and $gcd(p, q) \sim 1$) such that

$$0 < |\theta - \frac{p}{q}| < \frac{\varepsilon}{q}$$

i.e. θ is said to be well approximable by rational numbers.
(The inequality > 0 guarantees that we consider rationals $\frac{p}{q} \neq \theta$)

(iii) (Asymptotic Dirichlet's Theorem or Dirichlet's Theorem on Diophantine Equations) There exist infinitely many rational numbers $p/q \in \mathbb{Q}$ (with $p, q \in \mathbb{Z}, q > 0$ and $gcd(p, q) \sim 1$) such that

$$|\theta - \frac{p}{q}| < \frac{1}{q^2}$$

(We do not need to specify here that $\frac{p}{q} \neq \theta$, since we have infinitely many of them.)

(iv) (Uniform Dirichlet's Theorem) For any real number $Q > 1$, there exists a rational number $p/q \in \mathbb{Q}$ (with $p, q \in \mathbb{Z}, q > 0$ and $gcd(p, q) \sim 1$) such that $1 \leq q < Q$ and with the property that

$$0 < |\theta - \frac{p}{q}| < \frac{1}{qQ}$$

Proof $(ii) \Rightarrow (i)$: This result has already been proven, because we have explained the contraposite $\neg(i) \Longrightarrow \neg(ii)$ (see Equation (2.3)), namely:

$$\theta \in \mathbb{Q} \Longrightarrow \begin{array}{l} \text{there exists a positive constant } c > 0 \text{ such that} \\ \text{for all other rational numbers } p/q \in \mathbb{Q} \setminus \{\theta\} \\ \text{(with } p, q \in \mathbb{Z}, q > 0 \text{ and } gcd(p, q) \sim 1) \\ \text{the inequality } |\theta - \frac{p}{q}| > \frac{c}{q} \text{ holds} \end{array}$$

By the way the implication $(ii) \Rightarrow (i)$ is actually the useful part of the irrationality/rationality criterion, and paradoxically also the easiest one to prove! The other easy implications are $(iv) \Rightarrow (iii) \Rightarrow (ii) \Rightarrow (i)$.

Indeed, let us prove that $(iv) \Longrightarrow (iii)$:
Let $Q > 1$ be any real number. Then by the Uniform Dirichlet's Theorem, there exists a rational number $p/q \in \mathbb{Q}$ (with $p, q \in \mathbb{Z}, q > 0$ and

$gcd(p,q) \sim 1$) such that $1 \leq q < Q$ (which implies that $1 \geq \frac{1}{q} > \frac{1}{Q}$) and such that

$$0 < |\theta - \frac{p}{q}| < \frac{1}{qQ} < \frac{1}{q^2}.$$

Let Q' be any real number exceeding $|\theta - \frac{p}{q}|^{-1}$ (which implies that $\frac{1}{Q'} < |\theta - \frac{p}{q}|$). A second application of Uniform Dirichlet's Theorem shows that there exists a rational number $p'/q' \in \mathbb{Q}$ (with $p', q' \in \mathbb{Z}, q' > 0$ and $gcd(p', q') \sim 1$) such that $1 \leq q' < Q'$ (which implies that $1 \geq \frac{1}{q'} > \frac{1}{Q'}$) and such that

$$0 < |\theta - \frac{p'}{q'}| < \frac{1}{q'Q'} < \frac{|\theta - \frac{p}{q}|}{q'} \leq |\theta - \frac{p}{q}|$$

Thus, necessarily, we get: $\frac{p'}{q'} \neq \frac{p}{q}$.
Furthermore, we have that:

$$|\theta - \frac{p'}{q'}| < \frac{1}{q'Q'} < \frac{1}{(q')^2}$$

By iterating this process, we obtain a sequence $\{\frac{p_i}{q_i}\}_{i=1}^{\infty}$ of distinct rational numbers (with $p_i, q_i \in \mathbb{Z}, q_i > 0$ and $gcd(p_i, q_i) \sim 1$) such that for all $i = 1, 2, \ldots$

$$\begin{cases} |\theta - \frac{p_i}{q_i}| < |\theta - \frac{p_{i-1}}{q_{i-1}}| < \ldots < |\theta - \frac{p_1}{q_1}|, \\ \text{and} \\ 0 < |\theta - \frac{p_i}{q_i}| < \frac{1}{(q_i)^2} \end{cases}$$

Hence we have found infinitely many rational numbers $p/q \in \mathbb{Q}$ (with $p, q \in \mathbb{Z}, q > 0$ and $gcd(p, q) \sim 1$) such that

$$|\theta - \frac{p}{q}| < \frac{1}{q^2}.$$

Let us now prove that $(iii) \Longrightarrow (ii)$: Since there exist infinitely many rational numbers $p_i/q_i \in \mathbb{Q}$ (with $p_i, q_i \in \mathbb{Z}, q_i > 0$ and $gcd(p_i, q_i) \sim 1$) such that

$$|\theta - \frac{p_i}{q_i}| < \frac{1}{(q_i)^2},$$

then the set

$$\{q_i \in \mathbb{Z}^{>0} \mid i = 1, 2, \ldots\}$$

is infinite.
Otherwise, if there were only finitely many such $q_1, q_2, \ldots, q_M \in \mathbb{Z}^{>0}$, then, since there can only exist for each q_i ($i = 1, 2, \ldots, M$) finitely many $p_1^{(i)}, \ldots p_{r_i}^{(i)} \in \mathbb{Z}$ with $gcd(p_j^{(i)}, q_i) \sim 1$ ($j = 1, \ldots, r_i$) which satisfy

$$|\theta - \frac{p_j^{(i)}}{q_i}| < \frac{1}{(q_i)^2},$$

there would be only finitely many rationals $\frac{p_j^{(i)}}{q_i}$ $(i =, 1 \ldots, M$ and $j = 1, \ldots, r_i)$ which satisfy the inequality in (iii), which is a contradiction.
For that reason, since $\{q_i\}_{i=1}^{\infty}$ is an infinite sequence of positive integers, we have (by considering a subsequence if necessary): $q_i \to \infty$, or equivalently $\frac{1}{q_i} \to 0$, as $i \to \infty$.
So, for any $\varepsilon > 0$, there exists an integer $i_0 \in \mathbb{N}$ such that $\frac{1}{q_{i_0}} < \varepsilon$. Hence:

$$0 < |\theta - \frac{p_{i_0}}{q_{i_0}}| < \frac{1}{(q_{i_0})^2} = \frac{1}{q_{i_0}} \cdot \frac{1}{q_{i_0}} < \frac{\varepsilon}{q_{i_0}}$$

which proves (ii).

Let us now prove that $(i) \implies (iv)$: This part uses the pigeonhole or box principle. Let $\theta \in \mathbb{R} \setminus \mathbb{Q}$ and $Q > 1$ be given.
Define $N := \lceil Q \rceil$: this means that N is the integer such that $N - 1 < Q \leq N$. Since $Q > 1$, we have $N \geq 2$.
We recall, for any $x \in \mathbb{R}$, the following equality: $x = \lfloor x \rfloor + \{x\}$ with $\lfloor x \rfloor \in \mathbb{Z}$ (the floor of x) and $0 \leq \{x\} < 1$ (the fractional part of x).
Consider the subset E of the unit interval $[0, 1]$ which consists of the $N + 1$ elements

$$0, \{\theta\}, \{2\theta\}, \{3\theta\}, \ldots, \{(N-1)\theta\}, 1.$$

Since θ is irrational, these $N + 1$ elements are pairwise distinct. Split the interval $[0, 1]$ into N subintervals of length $1/N$:

$$I_j := \left[\frac{j}{N}, \frac{j+1}{N}\right] \quad (0 \leq j \leq N - 1).$$

By the pigeonhole principle, since we have N+1 elements and only N subintervals, one of these N subintervals, say I_{j_0}, contains at least two elements of E. Apart from 0 and 1, all elements $\{q\theta\}$ in E with $1 \leq q \leq N - 1$ are irrational, hence belong to the union of the *open* intervals $(\frac{j}{N}, \frac{j+1}{N})$ with $0 \leq j \leq N - 1$.
Case 1: If $j_0 = N - 1$, then the interval

$$I_{j_0} = I_{N-1} = \left[1 - \frac{1}{N}, 1\right]$$

contains 1 as well as another element of E of the form $\{q^*\theta\}$ with $1 \leq q^* \leq N - 1$. Set $p^* := \lfloor q^*\theta \rfloor + 1$. Then we have that $1 \leq q^* \leq N - 1 < Q$ by choice of N and we also have that:

$$p^* - q^*\theta = \lfloor q^*\theta \rfloor + 1 - \lfloor q^*\theta \rfloor - \{q^*\theta\} = 1 - \{q^*\theta\}$$

