Bachelor Thesis

DEGREE IN MATHEMATICS

Faculty of Mathematics
University of Barcelona

TRANSCENDENTAL NUMBERS

Author: Adina Nedelea

Director: Dr. Ricardo García López

Department: Algebra and Geometry

Barcelona, June 27, 2016

Summary

Transcendental numbers are a relatively recent finding in mathematics and they provide, togheter with the algebraic numbers, a classification of complex numbers.

In the present work the aim is to characterize these numbers in order to see the way from they differ the algebraic ones. Going back to ancient times we will observe how, since the earliest history mathematicians worked with transcendental numbers even if they were not aware of it at that time.

Finally we will describe some of the consequences and new horizons of mathematics since the apparition of the transcendental numbers.

Agradecimientos

El trabajo final de grado es un punto final de una etapa y me gustará agradecer a todas las personas que me han dado apoyo durante estos años de estudios y hicieron posible que llegue hasta aquí.

Empezaré por agradecer a quien hizo posible este trabajo, a mi tutor Ricardo García ya que sin su paciencia, acompañamiento y ayuda me hubiera sido mucho mas difícil llevar a cabo esta tarea.

Sigo con los agradecimientos hacia mi familia, sobretodo hacia mi madre quien me ofreció la libertad y el sustento aunque no le fuera fácil y a mi "familia adoptiva" Carles, Marilena y Ernest, quienes me ayudaron a sostener y pasar por todo el proceso de maduración que conlleva la carrera y no rendirme en los momentos difíciles. Gracias por la paciencia y el amor de todos ellos.

Gracias también a todos los compañeros de estudios durante estos años, principalmente a Ferran quien fue un eje de apoyo, consejo y compañía en momentos delicados hasta el día de hoy.

No por último, agradecer a las matemáticas porque aunque no es un camino fácil estudiarlas, me ayudaron a madurar mi manera de relacionarme y de entender el mundo.

Contents

1 Introduction to numbers

1.1 History background

If we go back in time, for example until the sixth century before Christ, during ancient Greece, mathematicians believed that all numbers were rational and Pythagoreans based their system on such a belief. It came as a surprise when they proved that $\sqrt{2}$ could not be written as a fraction and this is why such numbers were called irrational.
Over the years, mathematicians went deeper in the characterization of such numbers and step by step the theory got more detailed in the XIX century until they arrived to the notion of transcendental numbers.

In general, talking about history, trying to expose the facts, can be a difficult task since there is a danger in mixing up history as it actually happened with how we reformulate ideas now. True is that transcendence results are ofetn based on algebra theory, more precisely on Galois theory. We will see that the main difference between an algebraic and a transcendental number lies in the fact of being or not a sero of a polynomial equation. Thus, getting deeper in the classification of numbers is about getting deeper in the solubility of polynomial equations.

Évariste Galois (1811-1832)

> We mencioned Évariste Galois(1811-1832), this is because the main work and motivation of Galois was to found results and answers to solubility of polynomial equations. It may not be clear where his work started but his extraordinary mathematical intuition attracted since the second half of nineteenth century, great publicity far beyond the mathematical world. We can say that his ideas changed the theory of equations from its classical form into what now is known as Galois Theory, together with its associated 'abstract algebra', including the theory of groups and fields. We will not enter deeper in this theory, but we remark that there is an english translation of his work made by Neumann. Next we have the end of his testamentary letter.
>
> [...]*You will have this letter printed in the Revue Encyclopédique. Often in my life I have risked advancing propositions of which I was not certain. But all that I have written here has been in my head for almost a year and it is not in my interest to make a mistake so that one could suspect me of having announced theorems of which I did not have the complete proof. You will publicly ask Jacobi or Gauss to give their opinion not on the truth but on the importance of the theorems. After that there will, I hope, be people who will find profit in deciphering all this mess.*
>
> *I embrace you warmly.*
>
> *E Galois* *29 May 1832.*

For more details of the manuscripts and papers of Galois, see the book of Neumann [1]

Three of the oldest problems in mathematics

The theory of algebraic and transcendental numbers has enabled mathematicians to settle three well-known geometric problems that have come down from antiquity. These problems come from classical Greek geometry. According to Plato the only "perfect" geometric figures are the straight line and the circle. This belief had the effect of restricting the instruments available for performing geometric constructions to two: the ruler and the compass. With these instruments alone Euclid systematically set out in his *Elements* a wide range of constructions. [6, p.100]

So, in the straightedge and compass constructions problems, the ruler is used merely as a straight edge, an instrument for drawing a straight line but not for measuring or making off distances. [3, p.3]. In this way, during this period, many problems of construction raised, but these were gradually solved as there was formed a solid base of the euclidean geometry. But there were some of them that do not have solution, fact that was proved just when algebra had been more developed, in the nineteenth century.
We will mention three of them: squaring of the circle, the doubling of the cube and the trisection of an angle.

Doubling the cube

Reference to this problem occurs in many documents and there are different theories about how did it appear, one of them is about making bigger (doubling the volume) of a royal tomb.

There is another theory and this problem received the name of "Delian problem," according to an account given by the mathematician and historian Eutocius (sixth century A.D.), goes back to an old legend according to which the Delphic oracle in one of its utterances demanded the Delian altar block to be doubled. [7, p.170]

Regardless of how it started, mathematically, the problem consists of the construction of a cube whose volume is twice that of the unit cube. If the side of the given cube has length 1 unit, then the volume of the given cube is $1^3 = 1$. So if the volume of the larger cube should be 2, then its sides should have length $\sqrt[3]{2}$.
Hence the problem is reduced to that of constructing, from a segment of lenght 1, a segment of length $\sqrt[3]{2}$.