But we have for the fractional part $0 \leq \{q^*\theta\} < 1$, implying: $1 - \{q^*\theta\} > 0$. Moreover, 1 and $\{q^*\theta\}$ lie in $\left[1 - \frac{1}{N}, 1\right]$ with $\{q^*\theta\} \in \left(1 - \frac{1}{N}, 1\right)$, hence,

since $Q \leq N$:

$$0 < p^* - q^*\theta = 1 - \{q^*\theta\} < \frac{1}{N} \leq \frac{1}{Q}.$$

So by dividing by $q^* > 0$, we certainly have:

$$0 < |\theta - \frac{p^*}{q^*}| < \frac{1}{q^*Q} \text{ with } 1 \leq q^* < Q,$$

as desired.
Case 2: If $j_0 \neq N-1$, we have that $0 \leq j_0 \leq N-2$ and I_{j_0} contains two elements $\{q_1\theta\}$ and $\{q_2\theta\}$ with $0 \leq q_1 < q_2 \leq N-1$. We have, since $\{q_2\theta\}$ is an irrational number lying in the open interval $(\frac{j_0}{N}, \frac{j_0+1}{N})$, that:

$$|\{q_2\theta\} - \{q_1\theta\}| < \frac{1}{N} \tag{2.4}$$

Now set

$$q := q_2 - q_1, \quad p := \lfloor q_2\theta \rfloor - \lfloor q_1\theta \rfloor .$$

Then we have $0 < q = q_2 - q_1 \leq N-1 < Q$ and

$$|q\theta - p| = |q_2\theta - q_1\theta - \lfloor q_2\theta \rfloor + \lfloor q_1\theta \rfloor| = |\{q_2\theta\} - \{q_1\theta\}|$$

So we have from (2.4) and since $Q \leq N$:

$$0 < |q\theta - p| < \frac{1}{N} \leq \frac{1}{Q},$$

which implies that

$$0 < |\theta - \frac{p}{q}| < \frac{1}{qQ} \text{ with } 1 \leq q < Q,$$

as desired.
In both cases, the coprimality of the numerator and denominator of the rational number p/q is obtained easily by dividing through by $gcd(p,q)$. □

A refined version of the Asymptotic Dirichlet's Theorem (which dates back to 1842) was found by Adolf Hurwitz in 1891. One can prove it using either continued fractions or Farey sequences. We do not give a proof here, only the statement:

Proposition 2.2 *(Hurwitz's Theorem) Let θ be a real number. Then the following conditions are equivalent:*

(a) θ is irrational

(b) There exist infinitely many rational $p/q \in \mathbb{Q}$ (with $p, q \in \mathbb{Z}, q > 0$ and $gcd(p,q) \sim 1$) such that

$$0 < |\theta - \frac{p}{q}| < \frac{1}{\sqrt{5}q^2}$$

Remark 2.3 *Of course Condition (b) in Proposition 2.2 looks stronger than condition (iii) in the irrationality criterion (since $\frac{1}{\sqrt{5}q^2} \leq \frac{1}{q^2}$), so we certainly have $(b) \Longrightarrow (iii) \Longrightarrow \theta \in \mathbb{R} \setminus \mathbb{Q}$. But (b) is in fact equivalent to (iii), and that is what Hurwitz proved, by proving that $(a) \Longrightarrow (b)$.*
Moreover, the estimate in (b) with the constant $1/\sqrt{5}$ is optimal, in the sense that it is the best possible approximation we can have for the golden ratio $\varphi := \frac{1+\sqrt{5}}{2}$. Indeed, one can prove that for any real number $c < \frac{1}{\sqrt{5}}$, there are only finitely many rationals p/q (with $p, q \in \mathbb{Z}, q > 0$ and $gcd(p, q) \sim 1$) such that $|\varphi - \frac{p}{q}| < \frac{c}{q^2}$.

2.1.1 A Proof of the Irrationality of e

The real number

$$e := \sum_{i=0}^{\infty} \frac{1}{i!}$$

is well-known to be irrational. One can find many proofs of this fact, even very short ones. We will present a different proof of the irrationality of e using the irrationality criterion.

Assuming $e \in \mathbb{Q}$, then by the contraposite of condition (ii) of the irrationality criterion, there exists a positive constant $c > 0$ such that for every rational $\frac{p}{q} \neq e$ (with $p, q \in \mathbb{Z}, q > 0$ and $gcd(p, q) \sim 1$), we have:

$$|e - \frac{p}{q}| > \frac{c}{q} \Longleftrightarrow q \cdot |e - \frac{p}{q}| > c$$

Now, by the Archimedean principle, let n be a positive integer such that

$$0 < \frac{1}{n} < c$$

and consider the number

$$\sum_{i=0}^{n} \frac{1}{i!}$$

This real number is in fact a rational number of the form $\frac{p^*}{q^*}$ (with $p^*, q^* \in \mathbb{Z}$, $q^* > 0$ and $gcd(p^*, q^*) \sim 1$) satisfying $\frac{p^*}{q^*} \neq e$. To see this, just write the n+1 summands with the same denominator $n!$, and then set $q^* := n!$ and p^* the

corresponding numerator. We have then:

$$\begin{aligned}
c < q \cdot |e - \frac{p^*}{q^*}| &= n! \cdot \sum_{i=n+1}^{\infty} \frac{1}{i!} \\
&= n! \cdot \left(\frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \frac{1}{(n+3)!} + \dots \right) \\
&= n! \cdot \frac{1}{(n+1)!} \left(1 + \frac{1}{(n+2)} + \frac{1}{(n+2)(n+3)} + \frac{1}{(n+2)(n+3)(n+4)} + \dots \right) \\
&< n! \cdot \frac{1}{(n+1)!} \left(1 + \frac{1}{(n+1)} + \frac{1}{(n+1)(n+1)} + \frac{1}{(n+1)(n+1)(n+1)} + \dots \right) \\
&= n! \cdot \frac{1}{(n+1)!} \cdot \sum_{k=0}^{\infty} \frac{1}{(n+1)^k} \\
&= \frac{1}{n+1} \cdot \frac{1}{1 - \frac{1}{n+1}} = \frac{1}{n},
\end{aligned}$$

a contradiction to the fact that $1/n < c$, implying the irrationality of e.

2.2 Liouville's Approximation Theorem

The aim is to generalize the irrationality criterion into a criterion for transcendental numbers or equivalently into a criterion for algebraic numbers. We recall that a real number θ is irrational if and only if it is an algebraic number of degree 1 (see Proposition 1.7). This is equivalent, by Proposition 1.17, to θ being the root of a polynomial $g \in \mathbb{Z}[X]$ of degree 1 with integral coefficients and positive leading coefficient (since a polynomial of degree 1 is certainly non-constant and irreducible in $\mathbb{Q}[X]$).
We can actually bring out the relevant polynomials of degree 1 with integral coefficients for any irrational number θ simply by rewriting the inequalities of conditions (ii) and (iv) of the irrationality criterion as follows:

$$0 < |\theta - \frac{p}{q}| < \frac{\varepsilon}{q} \Leftrightarrow 0 < |q\theta - p| < \varepsilon$$

and

$$0 < |\theta - \frac{p}{q}| < \frac{1}{qQ} \Leftrightarrow 0 < |q\theta - p| < \frac{1}{Q}$$

So in fact, we have the following equivalence for the conditions (ii) and (iv) of the irrationality criterion:

$$\begin{array}{rl}
 & \text{for any } \varepsilon > 0 \\
 & \exists g = g(X) := qX - p \in \mathbb{Z}[X] \\
(ii) \iff & \text{with degree 1 and even with positive leading coefficient } q > 0 \\
 & \text{which is } \mathbb{Z} \text{ -primitive (i.e. } gcd(p,q) \sim 1) \\
 & \text{such that } 0 < |g(\theta)| < \varepsilon
\end{array}$$

and

$$(iv) \iff \begin{array}{l} \text{for any real number } Q > 1 \\ \exists g = g(X) := qX - p \in \mathbb{Z}[X] \\ \text{with degree 1 and even with leading coefficient } 1 \leq q < Q \\ \text{which is } \mathbb{Z} \text{ -primitive (i.e. } gcd(p,q) \sim 1) \\ \text{and such that } 0 < |g(\theta)| < \frac{1}{Q} \end{array}$$

By considering polynomials not just of degree 1, but of any degree, one can modify the criterion for a number to be rational into a criterion for a number to be algebraic (of any degree). This is exactly what Liouville did, as well as later mathematicians who generalized Liouville's result.

Liouville's criterion essentially takes up the idea that not only rational numbers, but also algebraic numbers in general cannot be very well approximated by rational numbers. So if a number can be very well approximated by rational numbers, then it must be transcendental. The exact meaning of "very well approximated" is explained in the next proposition called "Liouville's Approximation Theorem".

Liouville's criterion is unfortunately only a necessary condition for a number to be algebraic, and hence by taking the contrapositive, Liouville's criterion can be rewritten as a sufficient condition for a number to be transcendental. But his criterion was not strong enough to be necessary too, and indeed it fails to detect the transcendence of e, for example. However, it did provide a large class of real transcendental numbers. Liouville numbers have the privilege of a tight approximation by rational numbers. This fact is against our intuitive expectations, because it shows that in some respects real transcendental numbers are nearer to rational numbers than algebraic irrational numbers.