Many mathematicians from the antiquity dealt with this problem, opening up new frontiers in different mathematics areas. The problem continued being open and already in more modern times, mathematicians as René Descartes (1596-1650) or Isaac Newton (1643-1727) tried to find a solution in the euclidean geometry. It was not until 1837 when Pierre-Laurent Wantzel (1814-1848) made public the proof of the impossibility of the construction of the number $\sqrt[3]{2}$ with straightedge and compass.

The key of why is this problem impossible to be solved lies in the fact that with the methods of Galois theory one can prove that $\sqrt[3]{2}$ cannot be expressed in terms of rational numbers and nested square roots so it is not constructible. We will talk about constructible numbers later.

Pierre Laurent Wantzel (1814-1848)

We will expose the biography about this mathematician since it seems that he had a bright intelligence even if he did not achieved more inovative results.
He was born in Paris on 5th of june but during his childhood his father was serving in the army. After his return he became a mathematics professor.
Wantzel showed at a very young age great aptitude in mathematics as in other areas, Jean Claude Saint-Venant(1797 - 1886) said that:

[...] He soon surpassed even his master, who sent for the young Wantzel, at age nine, when he encountered a difficult surveying problem.

At the age of 12 he entenered to École des Arts et Métiers de Châlons and after two years he moved to the Collège Charlemagne. At the age of 15 he edited a second edition of Reynaud's Treatise on arithmetic giving a proof of a method for finding square roots which was widely used but previously unproved. At the age of 17 he received first prizes of French dissertation and Latin dissertation from the Collège Charlemagne.
One year later he was placed first in the entrance examination to the École Polytechnique and also first for the science section of the École Normale. Gaston Pinet said about him that

[...] he threw himself into mathematics, philosophy, history, music, and into controversy, exhibiting everywhere equal superiority of mind.

He seemed to said that he prefered the teaching of mathematics and so he became a lecturer in analysis at the École Polytechnique in 1838 and in 1840 he was made an engineer.
According to Saint-Venant his death was the result of overwork:

[...]one could reproach him for having been too rebellious against those counselling prudence. He usually worked during the evening, not going to bed until late in the night, then reading, and got but a few hours of agitated sleep, alternatively abusing coffee and opium, taking his meals, until his marriage, at odd and irregular hours.

Wantzel published over 20 works, three of these works are written jointly with Saint-Venant and concern the flow of air when there is a large pressure difference. De Lapparent sums up his other work as follows:

> *[...]We owe to him a note on the curvature of elastic rods, several works on the flow of air ... finally, in 1848, an important posthumous note on the rectilinear diameters of curves. It was he who first gave the integration of differential equations of the elastic curve.*

In pure mathematics Wantzel is famed for his work on solving equations by radicals. Gauss had stated that the problems of duplicating a cube and trisecting an angle could not be solved with ruler and compass but he gave no proofs. In 1837 Wantzel published in a paper in Liouville's Journal the first proofs of these results.
In 1845 Wantzel gave a new proof of the impossibility of solving all algebraic equations by radicals and writes in the introduction:

> *[...]Although Abel's proof is finally correct, it is presented in a form too complicated and so vague that it is not generally accepted. Many years previous, Ruffini, an Italian mathematician, had treated the same question in a manner much vaguer still and with insufficient developments, although he had returned to this subject many times. In meditating on the researches of these two mathematicians, and with the aid of principles we established in an earlier paper, we have arrived at a form of proof which appears so strict as to remove all doubt on this important part of the theory of equations.*

Saint-Venant, ponders the question of why Wantzel with one of the most impressive early achievements of any mathematician, should have failed to achieve even more innovative results despite his early death. He says:

> *[...]I believe that this is mostly due to the irregular manner in which he worked, to the excessive number of occupations in which he was engaged, to the continual movement and feverishness of his thoughts, and even to the abuse of his own facilities. Wantzel improvised more than he elaborated, he probably did not give himself the leisure nor the calm necessary to linger long on the same subject.*

To see more details and references to his work and life, see the Mac Tutor History of Mathematics archive [8]

Trisecting an arbitrary angle

The Greeks were concerned with the problem of constructing regular polygons, and it is likely that the trisection problem arose in this context because the construction of the regular polygon with nine sides necessitates the trisection of an angle.[3, p.1]

This problem consists in giving a construction which divides a given angle in three equal parts for every given angle. We remark this because there are some angles that can be trisected inside Platonic constraints.

So if we could trisect every angle then, we could trisect an angle of $60°$. This angle represents the countraexample that will lead us tho the impossibility of this problem.

Trisect the angle $60°$ is to construct an angle of $20°$. If this were possible then we could also construct a line segment of length $\cos 20°$.

Many mathematicians from the antiquity dealt with this problem. Some examples would be Archimedes (c.287 b.C. – c.212 b.C.) or Pappus (c.300 b.C.).[7].
As it happens with the doubling the cube problem, it was not until 1837 when Pierre-Laurent Wantzel (1814-1848) made public the proof of the impossibility of the construction of the number $\cos 20°$, with straightedge and compass. [3, p.104]

Squaring the circle

This problem, also known as *the quadrature of the circle* represents the most famous of the three problems we are treating in this work. Its insolubility is also the most difficult to prove, because it relies on the transcendence of π.