Here is the classical version of Liouville's criterion using an asymptotic estimate:

Theorem 2.4 *Let $\alpha \in \mathbb{C}$ be an algebraic number of degree $n \geq 1$. Then there exists a positive constant $c = c(\alpha) > 0$ depending only on α such that the inequality*

$$|\alpha - \frac{p}{q}| > \frac{c}{q^n} = \frac{c}{q^{deg(\alpha)}}$$

holds for all rational numbers $p/q \in \mathbb{Q} \setminus \{\alpha\}$ (with $p, q \in \mathbb{Z}, q > 0, gcd(p,q) \sim 1$) which are different from α.

Proof We can break up the proof into three different cases:

1. The case where $\alpha \in \mathbb{R}$ is an algebraic number of degree $n = 1$.

   That means (by Proposition 1.7) that α is rational. Hence, as we have seen before, by the contrapositive of condition (ii) of the irrationality

criterion, there exists $\varepsilon_0 > 0$ such that for any rational numbers p/q (with $p, q \in \mathbb{Z}, q > 0$ and $gcd(p, q) \sim 1$), we have: $|\alpha - \frac{p}{q}| = 0$ or $|\alpha - \frac{p}{q}| \geq \frac{\varepsilon_0}{q}$. So for any rational number p/q (with $p, q \in \mathbb{Z}, q > 0$ and $gcd(p, q) \sim 1$) which are different from α, we must have:

$$|\alpha - \frac{p}{q}| \geq \frac{\varepsilon_0}{q}$$

By taking $c := \varepsilon_0/2 > 0$ (which is a constant only depending on α), we get:

$$|\alpha - \frac{p}{q}| > \frac{c}{q} = \frac{c}{q^1} = \frac{c}{q^{deg(\alpha)}},$$

as wanted.

2. The case where $\alpha \in \mathbb{R}$ is a real algebraic number of degree $n \geq 2$.

   In this case, we have seen in Proposition 1.7 that α is necessarily an irrational number, because an algebraic number is of degree 1 if and only if it is a rational number. It follows, by Proposition 1.17, that there exists a non-constant polynomial $g \in \mathbb{Z}[X]$ with integral coefficients of degree $n \geq 2$ which is irreducible in $\mathbb{Q}[X]$ and which has α as root as well as a positive leading coefficient. Because $deg(g) = n \geq 2$ and because g is irreducible in $\mathbb{Q}[X]$, we know that this implies that g has no roots in $\mathbb{Q}$. Hence, we have that $g(p/q) \neq 0$ for all rational p/q (with $p, q \in \mathbb{Z}, q > 0$ and $gcd(p, q) \sim 1$).
   Let now p/q (with $p, q \in \mathbb{Z}, q > 0$ and $gcd(p, q) \sim 1$) be any rational number. We want to find a positive constant $c > 0$ depending only on α such that:

   $$|\alpha - \frac{p}{q}| > \frac{c}{q^n} = \frac{c}{q^{deg(\alpha)}}$$

   We do not need to consider rational numbers p/q different from α because α is irrational in our case.
   There are two subcases to consider:

   - $|\alpha - \frac{p}{q}| \geq 1$

     In this subcase, since $q > 0$ is a positive integer, we have $q \geq 1$, hence $q^2 \geq q \geq 1$, and so $q^n \geq q \geq 1$ for all $n \geq 2$. Therefore, we have

     $$0 < \frac{1}{q^n} \leq 1$$

     We then deduce that:

     $$|\alpha - \frac{p}{q}| \geq 1 \geq \frac{1}{q^n} > \frac{1}{2} \cdot \frac{1}{q^n}$$

By simply taking the constant $c := 1/2 > 0$ which is certainly independent of p/q, we get what we desired, that is:

$$|\alpha - \frac{p}{q}| > \frac{c}{q^n}$$

- $|\alpha - \frac{p}{q}| < 1$

  In this subcase, we write: $g = g(X) = a_n X^n + \dots a_1 X + a_0$ with $a_i \in \mathbb{Z}$ (and $a_n > 0$). So we have:

$$\begin{aligned} g\left(\frac{p}{q}\right) &= a_n \left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \dots + a_1\left(\frac{p}{q}\right) + a_0 \\ &= \frac{a_n p^n + a_{n-1}p^{n-1}q + \dots + a_1 p q^{n-1} + a_0 q^n}{q^n} \end{aligned}$$

  Since $g(\frac{p}{q}) \neq 0$ and since $q^n > 0$, then the numerator of the last big fraction is a non-zero integer, so we have:

$$|a_n p^n + a_{n-1}p^{n-1}q + \dots a_1 p q^{n-1} + a_0 q^n| \geq 1$$

  So we obtain:

$$|g\left(\frac{p}{q}\right)| = \frac{|a_n p^n + a_{n-1}p^{n-1}q + \dots + a_1 p q^{n-1} + a_0 q^n|}{q^n} \geq \frac{1}{q^n}$$

  Now, using the mean-value theorem for g, because g is certainly differentiable on $\mathbb{R}$, and hence on the open interval with distinct endpoints α and $\frac{p}{q}$, we obtain for some ξ between α and $\frac{p}{q}$ (by taking the absolute values):

$$|g\left(\frac{p}{q}\right)| = |0 - g\left(\frac{p}{q}\right)| = |g(\alpha) - g\left(\frac{p}{q}\right)| = |g'(\xi)| \cdot |\alpha - \frac{p}{q}|$$

  So considering the inequality $|g(\frac{p}{q})| \geq \frac{1}{q^n}$, we get:

$$\frac{1}{q^n} \leq |g'(\xi)| \cdot |\alpha - \frac{p}{q}| \tag{2.5}$$

  We want to majorate $|g'(\xi)|$. By the triangular inequality, we have: $|\xi| \leq |\xi - \alpha| + |\alpha|$. But in our subcase, $|\alpha - \frac{p}{q}| < 1$ and ξ lies between α and $\frac{p}{q}$, so we have $|\xi - \alpha| < 1$, and hence, we get the inequality $|\xi| < 1 + |\alpha|$.

  Now, for the derivative

$$g'(X) = n a_n X^{n-1} + (n-1)a_{n-1}X^{n-2} + \dots + a_1,$$

evaluated at ξ, we get:

$$g'(\xi) = na_n\xi^{n-1} + (n-1)a_{n-1}\xi^{n-2} + \ldots + a_1$$

We set $A := max(|a_1|, |a_2|, \ldots, |a_n|)$ which is a positive constant (since $a_n \neq 0$), only depending on g, hence on α. So, again by the triangular inequality, we get:

$$\begin{aligned}|g'(\xi)| &\leq n|a_n| \cdot |\xi|^{n-1} + (n-1)|a_{n-1}| \cdot |\xi|^{n-2} + \ldots + |a_1| \\ &\leq nA \cdot (|\xi|^{n-1} + |\xi|^{n-2} + \ldots + |\xi|^0) \\ &\qquad \text{(since } |a_i| \leq A \text{ for } i = 1, 2, \ldots, n) \\ &\leq nA \cdot [(1+|\alpha|)^{n-1} + (1+|\alpha|)^{n-2} + \ldots + (1+|\alpha|)^0]\end{aligned}$$

But since $(1+|\alpha|)^{n-i} \leq (1+|\alpha|)^{n-1}$ for all $i = 1, \ldots, n$, because $1 + |\alpha| \geq 1$ and $n \geq 2$, we obtain:

$$|g'(\xi)| \leq n \cdot A \cdot n \cdot (1+|\alpha|)^{n-1} = n^2 \cdot A \cdot (1+|\alpha|)^{n-1}$$

The constant $K := n^2 \cdot A \cdot (1+|\alpha|)^{n-1}$ is a positive constant only depending on α which satisfies

$$|g'(\xi)| \leq K \tag{2.6}$$

By multiplying both sides of (2.6) by $|\alpha - \frac{p}{q}| > 0$ (because α is irrational) and by considering (2.5), we get the inequalities:

$$\frac{1}{q^n} \leq |g'(\xi)| \cdot |\alpha - \frac{p}{q}| \leq K \cdot |\alpha - \frac{p}{q}|$$

which implies that

$$|\alpha - \frac{p}{q}| \geq \frac{1}{K} \cdot \frac{1}{q^n} > \frac{1}{2K} \cdot \frac{1}{q^n}$$

By taking $c := \frac{1}{2K} > 0$, we get the desired result.

3. The case where $\alpha \in \mathbb{C} \setminus \mathbb{R}$ is a *non-real* algebraic number.

   Then α is necessarily of degree $n \geq 2$ (otherwise it is rational by Proposition 1.7 and hence real, which is a contradiction). So by Proposition 1.13, since α is an algebraic number of degree n, then $\mathfrak{Re}(\alpha)$ is also an algebraic number with degree m with $1 \leq m \leq n$.
   Since $\mathfrak{Re}(\alpha)$ is a real algebraic number of degree $m \geq 1$, we can apply the proven cases 1 and 2 of Liouville's Approximation Theorem to get a positive constant $\tilde{c} = \tilde{c}(\mathfrak{Re}(\alpha)) > 0$ depending only on $\mathfrak{Re}(\alpha)$ such that the inequality

$$|\mathfrak{Re}(\alpha) - \frac{p}{q}| > \frac{\tilde{c}}{q^m} \tag{2.7}$$

holds for all rational numbers $p/q \in \mathbb{Q} \setminus \{\mathfrak{Re}(\alpha)\}$ (with $p, q \in \mathbb{Z}$, $q > 0$ and $gcd(p,q) \sim 1$) which are different from $\mathfrak{Re}(\alpha)$.
Now consider any rational number p/q (with $p, q \in \mathbb{Z}$, $q > 0$ and $gcd(p,q) \sim 1$) (which is necessarily different from α in our case).
Again we distinguish two subcases:

- If $\frac{p}{q} \neq \mathfrak{Re}(\alpha)$, then we surely have, using (2.7):

$$\begin{aligned} |\alpha - \frac{p}{q}| &= |(\mathfrak{Re}(\alpha) - \frac{p}{q}) + i\mathfrak{Im}(\alpha)| \\ &= \sqrt{\left(\mathfrak{Re}(\alpha) - \frac{p}{q}\right)^2 + (\mathfrak{Im}(\alpha))^2} \\ &\geq |\left(\mathfrak{Re}(\alpha) - \frac{p}{q}\right)| \\ &> \frac{\tilde{c}}{q^m} \\ &\geq \frac{\tilde{c}}{q^n} \end{aligned}$$

  because $1 \leq m \leq n$ and $q > 0$ implies that $1 \leq q^m \leq q^n$, which in turn implies that $\frac{\tilde{c}}{q^m} \geq \frac{\tilde{c}}{q^n}$, since $\tilde{c} > 0$.

- If $\frac{p}{q} = \mathfrak{Re}(\alpha)$, then we have trivially:

$$\begin{aligned} |\alpha - \frac{p}{q}| &= |(\mathfrak{Re}(\alpha) - \frac{p}{q}) + i\mathfrak{Im}(\alpha)| \\ &= |i\mathfrak{Im}(\alpha)| \\ &= |\mathfrak{Im}(\alpha)| \\ &> \frac{\mathfrak{Im}(\alpha)}{2} \cdot 1 \\ &\geq \frac{\frac{\mathfrak{Im}(\alpha)}{2}}{q^n} \end{aligned}$$

  since $q > 0$ and $n \geq 2$ imply that $q^n \geq 1$, which in turn implies that $\frac{1}{q^n} \leq 1$.

So by setting $c := min(\tilde{c}, \frac{\mathfrak{Im}(\alpha)}{2}) > 0$, we surely have for any rational number p/q (with $p, q \in \mathbb{Z}, q > 0$ and $gcd(p,q) \sim 1$) that

$$|\alpha - \frac{p}{q}| > \frac{c}{q^n},$$

as wanted. □

2.2.1 Liouville Numbers

Liouville's Approximation Theorem allowed Liouville to construct the first transcendental number in 1844, now called the Liouville constant, which is the number:

$$\alpha := \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$$

i.e.

$$\alpha = 0.11000100000000000000000100000000000000000000000000000000 \curvearrowright$$
$$00000000000000000000000000000000000000000000000000000001\ldots$$

with a digit 1 in its decimal expansion at the positions $1! = 1$ and $2! = 2$ and $3! = 6$ and $4! = 24$ and $5! = 120$, etc.

Remark 2.5 *The series defining α is convergent, since it is dominated by the geometric series $\sum_{k=1}^{\infty} \frac{1}{10^k}$, hence α is a real number. Moreover, α is obviously an irrational number, because its decimal expansion is not eventually periodic, because it has arbitrarily long strings of 0's since the 1's appear at ever growing positions after the decimal point.*

Proposition 2.6 *(Liouville constant) The Liouville constant $\alpha := \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ is a transcendental number.*

Proof Suppose α is an algebraic number. Then necessarily, since $\alpha \notin \mathbb{Q}$, we have that α is of degree $n \geq 2$. Hence by Liouville's Approximation Theorem, we can find a positive constant $c = c(\alpha) > 0$ such that the inequality

$$|\alpha - \frac{p}{q}| > \frac{c}{q^n} \tag{2.8}$$

holds for all rational numbers $p/q \in \mathbb{Q}$ (with $p, q \in \mathbb{Z}, q > 0, gcd(p, q) \sim 1$). We do not need to require that p/q be different from α, since α is irrational. Let $i \in \mathbb{N}$ be large enough so that

$$\frac{2}{10^{(n+i)! \cdot i}} < c \tag{2.9}$$

(This is possible, since $c > 0$ and the sequence $\{\frac{2}{10^{(n+i)! \cdot i}}\}_{i=1}^{\infty}$ goes to 0 as i goes to ∞).
Set $j := n + i$ so that, with this new notation, we have

$$\frac{2}{10^{j! \cdot i}} < c$$

Now consider the number p/q with $q := 10^{j!}$ and

$$\begin{aligned} p &:= 10^{j!} \cdot \sum_{k=1}^{j} \frac{1}{10^{k!}} \\ &= 10^{j!} \cdot (\frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \ldots + \frac{1}{10^{j!}}) \\ &= 10^{j!-1!} + 10^{j!-2!} + \ldots + 10^{j!-j!} \\ &= 10^{j!-1!} + 10^{j!-2!} + \ldots + 1 \end{aligned}$$

so that

$$\frac{p}{q} = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \ldots + \frac{1}{10^{j!}} = \sum_{k=1}^{j} \frac{1}{10^{k!}}$$

We certainly have that $p, q \in \mathbb{Z}, q > 0$ and $gcd(p, q) \sim 1$. So p/q is a relevant rational number which satisfies inequality (2.8):

$$|\alpha - \frac{p}{q}| > \frac{c}{q^n}$$

We will show that we also have:

$$|\alpha - \frac{p}{q}| \leq \frac{c}{q^n} \tag{2.10}$$

which is a contradiction, hence α is not an algebraic number, hence it is transcendental.
To prove inequality (2.10), we write:

$$\begin{aligned} |\alpha - \frac{p}{q}| &= \sum_{k=j+1}^{\infty} \frac{1}{10^{k!}} \\ &= \frac{1}{10^{(j+1)!}} + \frac{1}{10^{(j+2)!}} + \frac{1}{10^{(j+3)!}} + \frac{1}{10^{(j+4)!}} + \ldots \\ &= \frac{1}{10^{(j+1)!}} + \frac{1}{10^{(j+1)!(j+2)}} + \frac{1}{10^{(j+1)!(j+2)(j+3)}} + \frac{1}{10^{(j+1)!(j+2)(j+3)(j+4)}} + \ldots \\ &\leq \frac{1}{10^{(j+1)!}} + \frac{1}{10^{(j+1)! \cdot 1}} + \frac{1}{10^{(j+1)! \cdot 2}} + \frac{1}{10^{(j+1)! \cdot 3}} + \ldots \end{aligned}$$

Hence we have:

$$|\alpha - \frac{p}{q}| \leq \frac{1}{10^{(j+1)!}} \cdot (1 + \frac{1}{10} + \frac{1}{10^2} + \frac{1}{10^3} + \ldots)$$

But the last series in parentheses is a geometric series equal to

$$1 + \frac{1}{10} + \frac{1}{10^2} + \frac{1}{10^3} + \ldots = \frac{1}{1 - \frac{1}{10}} = \frac{10}{9} < 2$$

So we have, since $j := n + i$:

$$|\alpha - \frac{p}{q}| < \frac{1}{10^{(j+1)!}} \cdot 2 = \frac{2}{10^{j! \cdot (j+1)}} < \frac{2}{10^{j! \cdot j}} = \frac{2}{10^{j! \cdot (n+i)}} = \frac{2}{10^{j! \cdot i}} \cdot \frac{1}{10^{j! \cdot n}}$$

Now because $q := 10^{j!}$ and since $\frac{2}{10^{j! \cdot i}} < c$, we obtain:

$$|\alpha - \frac{p}{q}| < c \cdot \frac{1}{q^n} \tag{2.11}$$

which certainly implies the large inequality (2.10). □

The same idea can be used to prove that the number

$$\alpha := \sum_{k=1}^{\infty} \frac{1}{b^{k!}}$$

with b being any integer ≥ 2 is a transcendental number, or more generally, that the number

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

with b being any integer ≥ 2 and with $\{a_k\}_{k=1}^{\infty}$ being any sequence of integers such that $a_k \in \{0, 1, 2, \ldots, b-1\}$ for all k and $a_k \neq 0$ for infinitely many k, is also a transcendental number.
In fact, we can construct in a similar manner infinitely many transcendental numbers. They form a class of transcendental numbers, which we now call Liouville numbers in honour of Liouville.