The history of the problem is linked to that of calculating the area of a circle. Information about this is found in the Rhind Papyrus from c.1650 b.C., one of the most ancients mathematical manuscripts. There is stated that the area of a circle is: $A = (\frac{8}{9})^2 d^2$ where d represents de diameter. This lead us to have an approximation of $\pi = 4(\frac{8}{9})^2 = \frac{256}{81} = 3.1604\ldots$. The Papyrus contains no explanation of how this formula was obtained.[3, p.2]

Fifteen hundred years later Archimedes improved the aproximation to $3\frac{10}{71} < \pi < 3\frac{10}{70}$, that is, $3.1408... < \pi < 3.1428...$
A curiosity is that in the time of Greeks a special word was used to people who tried to square the cercle, that was $\tau\epsilon\tau\rho\alpha\gamma\omega\nu\iota\zeta\epsilon\iota\nu$(tetragonidzein) which means *to occupy oneself with the quadrature*.[3, p.2]

We know that a circle of radius 1 has area equal to π so a square with the same area would have sides of length $\sqrt{\pi}$. Thus if squaring the circle could be done with straightedge and compass, it would follow that $\sqrt{\pi}$ is constructible.
This would mean, as we will see in section 5, that $\sqrt{\pi}$ is algebraic over $\mathbb{Q}$. But this would lead to π being itself algebraic over $\mathbb{Q}$.

So in order to prove the insolubility of squaring the circle, it suffice to show that π is not algebraic over $\mathbb{Q}$, that is, that π is a transcendental number.

We start and base our work in how transcendental numbers appeared. For this purpose, the first thing we do is to classify numbers into rational and irrational since the first transcendental numbers known were constructed aproximating irrational numbers by rational ones.

1.2 Rational and Irrational numbers: $\mathbb{Q}$ and $\mathbb{R} - \mathbb{Q}$

Definition 1.2.1. *A rational number is a number that can be put in the form $\frac{a}{d}$ where a and d are integers and d is not zero.*

Exploring a bit more the rationals, we can speak about the decimal representation of a number. In this way, rationals can be classified into ones that have terminating or finite decimals (for example $\frac{1}{80} = 0.0125$) and in the ones that have infinite decimal representation (for example $\frac{5}{11} = 0.454545\ldots$). We have several results and descriptions:

- Any rational fraction $\frac{a}{b}$ is expressible as a terminating decimal or an infinite periodic decimal ; conversely, any decimal expansion which is either terminating or infinite periodic is equal to some rational number.
- A rational fraction $\frac{a}{b}$ in lowest terms has a terminating decimal expansion if and only if the integer b has no prime factors other than 2 and 5.

About these descriptions see chapter 2.2 of [**?**, p.23]

The word 'irrational', makes reference to the impossibility of expressing a number in ratio format: $\frac{a}{b}$. Irrational numbers don't own any of the properties of the rational numbers: they do not constitute a closed set under any of the operations of addition, substraction, multiplication or division.

However, other properties are fulfilled: if $\alpha \in \mathbb{R} - \mathbb{Q}$ and $r \in \mathbb{Q} \neq 0$, then

$$\alpha + r,\ \alpha - r,\ r - \alpha,\ r\alpha,\ \frac{\alpha}{r},\ \frac{r}{\alpha},\ -\alpha,\ \alpha^{-1} \in \mathbb{R} - \mathbb{Q}$$

We will see now that numbers such as $\sqrt{7}$, $\sqrt[3]{5}$ or $\sqrt[5]{91}$ are irrational. Establish the irrationality of such numbers is based on shifting the emphasis from the numbers themselves to simple algebraic equations having the numbers as roots. So the method we are about to describe for deciding whether or not a given number is irrational can be applied if and only if we can write down a polynomial equation which has the considered number as a root.

Definition 1.2.2. *A polynomial equation with integer coefficients is an equality of the form:*

$$c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0 = 0$$

where $c_n \neq 0$ and $c_i \in \mathbb{Z}$.

Proposition 1.2.1. *A number of the form $\sqrt[n]{a}$, where a and n are positive integers, it is either irrational or an integer.*

Proof. Recall that if a polynomial equation with integer coefficients has a rational root $\frac{a}{b}$ then a is a divisor of c_0 and b is a divisor of c_n.

Then, the proof follows from that $\sqrt[n]{a}$ is a root of the equation $x^n - a = 0$. Since here the leading coefficient is 1, if this equation would have a rational root $\frac{c}{d}$ then d would be a divisor of the leading coefficient, in this case 1, so this rational root would be in fact an integer. $\square$

This argument it can be used for any given number α which is a root of a polynomial equation in order to decide if it is or not irrational.

1.3 Algebraic and transcendental numbers

At this point we open a new classification of the real numbers, formalized on the second half of the nineteenth century by Joseph Liouville who demonstrated in 1844 the existence of the transcendental numbers.

However a closely related study of irrational numbers had constituted a major focus of attention for at least a century preceding. Indeed, by 1744, Euler had already established the irrationality of the constant e and by 1761, Lambert had confirmed the irrationality of π. [11].

We get now to the classification of real numbers in algebraic and transcendentals.

Definition 1.3.1. *A complex number $\alpha \in \mathbb{C}$ is algebraic if it is a root of a polynomial equation with integer coefficients.*

Definition 1.3.2. *A transcendental number is a number that is not algebraic.*

Remarks:

i) All rational numbers $\frac{a}{b}$ are algebraic since they satisfy the polynomial equation: $bx - a = 0$, so all transcendental numbers are irrational.

ii) An algebraic number can be irrational too, $\sqrt{2}$ is an example: it is irrational but satisfies: $x^2 - 2 = 0$.

We speak about them, but we have not proved the existence of transcendental numbers. About the existence of such numbers, there appeared two proofs, one of them, the one of Cantor from year 1874 is based on concepts of set cardinality: he observed that the set of all algebraic numbers, denoted by $\overline{\mathbb{Q}}$, has the same cardinality as the set of natural numbers $\mathbb{N}$, in contrast to the set of real numbers $\mathbb{R}$ which is uncountable. From this fact, we can conclude that there are 'a lot more' transcendent numbers than algebraic ones.

Cantor's proof is far from proving the existence through an example of a transcendental number, let alone to say if a given number is transcendental or not. We will see that to prove the transcendence of a concrete number is a difficult problem.

The one who achieved the existence of transcendental numbers with examples was Liouville in 1844. He constructed a number which is transcendental, using aproximations of irrationals numbers by rationals. He proved the transcendence of some concrete given numbers.

2 Aproximation of irrational numbers by rational numbers

Liouville was who observed that the earliest results of continous fractions revelead basic features concerning the approximation of irrational numbers by rationals. He revealed that there exists a limit to the accuracy with which any algebraic number, not itself rational, can be approximated by rationals.

In order to analyse Liouville's example, we will work deeper with the irrational numbers by analyzing differents ways of aproximating them by rational numbers. We start with aproximations by integers:

Theorem 2.0.1. *Given any irrational number $\alpha \in \mathbb{R}$, there is a unique integer $m \in \mathbb{Z}$ such that:*

$$-\frac{1}{2} < \alpha - m < \frac{1}{2}$$

The proof for this theorem can be found at [5, p.85].

Now we pass to aproximations by rationals, here we can think in decimals, so let us see an example of one way of approximation that we can use for any given number. For example if we take $\sqrt{2}$ we know that $\sqrt{2} = 1.41421...$ Then we can get closer to $\sqrt{2}$ moving within the infinite sequence:

$$\frac{1}{1}, \frac{14}{10}, \frac{141}{100}, \frac{1414}{1000}, \frac{14142}{10000}, \frac{141421}{100000}, \dots$$

However, these rational numbers have the special feature that their denominators are powers of 10. In order to get away from this dependence on the denominators, first we will see that every irrational number can be approximated by a rational number having any given denominator.

Theorem 2.0.2. *Let α be any irrational number and n be any positive integer. Then there is a rational number with denominator n, $\frac{m}{n}$, such that:*

$$-\frac{1}{2n} < \alpha - \frac{m}{n} < \frac{1}{2n}$$

Proof. In general, beginning with any irrational α and any positive integer n, we note that $n\alpha$ is irrational.

Then we define m as the nearest integer to $n\alpha$, and applying Theorem 2.0.1 for $n\alpha$ we get:

$$-\frac{1}{2} < n\alpha - m < \frac{1}{2}$$

Next we divide by the positive integer n and obtain:

$$-\frac{1}{2n} < \alpha - \frac{m}{n} < \frac{1}{2n}$$

□

So, any irrational number can be approximated by a rational number $\frac{m}{n}$ with an error less than $\frac{1}{2n}$, but can this be done with less error? In the next theorem we show that the approximation by $\frac{m}{n}$ can be made within $\frac{1}{kn}$ for any specified k and certain values of n.

Theorem 2.0.3. *Given any irrational number α and any positive integer k, there is a rational number $\frac{m}{n}$ whose denominator n does not exceed k, such that:*

$$-\frac{1}{nk} < \alpha - \frac{m}{n} < \frac{1}{nk}$$

Proof. Given an irrational number α and a positive integer k, we take the k numbers: $\alpha, 2\alpha, 3\alpha, 4\alpha, ...k\alpha$, and write each of these numbers as an integer plus a fractional part:

$$j\alpha = a_j + \beta_j \tag{2.1}$$

where $a_j \in \mathbb{Z}$ and $\beta_j \in (0,1)$ are irrational.
Next we divide the unit interval into k parts, $I_1, I_2, \ldots I_k$ each of length $\frac{1}{k}$ with

$$I_j = \left(\frac{j-1}{k}, \frac{j}{k}\right)$$

Because of the irrationality of β_j $\forall j \in \{1, 2, \ldots, k\}$, none of them are equal to any of the interval limits $\frac{j}{k}$ which are rational numbers. Thus each β lies in exactly one of the intervals $I_1, I_2, \ldots, I_k$. Here we have two possibilities:

Case 1) The first interval, I_1 contains one or more $\beta's$.

$$\left.\begin{array}{l}\text{Consider } \beta_n \in I_1 \text{ where } n \leq k \\ \text{But } \beta_n = n\alpha - a_n\end{array}\right| \Rightarrow 0 < n\alpha - a_n < \tfrac{1}{k} \Rightarrow -\tfrac{1}{k} < n\alpha - a_n < \tfrac{1}{k}$$

If we divide through by n we get:

$$-\frac{1}{kn} < \alpha - \frac{a_n}{n} < \frac{1}{kn} \quad \text{and finally } m := a_n.$$

Case 2) It does not exist any $j \in \{1, 2, \ldots, k\}$ so that $\beta_j \in I_1$.
In this case there is at least one interval I_i that contains two or more $\beta's$.
Denote β_r and β_j with $j, r \in \{1, 2, \ldots, k\}, j > r$ these two values that are found in the same interval I_i. So we have that $0 < j - r < k$.

$$\left.\begin{array}{l}\beta_r, \beta_j \in I_i \Rightarrow -\frac{1}{k} < \beta_j - \beta_r < \frac{1}{k} \\ \text{but } \beta_j = j\alpha - a_j \\ \text{and } \beta_r = r\alpha - a_r\end{array}\right| \Rightarrow -\tfrac{1}{k} < (j\alpha - a_j) - (r\alpha - a_r) < \tfrac{1}{k} \Rightarrow$$

$$\Rightarrow -\tfrac{1}{k} < (j-r)\alpha - (a_j - a_r) < \tfrac{1}{k}$$

$$\text{We now define } \left.\begin{array}{l} n := j - r \\ m := a_j - a_r\end{array}\right| \Rightarrow -\tfrac{1}{k} < n\alpha - m < \tfrac{1}{k} \text{ and we divide by } n \Rightarrow$$

$$\Rightarrow -\frac{1}{kn} < \alpha - \frac{m}{n} < \frac{1}{kn} \quad \text{where } n < k.$$