Definition 2.7 *(Liouville Numbers) A Liouville number is a real number α with the property that, for every positive integer $n \geq 1$, there exists a pair of integers (p, q) with $q > 1$ (i.e. $q \geq 2$) such that*

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

Liouville numbers can be approximated "quite closely" by rational numbers. They are precisely the transcendental numbers that can be more closely approximated by rational numbers than any algebraic irrational number.

Remark 2.8 *The Liouville constant is an example of a Liouville number. Indeed, it suffices to adapt the proof of Proposition 2.6, by taking $i \in \mathbb{N}$ large enough so that*

$$\frac{2}{10^{(n+i)! \cdot i}} < 1 \tag{2.12}$$

(This is possible, since the corresponding sequence goes to 0 as i goes to ∞).
Then by setting $j := n + i$ and considering the rational number p/q with $q := 10^{j!}$ and

$$\begin{aligned} p &:= 10^{j!} \cdot \sum_{k=1}^{j} \frac{1}{10^{k!}} \\ &= 10^{j!} \cdot (\frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \ldots + \frac{1}{10^{j!}}) \\ &= 10^{j!-1!} + 10^{j!-2!} + \ldots + 10^{j!-j!} \\ &= 10^{j!-1!} + 10^{j!-2!} + \ldots + 1 \end{aligned}$$

we can prove inequality (2.11) with $c = 1$, namely:

$$|\alpha - \frac{p}{q}| < \frac{1}{q^n} \tag{2.13}$$

as wanted.

Here is an expected proposition:

Proposition 2.9 *Liouville numbers are transcendental.*

Proof Let α be a Liouville number. First, we show that α must be irrational. Assume the contrary, i.e. $\alpha = a/b$ for some integers a and b with $b > 0$. Let n be a positive integer large enough so that $2^{n-1} > b$ (i.e. $n > 1 + log_2(b)$). Then for any pair of integers (p, q) with $q > 1$, we will prove that

$$0 = \left|\alpha - \frac{p}{q}\right| \text{ or } \left|\alpha - \frac{p}{q}\right| \geq \frac{1}{q^n}, \tag{2.14}$$

which is a contradiction to the definition of a Liouville number. Hence α is irrational, as wanted.
Indeed, for any pair of integers (p, q) with $q > 1$, we have;

$$|\alpha - \frac{p}{q}| = |\frac{a}{b} - \frac{p}{q}| = \frac{|aq - bp|}{bq}$$

If $|aq - bp| = 0$, we would have

$$|\alpha - \frac{p}{q}| = \frac{|aq - bp|}{bq} = 0,$$

meaning that such a pair (p, q) satisfies the first equality in (2.14), irrespective of any choice of n.
If, on the other hand, $|aq - bp| > 0$, then, since $aq - bp$ is an integer, we can assert the sharper inequality $|aq - bp| \geq 1$. From this, it follows that

$$|\alpha - \frac{p}{q}| = \frac{|aq - bp|}{bq} \geq \frac{1}{bq}$$

Now the last inequality implies

$$|\alpha - \frac{p}{q}| \geq \frac{1}{bq} > \frac{1}{2^{n-1}q} \geq \frac{1}{q^n}$$

(by choice of $n > 1 + log_2(b)$ and because $q \geq 2 \Longrightarrow 2^{n-1}q \leq q^n$).
Therefore, in this case, such pair of integers (p, q) satisfies the second inequality in (2.14), for some large enough positive n. Thus, we have established (2.14), as wanted.
Now, assume α is an irrational algebraic number, i.e. assume α is a real algebraic number of degree $n \geq 2$. By Liouville's Approximation Theorem, there exists a positive constant $c > 0$ such that

$$|\alpha - \frac{p}{q}| > \frac{c}{q^n} \tag{2.15}$$

holds for all integers p and q with $q > 0$ and $gcd(p, q) \sim 1$. Let r be a positive integer for which $2^r \geq 1/c$. Since α is a Liouville number, then for the positive integer $n + r$, there are integers p^* and q^* with $q^* > 1$ such that

$$|\alpha - \frac{p^*}{q^*}| < \frac{1}{(q^*)^{n+r}} \leq \frac{1}{2^r(q^*)^n} \leq \frac{c}{(q^*)^n}$$

(by choice of r and because $q^* \geq 2 \Longrightarrow 2^r \leq (q^*)^r$).
This contradicts (2.15) and, hence, establishes that α is transcendental. □

We can ask ourselves whether the Liouville numbers form a big set of transcendental numbers or not. The next proposition given without proof answers this question:

Proposition 2.10 *The set of Liouville numbers in* $[0, 1]$ *has measure 0.*

We have seen that all Liouville numbers are transcendental. But the converse is not true. Indeed:

Corollary 2.11 *There are transcendental numbers which are not Liouville numbers.*

Proof Since the set $\mathbb{A}$ of algebraic numbers is countable, the set of real algebraic numbers in $[0, 1]$ has certainly measure 0. Hence, the set of real transcendental numbers in $[0, 1]$ has measure infinite (equal to the power of the continuum), like the measure of $[0, 1]$. Hence the set of real transcendental numbers in $[0, 1]$ cannot be the set of Liouville numbers in $[0, 1]$, because their measure differ (enormously!) □

Finding a transcendental number which is not a Liouville number is not easy. The numbers e and π are two such examples. One can prove for example that e is not a Liouville number by considering its expansion in simple continued fractions, but we will not give the proof here.

2.2.2 Generalizations of Liouville's Approximation Theorem

Let α be an irrational algebraic real number of degree $n \geq 2$.
Liouville's Approximation Theorem states that there exists a positive constant $c = c(\alpha) > 0$ such that

$$|\alpha - \frac{p}{q}| > \frac{c}{q^n} \tag{2.16}$$

holds for all rational numbers $p/q \in \mathbb{Q}$ (with $p, q \in \mathbb{Z}$, $q > 0$ and $gcd(p, q) \sim 1$).

On the other hand, since α is irrational, the Asymptotic Dirichlet's Theorem states that there exist infinitely many rational numbers $p/q \in \mathbb{Q}$ (with $p, q \in \mathbb{Z}$, $q > 0$ and $gcd(p, q) \sim 1$) such that

$$|\alpha - \frac{p}{q}| < \frac{1}{q^2} \tag{2.17}$$

For $n = 2$, we see that both estimates (2.16) and (2.17) are sharp. This is no longer true for $n \geq 3$. We discuss here improvements of Liouville's Approximation Theorem; these improvements are deep and we state them without proof.

Those statements, in which the exponent k will be specified below in Theorems 2.12 to 2.15, have to be understood as follows:

For every irrational algebraic number α of degree n (necessarily ≥ 2) and for any positive real number $\varepsilon > 0$, there are only finitely many rational numbers $p/q \in \mathbb{Q}$ (with $p, q \in \mathbb{Z}$, $q > 0$ and $gcd(p, q) \sim 1$) which satisfy the inequality:

$$|\alpha - \frac{p}{q}| < \frac{1}{q^{k+\varepsilon}}. \tag{2.18}$$

As a consequence, we can state:
For every irrational algebraic number α of degree n (necessarily ≥ 2) and for any positive real number $\varepsilon > 0$, there exists a positive constant $c = c(\alpha, \varepsilon) > 0$ depending only on α and ε such that the inequality

$$|\alpha - \frac{p}{q}| > \frac{c}{q^{k+\varepsilon}} \tag{2.19}$$

holds for any rational number $p/q \in \mathbb{Q}$ (with $p, q \in \mathbb{Z}$, $q > 0$ and $gcd(p, q) \sim 1$).

We can convince ourselves that the case $k = n$ in the inequality (2.19) gives a version of Liouville's Approximation Theorem.

Liouville's Approximation Theorem has been strengthened over the years by successively improving the exponent k:

Theorem 2.12 *(Thue 1909) If $n \geq 3$, the inequality (2.19) holds true for $k = \frac{n}{2} + 1$*

Theorem 2.13 *(Siegel 1921) If $n \geq 3$, the inequality (2.19) holds true for $k = 2\sqrt{n}$*

Theorem 2.14 *(Dyson 1947) If $n \geq 3$, the inequality (2.19) holds true for $k = \sqrt{2n}$*

Theorem 2.15 *(Roth 1955) If $n \geq 2$, the inequality (2.19) holds true for $k = 2$*

We note that all those theorems are not currently effective, i.e. there is no bound known on the possible values of p, q given α.

Theorem 2.15 had been conjectured by Siegel in 1921. Even though Thue, Siegel, and Dyson had successively improved Liouville's original exponent n, it was Roth who proved Siegel's conjectured exponent in 1955, and won a Fields Medal for this work. Still, Theorem 2.15 is often called the Thue-Siegel-Roth Theorem. It is the best possible of its kind; the exponent 2 cannot indeed be decreased, because Roth's statement would fail on setting $\varepsilon = 0$ due to the Asymptotic Dirichlet's Theorem.