In this way the proof of the theorem is complete. $\square$

Theorem 2.0.4. *Given any irrational number α, there are infinitely many rational numbers $\frac{m}{n}$ in lowest terms such that $-\frac{1}{n^2} < \alpha - \frac{m}{n} < \frac{1}{n^2}$*

Proof. Let's supose, on the contrary, that there exists only a finite quantity of rational numbers, in lowest terms,

$$\frac{m_1}{n_1}, \quad \frac{m_2}{n_2}, \quad \dots, \quad \frac{m_i}{n_i}$$

that satisfy the assertion of the theorem.
We consider now the numbers

$$\alpha - \frac{m_1}{n_1}, \quad \alpha - \frac{m_2}{n_2}, \quad \dots, \quad \alpha - \frac{m_i}{n_i}$$

Observe that these numbers are irrational, since α is irrational, some of them positive and some of them negative, but neither of these is zero.
Let's take $k \in \mathbb{N}$ so that:

$$\begin{cases} 0 < \frac{1}{k} < \alpha - \frac{m_j}{n_j} & \forall j \in \{0, \dots, i\} \text{ so that } \alpha - \frac{m_j}{n_j} > 0 \\ \alpha - \frac{m_j}{n_j} < -\frac{1}{k} < 0 & \forall j \in \{0, \dots, i\} \text{ so that } \alpha - \frac{m_j}{n_j} < 0. \end{cases}$$

With this value of k, neither of the next inequalities is true:

$$-\tfrac{1}{k} < \alpha - \tfrac{m_1}{n_1} < \tfrac{1}{k}$$

$$-\tfrac{1}{k} < \alpha - \tfrac{m_2}{n_2} < \tfrac{1}{k}$$

$$\vdots$$

$$-\tfrac{1}{k} < \alpha - \tfrac{m_i}{n_i} < \tfrac{1}{k}$$

To continue, we apply with this value of k, the *Theorem* 2.0.3, so there results that:

$$\exists\, \frac{m}{n} \in \mathbb{Q} \textit{ with } n < k \textit{ so that } -\frac{1}{nk} < \alpha - \frac{m}{n} < \frac{1}{nk} \quad \Rightarrow \quad -\frac{1}{k} < \alpha - \frac{m}{n} < \frac{1}{k}$$

In this point we can observe that there is a contradiction since from this last step we obtain that $\frac{m}{n} \neq \frac{m_j}{n_j}$ $\forall j \in \{1, 2, \dots, i\}$ which means that there exists another rational number $\frac{m}{n}$ which satisfy the Theorem. $\square$

In fact there is a limit Theorem which gives the best approximation of any irrational number:

Theorem 2.0.5. *Hurwitz's Theorem*
Given any irrational number α, exists infinitely many rational numbers $\frac{m}{n}$ so that:

$$-\frac{1}{\sqrt{5}n^2} < \alpha - \frac{m}{n} < \frac{1}{\sqrt{5}n^2}.$$

For constants greater than $\sqrt{5}$, there exist irrationals α for which the above approximation holds only for finitely many rationals $\frac{m}{n}$.

The proof can be found at [9, p.23].

At this point is where we can make the difference between algebraic and transcendental numbers. This far we were talking about irrational numbers in general. The main idea is that non-rational algebraic numbers can not be so well aproximated by rational numbers as it is with transcendental numbers.
At first sight it does not "make sense". For now it is clear that all rationals are algebraic, and that a part of the irrationals are also algebraic. So what we are saying is that these irrational algebraic numbers are badly approximated by algebraic rationals in comparation with the approximations of transcendental numbers which are far from being connected with the rationals.

For now we will prove the existence of transcendental numbers introducing the Liouville number α, with whom Liouville demonstrates that there are irrational numbers that are not algebraic.

2.1 First construction of transcendence: Liouville numbers

Definition 2.1.1. *A real number α is a Liouville number if for every positive integer j, there are integers m and n with $n > 1$ such that*

$$0 < |\alpha - \frac{m}{n}| < \frac{1}{n^j}.$$

We will take now the most famous Liouville number: $\alpha = 0,11000100...$ where the ones occur in the decimal places numbered $1!, 2!, 3!, 4!, 5!, 6!, 7!, ...$

Consequently α can be written like a sum of negative powers of 10:

$$\begin{aligned}\alpha &= 10^{-1!} + 10^{-2!} + 10^{-3!} + 10^{-4!} + 10^{-5!} + \dots \\ &= 10^{-1} + 10^{-2} + 10^{-6} + 10^{-24} + 10^{-120} + \dots \\ &= 0.1 + 0.01 + 0.000001 + \dots\end{aligned} \tag{2.2}$$

Theorem 2.1.1.

$$\textit{The Liouville number } \alpha = \sum_{j=1}^{\infty} \frac{1}{10^{j!}} \textit{ is a transcendental number.} \tag{2.3}$$

Proof.
First of all notice that $\sum_{j=1}^{\infty} \frac{1}{10^{j!}}$ is convergent since $|\frac{1}{10^{j!}}| < \frac{1}{10^j}$ $\forall j \in \mathbb{N}$ and $\sum_{j=1}^{\infty} \frac{1}{10^j}$ is a geometric series.

In order to demonstrate the assertion of the theorem, we will use some lemmas. We will start by making an aproximation of α by rationals and we will use a polynomial $f(x)$ of lowest degree which has α as a root. This will give us two different ways of 'mesuring' the order of magnitude for $f(\alpha) - f(\beta)$. Finally this two different ways of approaching $f(\alpha) - f(\beta)$ will give a conflict and we will deduce that α is

transcendental.
In order to start, we take:

$$\begin{aligned}\beta &= 10^{-1!} + 10^{-2!} + 10^{-3!} + \cdots + 10^{-j!} \\ &= \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}} + \cdots + \frac{1}{10^{j!}}, \quad j \in \mathbb{N}.\end{aligned}$$

β is a good aproximation of α and is a rational number since is a sum of fractions. For the moment we do not fix the value of j.

We can write β as unique fraction if we take the common denominator $10^{j!}$:

$$\beta = \frac{t}{10^{j!}} \ \textit{where}\ t \in \mathbb{N} \tag{2.4}$$

Then β is very close to α:

$$\alpha - \beta = 10^{-(j+1)!} + 10^{-(j+2)!} + \ldots \quad |\Longrightarrow \alpha - \beta < \frac{2}{10^{(j+1)!}} \tag{2.5}$$

In particular we have that for $r, s \in \mathbb{N}$:

$$\begin{aligned} 0 < \alpha^r < 1 \\ 0 < \beta^s < 1 \\ 0 < \alpha^r \beta^s < 1 \end{aligned} \tag{2.6}$$

To prove that α is transcendental we shall suppose that α is algebraic and then we shall obtain a contradiction.
Let us assume that $\alpha \in \overline{\mathbb{Q}} \Rightarrow \alpha$ satisfies an algebraic equation with integer coeficients. Selecting one of lowest degree, we have that α is a root of no equation of degree less than n and there is

$$\begin{aligned} f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_2 x^2 + c_1 x + c_0, \quad c_i \in \mathbb{Z} \\ \textit{with} \quad f(\alpha) = 0 \end{aligned} \tag{2.7}$$

Lemma 2.1.1. *The number β is not a root of $f(x)$, that is to say $f(\beta) \neq 0$.*

Proof. If β were a root of $f(x)$ then $(x - \beta)$ would be a factor of $f(x)$:

$$\left.\begin{array}{l} f(x) = (x-\beta)q(x) \ \text{ where } q(x) \in \mathbb{Q}[x] \\ q(x) \text{ have one degree less than } f(x) \\ \text{But } \alpha \text{ is a root of } f(x) \end{array}\right| \Rightarrow f(\alpha) = (\alpha - \beta)q(\alpha) = 0 \ |\!\Rightarrow q(\alpha) = 0.$$

We define now k as the product of all denominators of the rational coefficients of $q(x)$. In this way $kq(x)$ has integer coefficients and α is a root of $kq(x)$.

But this is a contradiction since α satisfies no equation of degree less than n with integer coefficients. So $f(\beta) \neq 0$. □

To go on with the proof of *Theorem* 2.1.1 we will prove now a lemma about the order of magnitude between $|f(\alpha) - f(\beta)|$ and $\alpha - \beta$:

Lemma 2.1.2. *There exists a number*

$$N := n|c_n| + (n-1)|c_{n-1}| + (n-2)|c_{n-2}| + \cdots + 2|c_2| + |c_1| \tag{2.8}$$

dependent only on the coefficients of $f(x)$ and its degree, such that:

$$|f(\alpha) - f(\beta)| < N(\alpha - \beta)$$

Proof. *In the course of the proof we will use the identity*

$$\alpha^k - \beta^k = (\alpha - \beta)(\alpha^{k-1} + \alpha^{k-2}\beta + \alpha^{k-3}\beta^2 + \cdots + \alpha^2\beta^{k-3} + \alpha\beta^{k-2} + \beta^{k-1}) \tag{2.9}$$

To start the proof we will compute:

$$\begin{aligned} f(\alpha) - f(\beta) &= c_n(\alpha^n - \beta^n) + c_{n-1}(\alpha^{n-1} - \beta^{n-1}) + \cdots + c_1(\alpha - \beta) \\ &\overset{(2.6)}{=} (\alpha - \beta)[c_n(\alpha^{n-1} + \alpha^{n-2}\beta + \cdots + \alpha\beta^{n-2} + \beta^{n-1}) + \\ &\qquad + c_{n-1}(\alpha^{n-2} + \alpha^{n-3}\beta + \cdots + \alpha\beta^{n-3} + \beta^{n-2}) + \\ &\qquad + \cdots + c_1] \end{aligned} \tag{2.10}$$

Using now *eq.*(2.6) we have that:

$$(\alpha^k - \beta^k) < (\alpha - \beta)(1 + 1 + \cdots + 1) = k(\alpha - \beta).$$

So we can now finish the proof:

$$\begin{aligned} |f(\alpha) - f(\beta)| &< |\alpha - \beta|[n|c_n| + (n-1)|c_{n-1}| + \cdots + |c_1|] \\ &= N(\alpha - \beta) \end{aligned}$$

□

In order to finish the proof of the transcendence of α, we now look at $f(\alpha) - f(\beta)$ in another way:

Lemma 2.1.3. *The number $|f(\alpha) - f(\beta)| \cdot 10^{j!n} \in \mathbb{N}$, no matter what value is assigned to the positive integer j.*

Proof. Since $f(\alpha) = 0$ we have that $|f(\alpha) - f(\beta)| \cdot 10^{nj!} = |f(\beta)| \cdot 10^{nj!}$.
We have

$$\begin{aligned} f(\beta) &= c_n\beta^n + c_{n-1}\beta^{n-1} + c_{n-2}\beta^{n-2} \cdots + c_1\beta + c_0 \\ &\overset{(2.4)}{=} \frac{c_n t^n}{10^{nj!}} + \frac{c_{n-1}t^{n-1}}{10^{(n-1)j!}} + \frac{c_{n-2}t^{n-2}}{10^{(n-2)j!}} + \cdots + \frac{c_1 t}{10^{j!}} + c_0 \end{aligned}$$