There is a stronger conjecture of Serge Lang that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2 \log(q)^{1+\varepsilon}}$$

can have only finitely many solutions in integers p and q.

Chapter 3

Transcendence of e

We will explain the original proof of the transcendence of e, as discovered by Hermite in 1873. Before starting with the proof, we need to state some preliminary results.

3.1 Preliminaries

We start by introducing an auxiliary function which will happen to be very useful in the proof of the transcendence of e.

Definition 3.1 *(Auxiliary function) For any polynomial $f \in \mathbb{R}[X]$ (of whatever degree ≥ 1) and for any complex number $t \in \mathbb{C}$, let $I(t;f)$ denote the following function*

$$I(t;f) := \int_\gamma e^{t-z} f(z)\, dz,$$

where γ is the line joining 0 and t in the complex plane, i.e.

$$\begin{array}{rccc} \gamma: & [0,1] & \to & \mathbb{C} \\ & \theta & \mapsto & \gamma(\theta) := \theta t \end{array}$$

By definition of complex line integrals, we have:

$$I(t;f) := \int_0^1 e^{t-\gamma(\theta)} f(\gamma(\theta))\gamma'(\theta) d\theta = \int_0^1 e^{t-\theta t} f(\theta t) t\, d\theta$$

Remark 3.2 *By Cauchy's theorem, since the function $z \mapsto e^{t-z} f(z)$ is holomorphic on the domain $\mathbb{C}$, the complex line integral $I(t;f)$ is the same over any piecewise continuously differentiable path joining 0 and t in $\mathbb{C}$ and depends only on the endpoints 0 and t. That is why we can simply write without ambiguity:*

$$I(t;f) = \int_0^t e^{t-z} f(z)\, dz$$

We will now mention some small properties of $I(t;f)$.

Lemma 3.3 *With the same notations as before, we have:*

$$I(t;f) = e^t f(0) - f(t) + I(t;f')$$

Proof We recall the formula about partial integration: Let v, w be two holomorphic functions on a domain $G \subseteq \mathbb{C}$. Let $\gamma : [a,b] \to G$ be continuous and piecewise differentiable. Then the following holds:

$$\int_\gamma v(z)w'(z)dz = [v(z)w(z)]_{\gamma(a)}^{\gamma(b)} - \int_\gamma v'(z)w(z)dz$$

By simply applying this formula to the line γ joining 0 and t and to the following functions:

$$\begin{cases} v := f(z) \rightsquigarrow dv = f'(z)dz \\ dw := e^{t-z}dz \rightsquigarrow w = -e^{t-z} \end{cases}$$

we get:

$$\begin{aligned} I(t;f) &= \int_\gamma v(z)w'(z)dz \\ &= [-e^{t-z}f(z)]_0^t - \int_0^t (-e^{t-z})f'(z)dz \\ &= -e^{t-t}f(t) + e^{t-0}f(0) + I(t;f') \\ &= e^t f(0) - f(t) + I(t;f'), \end{aligned}$$

as desired. □

By iterating the process in Lemma 3.3, we obtain for any polynom $f \in \mathbb{R}[X]$ of degree m:

Lemma 3.4 *With the same notations as before, and for any polynom $f \in \mathbb{R}[X]$ of degree m, we have:*

$$I(t;f) = e^t \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(t)$$

Proof We apply Lemma 3.3 to $f, f', f'', \ldots, f^{(m)}$ to obtain:

$$\begin{aligned} I(t;f) &= e^t f(0) - f(t) + I(t;f') \\ I(t;f') &= e^t f'(0) - f'(t) + I(t;f'') \\ I(t;f'') &= e^t f''(0) - f''(t) + I(t;f''') \\ &\vdots \\ I(t;f^{(m)}) &= e^t f^{(m)}(0) - f^{(m)}(t) + I(t;f^{(m+1)}) \end{aligned}$$

But $deg(f) = m$, hence $f^{(m+1)} \equiv 0$, so we have: $I(t; f^{(m+1)}) = \int_\gamma e^{t-z} \cdot 0 \, dz = 0$.
Putting together all those equalities, we get:

$$I(t;f) = e^t f(0) - f(t) + e^t f'(0) - f'(t) + e^t f''(0) - f''(t) + \ldots + e^t f^{(m)}(0) - f^{(m)}(t)$$

which equals to:

$$I(t;f) = e^t \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(t),$$

as desired. □

Now we are interested in finding an upper bound for $|I(t;f)|$ when $f \in \mathbb{R}[X]$ is a polynomial with real coefficients of degree m:

Lemma 3.5 *With the same notations as before, and for any polynom $f \in \mathbb{R}[X]$ of degree m, we have:*

$$|I(t;f)| \leq |t| \cdot e^{|t|} \cdot sup_{\xi \in \mathbb{C}, |\xi| \leq |t|} \, |f(\xi)|$$

Proof The proof is based on the triangular inequality for integrals. We have by definition of the auxiliary function:

$$|I(t;f)| = |\int_0^1 e^{t-\theta t} f(\theta t) t \, d\theta| \leq \int_0^1 |e^{t-\theta t}| \cdot |f(\theta t)| \cdot |t| \, d\theta$$

But we know that $|e^z| = e^{\mathfrak{Re}(z)}$ and $\mathfrak{Re}(z) \leq |z|$ for all $z \in \mathbb{C}$, so we obtain for all $\theta \in [0,1]$:

$$|e^{t-\theta t}| = e^{\mathfrak{Re}(t-\theta t)} \leq e^{|t-\theta t|} = e^{|t| \cdot |1-\theta|} \leq e^{|t| \cdot 1} = e^{|t|}$$

Now, for the term $|f(\theta t)|$, we have for all $\theta \in [0,1]$:

$$|f(\theta t)| \leq sup_{\theta \in [0,1]} |f(\theta t)| \leq sup_{\xi \in \mathbb{C}, |\xi| \leq |t|} \, |f(\xi)|$$

since $|\theta t| \leq |t|$. Now putting those inequalities together, we obtain:

$$|I(t;f)| \leq |t| \cdot e^{|t|} \cdot sup_{\xi \in \mathbb{C}, |\xi| \leq |t|} \, |f(\xi)| \cdot \int_0^1 d\theta,$$

which gives the desired upper bound. □

Now, we consider a particular polynom $f \in \mathbb{R}[X]$:

$$f = f(X) = X^{p-1}(X-1)^p \ldots (X-n)^p$$

where $n \in \mathbb{N}^{\geq 1}$ and p is any positive integer greater than 2.
We note that the degree of f is:

$$deg(f) = p - 1 + np = (n+1)p - 1$$

We also note that the roots of f are $0, 1, 2, \ldots, n$. The root 0 is a root of order $p-1$, and the root k for $k = 1, 2, \ldots, n$ is a root of order p. Therefore we certainly have:

$$\begin{cases} f^{(j)}(0) = 0 \text{ for } 0 \leq j < p-1 \\ f^{(j)}(k) = 0 \text{ for } 0 \leq j < p \quad (k = 1, 2, \ldots, n) \end{cases}$$

We can give a formula for the successive derivatives of f at the root 0:

Lemma 3.6 *For the particular polynom $f = f(X) = X^{p-1}(X-1)^p \ldots (X-n)^p$ (with $p \in \mathbb{N}^{\geq 2}$), we have:*

$$f^{(j)}(0) = \begin{cases} 0 & \text{if } 0 \leq j \leq p-2 \\ (p-1)!(0-1)^p \ldots (0-n)^p = (p-1)!(-1)^{np}(n!)^p & \text{if } j = p-1 \\ \equiv 0 \,(mod\, p!) & \text{if } j \geq p \end{cases}$$

Proof The first case when $0 \leq j \leq p-2$ follows from the order $p-1$ of the root 0 of f, as already discussed.
We note that f is of the form: $f(X) = X^{p-1} \cdot (g(X))^p$ with

$$g(X) = (X-1) \cdot \ldots \cdot (X-n) \in \mathbb{Z}[X]$$

Now, by the Leibniz's formula, we get:

$$f^{(p-1)}(X) = \sum_{r=0}^{p-1} \binom{p-1}{r} (X^{p-1})^{(r)} \cdot ((g(X))^p)^{(p-1-r)}$$

But for the r^{th} derivative of the monomial X^{p-1}, we have:

$$\begin{cases} (X^{p-1})^{(r)} = (p-1)(p-2)\ldots(p-r)X^{p-1-r} & \text{for } 0 \leq r \leq p-1 \\ (X^{p-1})^{(r)} \equiv 0 & \text{for } r \geq p \end{cases}$$