Multiplying now by $10^{nj!}$ we obtain:

$$f(\beta) \cdot 10^{nj!} = c_n t^n + c_{n-1}t^{n-1} \cdot 10^{j!} + c_{n-2}t^{n-2} \cdot 10^{2j!} + \cdots + c_1 t \cdot 10^{(n-1)j!}$$

Observe that the left-hand side is a non-zero integer, because $f(\beta) \neq 0$.
Taking absolute values, we see that $f(\beta) \cdot 10^{nj!}$ is a positive integer and so the lemma is proved.
□

At this point, we will choose now the value of j used in the definition of β. We will show that for a convenient j the number given by *Lemma* 2.1.4 lies between 0 and 1. This fact will give a contradiction to the last *Lemma* 2.1.4. Then the supposition that α is algebraic is false and so α must be transcendental.
Let's see that $0 < |f(\alpha) - f(\beta)| \cdot 10^{nj!} < 1$:

$$|f(\alpha) - f(\beta)| \cdot 10^{nj!} \overset{Lemma.2.1.3}{<} N(\alpha - \beta) \cdot 10^{nj!} \overset{(2.5)}{<} \frac{2N \cdot 10^{nj!}}{10^{(j+1)!}}$$

But $\dfrac{2N \cdot 10^{nj!}}{10^{(j+1)!}} = \dfrac{2N}{10^{(j+1)!-nj!}}$ where the denominator can be written as follows:

$$(j+1)! - nj! = (j+1)j! - nj! = j!(j+1-n)$$

Observe that this exponent can be made as large as desired for fixed n, by taking j very large. At this point we observe that:

- n and N are fixed: n is the degree of α and N is fixed by definition.
- j depends neither on n or N and we can take it so large that

  $$0 < \frac{2N \cdot 10^{nj!}}{10^{(j+1)!}} < 1 \text{ is satisfied.}$$

  But looking back, we have:
  $|f(\alpha) - f(\beta)| \cdot 10^{j!n} \in \mathbb{N}$ and at the same time,
  $|f(\alpha) - f(\beta)| \cdot 10^{j!n} \in \mathbb{N} < \frac{2N \cdot 10^{nj!}}{10^{(j+1)!}}$
  Thus we have a contradiction since we have a natural number which is smaller than 1. So α must be transcendental.

□

3 Euler's constant e and its transcendence

For now we just have seen the proof of the existence of transcendental numbers through the Liouville number, specially constructed for this purpose. Although there are more transcendental numbers than algebraic ones, it has been surprisingly difficult to exhibit any transcendental number. To enter more deeply into this kind of numbers we will start with the first example of a common number which is transcendental: the number e, the base of natural logarithms.
Historicaly it was in 1873 when there apepared Hermite's epoch-making memoir entitled *Sur la fonction exponentielle.* Hermite's work we can say that began a new era because many future work is based on generalizing his work.

First of all we will prove that e is irrational and after that we will go on demonstrating that e is transcendental.

3.1 Irrationality of e

Euler's number is an irrational number: $e \in \mathbb{R} - \mathbb{Q}$. This was first established by Euler in 1744 using infinite continued fractions. We present a different proof so for that we will choose the expression of e as the sum of the infinite series:

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

For any n, e can be rewritten as:

$$\begin{aligned} e &= \left(1 + \frac{1}{2!} + \frac{1}{3!} + \ldots + \frac{1}{n!}\right) + \frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \ldots \\ &= \left(1 + \frac{1}{2!} + \frac{1}{3!} + \ldots + \frac{1}{n!}\right) + \frac{1}{n!}\left(\frac{1}{n+1} + \frac{1}{(n+2)(n+1)} + \ldots\right) \end{aligned}$$

Now the second term in parentheses is positive and bounded by the sum of the geometric series

$$\frac{1}{n+1} + \frac{1}{(n+1)^2} + \cdots = \frac{1}{n}$$

So now we have that:

$$e \leq \left(1 + \frac{1}{2!} + \frac{1}{3!} + \ldots + \frac{1}{n!}\right) + \frac{1}{n \cdot n!}$$

Therefore, writing the sum $1 + \frac{1}{2!} + \frac{1}{3!} + \ldots + \frac{1}{n!}$ as a fraction with common denominator $n!$, say as $\frac{p_n}{n!}$, we obtain:

$$0 < e - \frac{p_n}{n!} \leq \frac{1}{n \cdot n!}$$

Finally we clear the denominator $n!$ to get:

$$0 < n!e - p_n \leq \frac{1}{n}$$

If e is rational, then $n!e$ is an integer when n is large. But that makes $n!e - p_n$ an integer located in the open interval $(0, 1/n)$, which is absurd. We have a contradiction, so e is irrational.

3.2 Transcendence of e

Hermite's original proof was simplified by Karl Weierstrass, David Hilbert, Adolf Hurwitz and Paul Gordan. We will give the simplified version where we use a generalization of the problem of simultaneous approximation of irrationals.