So, evaluated at $X = 0$, we get:

$$(X^{p-1})^{(r)}\Big|_{X=0} \neq 0 \text{ only when } r = p-1,$$

in which case we get:

$$(X^{p-1})^{(p-1)}\Big|_{X=0} = (p-1)!$$

This implies in the second case when $j = p-1$ that:

$$\begin{aligned}
f^{p-1}(X)\Big|_{X=0} &= \sum_{r=0}^{p-1} \binom{p-1}{r} (X^{p-1})^{(r)}\Big|_{X=0} \cdot ((g(X))^p)^{(p-1-r)}\Big|_{X=0} \\
&= \sum_{r=0}^{p-2} \binom{p-1}{r} (X^{p-1})^{(r)}\Big|_{X=0} \cdot ((g(X))^p)^{(p-1-r)}\Big|_{X=0} \\
&\qquad + (X^{p-1})^{(p-1)}\Big|_{X=0} \cdot ((g(X))^p)^{(p-1-(p-1))}\Big|_{X=0} \\
&= 0 + (p-1)! \cdot (g(0))^p \\
&= (p-1)!(0-1)^p(0-2)^p \dots (0-n)^p \\
&= (p-1)!(-1)^{np}(1 \cdot 2 \cdot \ldots \cdot n)^p \\
&= (p-1)!(-1)^{np}(n!)^p,
\end{aligned}$$

as desired.
Now, for the third case when $j \geq p$, we get again by the Leibniz's formula:

$$f^{(j)}(X) = \sum_{r=0}^{j} \binom{j}{r} (X^{p-1})^{(r)} \cdot ((g(X))^p)^{(j-r)}$$

Since we have that $(X^{p-1})^{(r)} \equiv 0$ for $r \geq p$, the sum in the formula for the j^{th} derivative of f with $j \geq p$ is reduced to the following sum:

$$f^{(j)}(X) = \sum_{r=0}^{p-1} \binom{j}{r} (X^{p-1})^{(r)} \cdot ((g(X))^p)^{(j-r)}$$

Now, evaluated at $X = 0$, we get:

$$f^{(j)}(X)\Big|_{X=0} = \sum_{r=0}^{p-1} \binom{j}{r} (X^{p-1})^{(r)}\Big|_{X=0} \cdot ((g(X))^p)^{(j-r)}\Big|_{X=0}$$

But since the term $(X^{p-1})^{(r)}\Big|_{X=0}$ is not zero only for $r = p-1$, in which case it is equal to $(p-1)!$, we get:

$$\begin{aligned}
f^{(j)}(X)\Big|_{X=0} &= \binom{j}{p-1} (X^{p-1})^{(p-1)}\Big|_{X=0} \cdot ((g(X))^p)^{(j-(p-1))}\Big|_{X=0} \\
&= \binom{j}{p-1} (p-1)! \cdot ((g(X))^p)^{(j-(p-1))}\Big|_{X=0}
\end{aligned}$$

Now for $j \geq p$, we certainly have that the order $j-(p-1)$ of the derivative of $(g(X))^p$ is strictly positive.

Let us calculate the i^{th} derivative $((g(X))^p)^{(i)}$ for any $i > 0$.
We have from the chain rule:

$$\begin{aligned}(g(X))^p)^{(i)} &= (((g(X))^p)')^{(i-1)} \\ &= [p \cdot (g(X))^{p-1} \cdot g'(X)]^{(i-1)} \\ &= p \cdot [(g(X))^{p-1} \cdot g'(X)]^{(i-1)}\end{aligned}$$

So for $i = j - (p-1) > 0$ (in the case when $j \geq p$), we get for the evaluation at $X = 0$:

$$\begin{aligned}((g(X))^p)^{(j-(p-1))}\Big|_{X=0} &= p \cdot [(g(X))^{p-1} \cdot g'(X)]^{(j-(p-1)-1)}\Big|_{X=0} \\ &= p \cdot [(g(0))^{p-1} \cdot g'(0)]^{(j-p)} \\ &= p \cdot l,\end{aligned}$$

where $l := [(g(0))^{p-1} \cdot g'(0)]^{(j-p)}$.

But the polynomial $(g(X))^{p-1} \cdot g'(X)$ has integral coefficients, as a product of two such polynomials, because $g(X) = (X-1)\dots(X-n) \in \mathbb{Z}[X]$, hence not only $g'(X) \in \mathbb{Z}[X]$, but also $(g(X))^{p-1} \in \mathbb{Z}[X]$.
So, the number l is in fact an integer, as it is the constant term of a polynomial with integral coefficients.
Therefore, for the case $j \geq p$, we have that:

$$f^{(j)}(0) = f^{(j)}(X)\Big|_{X=0} = \binom{j}{p-1}(p-1)! \cdot p \cdot l$$

is an integer divisible by $(p-1)! \cdot p = p!$ (because $\binom{j}{p-1}$ and l are both integers), which implies that, in the case when $j \geq p$:

$$f^{(j)}(0) \equiv 0 \,(mod\ p!),$$

as desired. □

We can also give a formula for the successive derivatives of f at any other roots $k = 1, 2, \dots, n$:

Lemma 3.7 *For the particular polynom $f = f(X) = X^{p-1}(X-1)^p \dots (X-n)^p$ (with $p \in \mathbb{N}^{\geq 2}$), we have for $k = 1, \dots, n$:*

$$f^{(j)}(k) = \begin{cases} 0 & \text{if } 0 \leq j \leq p-1 \\ \equiv 0 \,(mod\ p!) & \text{if } j \geq p \end{cases}$$

Proof The first case when $0 \leq j \leq p-1$ is obvious, as mentioned before, because k (with $k = 1, \dots, n$) is a zero of f of order p.

The second case, when $j \geq p$, is the same as before. Indeed, as in the proof of Lemma 3.6, we arrive at the conclusion:

$$f^{(j)}(k) = \binom{j}{p-1}(p-1)! \cdot p \cdot [(g(k))^{p-1} \cdot g'(k)]^{(j-p)} = \binom{j}{p-1}(p-1)! \cdot p \cdot \tilde{l}$$

where $\tilde{l} := [(g(k))^{p-1} \cdot g'(k)]^{(j-p)} \in \mathbb{Z}$. So $f^{(j)}(k)$ is certainly an integer divisible by $(p-1)! \cdot p = p!$ (because $\binom{j}{p-1}$ and $\tilde{l}$ are both integers), hence the desired result. □

3.2 The Original Proof of Hermite

Now we can turn to the main proof of the transcendence of e which is a proof by contradiction.
Assume e is an algebraic number. Since e is irrational (see Section 2.1.1), we know that if e is an algebraic number, it should be an algebraic number of degree $n \geq 2$. By Proposition 1.17, this means that there exists a polynomial

$$g = g(X) = a_n X^n + \ldots + a_1 X + a_0 \in \mathbb{Z}[X]$$

with integral coefficients of degree $n \geq 2$, having e as a root, and being irreducible in $\mathbb{Q}[X]$ (as well as with positive leading coefficient).
In other words, there exist $n \in \mathbb{N}^{\geq 2}$ and $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ with $a_n \neq 0$ (even $a_n > 0$) such that:

$$g(e) = a_n \cdot e^n + \ldots + a_1 \cdot e + a_0 = 0$$

We can further assume that $a_0 \neq 0$, because otherwise, g would not have any constant term and hence g would have 0 as a root, which is a contradiction, because any irreducible polynomial in $\mathbb{Q}[X]$ of degree at least 2 has no rational root.
We now consider the previous polynomial $f \in \mathbb{Z}[X]$, namely:

$$f = f(X) = X^{p-1}(X-1)^p \ldots (X-n)^p,$$

but only for a large positive *prime* number p, such that $p > n$ and also such that $p > |a_0|$.
Let m denote the degree of f, i.e. $m = (n+1)p - 1$. We certainly have, since $p \geq 2$, that $m \geq p$.
We consider the following combination involving the auxiliary function $I(t; f)$ defined in (3.1) for $t = 0, 1, 2, \ldots, n$:

$$J := a_0 \cdot I(0; f) + a_1 \cdot I(1; f) + \ldots + a_n \cdot I(n; f) = \sum_{k=0}^{n} a_k \cdot I(k; f)$$

where the a_i's are the integral coefficients of g.
We claim that

$$J = -\sum_{k=0}^{n} a_k \sum_{j=0}^{m} f^{(j)}(k) \tag{3.1}$$

Indeed, we have via Lemma 3.4:

$$\begin{aligned} J &= a_0 I(0;f) + a_1 I(1;f) + \ldots + a_n I(n;f) \\ &= a_0 \left(e^0 \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(0) \right) + a_1 \left(e^1 \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(1) \right) \\ &\qquad + \ldots + a_n \left(e^n \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(n) \right) \\ &= \sum_{j=0}^{m} f^{(j)}(0) \cdot (a_0 e^0 + a_1 e^1 + \ldots + a_n e^n) - a_0 \sum_{j=0}^{m} f^{(j)}(0) - \ldots - a_n \sum_{j=0}^{m} f^{(j)}(n) \end{aligned}$$

Since $a_0 e^0 + a_1 e^1 + \ldots + a_n e^n = g(e) = 0$, we get:

$$J = -\sum_{k=0}^{n} a_k \sum_{j=0}^{m} f^{(j)}(k),$$

as claimed.

CLAIM 1: $J \in \mathbb{Z}$

This is clearly true, using Equation (3.1), since all the a_i's are integer and since $f \in \mathbb{Z}[X]$ implies that $f^{(j)} \in \mathbb{Z}[X]$ (for $j = 0, 1, \ldots, m$), which in turn implies that the evaluation of $f^{(j)}$ at the integers $k = 0, 1, \ldots, n$ remains an integer.

CLAIM 2: $J \neq 0$

We have by taking out the term for $k = 0$ in Equation (3.1):

$$J = -a_0 \sum_{j=0}^{m} f^{(j)}(0) - \sum_{k=1}^{n} a_k \sum_{j=0}^{m} f^{(j)}(k)$$

If $J = 0$, we would have:

$$-a_0 \sum_{j=0}^{m} f^{(j)}(0) = \sum_{k=1}^{n} a_k \sum_{j=0}^{m} f^{(j)}(k) \tag{3.2}$$

We look at the left-handside of (3.2) and use the formula for the successive derivatives of f at 0 from Lemma 3.6 (and noting that $m \geq p$) to obtain:

$$-a_0 \sum_{j=0}^{m} f^{(j)}(0) = -a_0 \cdot \left[(p-1)!(-1)^{np} (n!)^p + \sum_{j=p}^{m} f^{(j)}(0) \right]$$

We claim that this integer composed of two terms is not divisible by $p!$.
Indeed, the second term

$$-a_0 \cdot \sum_{j=p}^{m} f^{(j)}(0)$$

is an integer equal to 0 modulo $p!$, hence it is divisible by $p!$, since we have $f^{(j)}(0) \equiv 0\,(mod\,p!)$ for $j \geq p$, via Lemma 3.6.
So the divisibility of $-a_0 \sum_{j=0}^{m} f^{(j)}(0)$ by $p!$ depends on the divisibility by $p!$ of the first term

$$-a_0 \cdot (p-1)!(-1)^{np}(n!)^p$$

Since we have chosen p to be a large prime such that $p > n$, then p doesn't appear in the prime factorization of $n!$, and hence of $(n!)^p$, (because $p > n$) and of course p doesn't appear in the prime factorization of $(p-1)!$ either (because p is prime), and so the product $(p-1)!(-1)^{np}(n!)^p$ is not an integer divisible by $(p-1)! \cdot p = p!$. Furthermore, since we have chosen p prime such that $p > |a_0|$, again p doesn't appear in the prime factorization of a_0, and so the integer $-a_0 \cdot (p-1)!(-1)^{np}(n!)^p$ is not divisible by $(p-1)!p = p!$, i.e. the left handside of (3.2) is an integer not divisible by $p!$, i.e.

$$-a_0 \sum_{j=0}^{m} f^{(j)}(0) \not\equiv 0\,(mod\,p!) \tag{3.3}$$

On the other hand, the right-handside of (3.2) is equal to:

$$\sum_{k=1}^{n} a_k \sum_{j=0}^{m} f^{(j)}(k) = \sum_{k=1}^{n} a_k \left(\sum_{j=0}^{p-1} f^{(j)}(k) + \sum_{j=p}^{m} f^{(j)}(k) \right) = \sum_{k=1}^{n} a_k \left(0 + \sum_{j=p}^{m} f^{(j)}(k) \right)$$

using the successive derivatives of f at $k = 1, \ldots, n$ from Lemma 3.7 (and noting that $m \geq p$). Moreover, by the same lemma, we know that: $f^{(j)}(k)$ is an integer divisible by $p!$ for all $k = 1, \ldots, n$. So the right-handside of (3.2) is an integer divisible by $p!$, i.e.

$$\sum_{k=1}^{n} a_k \sum_{j=0}^{m} f^{(j)}(k) \equiv 0\,(mod\,p!) \tag{3.4}$$

Equations (3.3) and (3.4) lead to a contradiction, since both handsides of (3.2) should be divisible by the same integer, which implies that $J \neq 0$, as desired.

CLAIM 3: J is divisible by $(p-1)!$

As before, we take out the term for $k = 0$ in (3.1):

$$J = -a_0 \sum_{j=0}^{m} f^{(j)}(0) - \sum_{k=1}^{n} a_k \sum_{j=0}^{m} f^{(j)}(k)$$

The first summation is equal as before to:

$$-a_0 \sum_{j=0}^{m} f^{(j)}(0) = -a_0 \cdot (p-1)!(-1)^{np}(n!)^p$$

which is certainly divisible by $(p-1)!$
The second summation

$$-\sum_{k=1}^{n} a_k \sum_{j=0}^{m} f^{(j)}(k)$$

has been proven to be divisible by $p!$ (see Equation (3.4)), and hence by $(p-1)!$. Hence J is the sum of two summations, each divisible by $(p-1)!$, implying the desired claim.

Because of Claims 1,2,3, the integer J is a non-zero integer divisible by $(p-1)!$, so necessarily, we have:

$$|J| \geq (p-1)! \tag{3.5}$$

We will arrive at a contradiction by finding an upper bound for $|J|$.

By using Lemma 3.5, we have for $k = 0, 1, \ldots, n$:

$$|I(k;f)| \leq |k|e^{|k|} sup_{\xi \in \mathbb{C}, |\xi| \leq |k|} \ |f(\xi)|$$

So we have that:

$$|J| \leq \sum_{k=0}^{n} |a_k||I(k;f)| \leq \sum_{k=0}^{n} |a_k||k|e^{|k|} sup_{\xi \in \mathbb{C}, |\xi| \leq |k|} \ |f(\xi)| \tag{3.6}$$

Let $A := max(|a_0|, \ldots, |a_n|) > 0$ (because $a_n \neq 0$ and even $a_0 \neq 0$).
So, for $k = 0, 1, \ldots, n$, we certainly have:

$$|a_k| \leq A \text{ and } e^{|k|} = e^k \leq e^n \text{ and } |k| = k \leq n \tag{3.7}$$

Moreover, we have:

$$sup_{\xi \in \mathbb{C}, |\xi| \leq |k|} \ |f(\xi)| \leq sup_{\xi \in \mathbb{C}, |\xi| \leq n} |f(\xi)|$$

By definition of f, we also have:

$$|f(\xi)| = |\xi|^{p-1} \cdot |\xi - 1|^p \ldots |\xi - n|^p$$

So, for $i = 0, \ldots, n$ and for $|\xi| \leq n$, we have:

$$|\xi - i| \leq |\xi| + i \leq n + i \leq 2n,$$

which implies for $|\xi| \leq n$ that

$$|f(\xi)| \leq (2n)^{p-1+np} = (2n)^m,$$

which in turn implies

$$sup_{\xi\in\mathbb{C},|\xi|\leq n}|f(\xi)| \leq (2n)^{p-1+np} = (2n)^m$$

However, we have the trivial estimate:

$$m = p-1+np \leq p+np \leq np+np = 2np$$

So we have:

$$sup_{\xi\in\mathbb{C},|\xi|\leq n}|f(\xi)| \leq (2n)^{2np} = ((2n)^{2n})^p \tag{3.8}$$

Hence, we have, using (3.6), (3.7) and (3.8):

$$|J| \leq A\cdot n\cdot e^n\cdot((2n)^{2n})^p\cdot\sum_{k=0}^{n}1 = A\cdot e^n\cdot n\cdot((2n)^{2n})^p\cdot(n+1)$$

By taking $c_1 := A\cdot e^n\cdot n\cdot(2n)^{2n}\cdot(n+1) > 0$ and $c_2 := (2n)^{2n} > 0$, which are two positive constants independent of p, we have:

$$|J| \leq c_1\cdot c_2^{p-1} \tag{3.9}$$

But we know that the exponential of c_2

$$e^{c_2} = 1+\frac{c_2}{1!}+\frac{c_2^2}{2!}+\ldots+\frac{c_2^i}{i!}+\ldots$$

is a convergent series. Hence, for its general term, we have:

$$\frac{c_2^i}{i!}\to 0 \text{ as } i\to\infty$$

In particular, since $c_1 > 0$, if p is large enough, then $(p-1)$ is large enough to have:

$$\frac{c_2^{p-1}}{(p-1)!} < \frac{1}{c_1}$$

So we get

$$c_1\cdot\frac{c_2^{p-1}}{(p-1)!} < 1 \tag{3.10}$$

Hence, for p prime large enough such that $p > n$ and $p > |a_0|$ and such that $c_1\cdot\frac{c_2^{p-1}}{(p-1)!} < 1$ (this is possible since there are infinitely many primes), we get, using (3.5) and (3.9):

$$(p-1)! \leq |J| \leq c_1\cdot c_2^{p-1} \Longrightarrow (p-1)! \leq c_1\cdot c_2^{p-1} \Longrightarrow c_1\cdot\frac{c_2^{p-1}}{(p-1)!} \geq 1$$

which is a contradiction to (3.10). Hence, e is not an algebraic number, hence e is a transcendental number.