Theorem 3.2.1. *The e number is transcendental.*

Proof. Let us assume that e is not transcendental, so it is an algebraic number and:

$$a_m e^m + \cdots + a_1 e + a_0 = 0 \quad \text{where} \quad a_j \in \mathbb{Z}\, \forall j, \quad a_0 \neq 0. \tag{3.1}$$

We define the polynomial in x of degree $mp + p - 1$:

$$f(x) = \frac{x^{p-1}(x-1)^p(x-2)^p \cdot \ldots \cdot (x-m)^p}{(p-1)!} \text{ where } p \text{ is an arbitrary prime number.}$$

To continue, we first observe that $f^{(mp+p)}(x) = 0$ and we take:

$$F(x) = \sum_{j=0}^{\infty} f^{(j)}(x) = f(x) + f'(x) + f''(x) + \ldots + f^{(mp+p-1)}(x)$$

We calculate:

$$\frac{d}{dx}\left[e^{-x}F(x)\right] = e^{-x}\left(F'(x) - F(x)\right) = -e^{-x}f(x)$$

For any j now we integrate in both sides between 0 and j and after multiplying by a_j we obtain :

$$\begin{aligned} a_j \int_0^j e^{-x} f(x)dx &= a_j \left[-e^{-x}F(x)\right]_0^j \\ &= a_j F(0) - a_j e^{-j} F(j) \end{aligned} \tag{3.2}$$

Multiplying by e^j and summing over $j = 0, 1, \ldots, m$:

$$\begin{aligned} \sum_{j=0}^{m} \left(a_j e^j \int_0^j e^{-x} f(x)dx \right) &= F(0)\sum_{j=0}^{m} a_j e^j - \sum_{j=0}^{m} a_j F(j) \\ &\overset{(3.2)}{=} -\sum_{j=0}^{m} \sum_{i=0}^{mp+p-1} a_j f^{(i)}(j) \end{aligned} \tag{3.3}$$

We observe that:

$$\begin{aligned} f'(x) = \frac{1}{(p-1)!}[&(p-1)x^{p-2}(x-1)^p(x-2)^p \cdot \ldots \cdot (x-m)^p + \\ &+ x^{p-1}p(x-1)^{p-1}(x-2)^p \cdot \ldots \cdot (x-m)^p + \\ &+ x^{p-1}p(x-1)^p(x-2)^{p-1} \cdot \ldots \cdot (x-m)^p + \ldots] \end{aligned} \tag{3.4}$$

Next we claim that each $f^{(i)}(j)$ takes integer values at $j = \{0, 1, 2, \ldots m\}$. In order to establish the claim we will use Leibniz's rule for differentiating a product:

$$\frac{d^m}{dx^m}(uv) = \sum_{r=0}^{m} \binom{m}{r} \frac{d^r u}{dx^r} \frac{d^{m-r} v}{dx^{m-r}}$$

In this way, if $f(x)$ is differentiated fewer than p times, then the value of $f^{(i)}$ is 0 whenever $x = j$, for $j \in \{0, 1, 2, \ldots m\}$ since $f^{(i)}(x)$ have at least one factor $(x - j)$.

If $f(x)$ is differentiated p or more times, then the unique non-zero terms arise when setting $x = j \neq 0$ and come from the factor $(x-j)^p$. Since $\frac{p!}{(p-1)!} = p$, all such terms are integers divisible by p. The only exception is when $j = 0$. In this case the first nonzero term occurs when $i = p - 1$:

$$\begin{aligned} f^{(p-1)}(x) &= \frac{1}{(p-1)!}\left[(p-1)!x^0(x-1)^p(x-2)^p \cdot \ldots \cdot (x-m)^p + \ldots\right] \Rightarrow \\ \Rightarrow f^{(p-1)}(0) &= (-1)^p(-2)^p \cdot \ldots \cdot (-m)^p \end{aligned} \tag{3.5}$$

Subsequent non-zero terms are all multiple of p:

$$\begin{aligned} f^{(p)}(x) = \frac{1}{(p-1)!}[p!(x-1)^{p-1}(x-2)^p \cdot \ldots \cdot (x-m)^p + \\ + (x-1)^p p(x-2)^{p-1} \cdot \ldots \cdot (x-m)^p + \ldots] \Rightarrow \end{aligned}$$

$$\Rightarrow f^{(p)}(0) = \frac{1}{(p-1)!}\left[p!(-1)^{p-1}(-2)^p \cdot \ldots \cdot (-m)^p + (-1)^p p(-2)^{p-1} \cdot \ldots \cdot (-m)^p\right] \tag{3.6}$$

Finally, the value of the Equation (3.3) is:

$$K_p + a_0(-1)^p \ldots (-m)^p \qquad \text{for some } K \in \mathbb{Z}.$$

Depending on the value of p, the integer $a_0(-1)^p \ldots (-m)^p$ is not divisible by p. This happens when $p > max(m, |a_0|)$, so for sufficiently large primes p the value of (3.3) is an integer not divisible by p, hence not 0.

On the other hand we will now estimate the integral of (3.4). Looking the definition of $f(x)$, if $0 \leq x \leq m$, then: $|f(x)| \leq \frac{m^{mp+p-1}}{(p-1)!}$ in addition if f is a integrable function then $|f|$ is integrable too and is verified that :

$$\begin{aligned} \left|\sum_{j=0}^{m} a_j e^j \int_0^j e^{-x} f(x)dx\right| &\leq \sum_{j=0}^{m} |a_j e^j| \int_0^j \frac{m^{mp+p-1}}{(p-1)!}dx \\ &\leq \sum_{j=0}^{m} |a_j e^j| j \frac{m^{mp+p-1}}{(p-1)!} \underset{p\to\infty}{\longrightarrow} 0 \end{aligned} \tag{3.7}$$

At this point we arrive to a contradiction since we have proved that the value of (3.3) is not an integer for p big enough. So the suposition of e being an algebraic number is false, therefore, e is transcendental.

$\square$

4 Further examples: π number and its transcendence

In order to demonstrate that π is a transcendental number, a fact that was achieved by Lindemann in 1882, we will need some more algebra: results from the theory of symmetric polynomials. Then, using ideas from the proof of the transcendence of e we will give the proof for π.

4.1 Results from the theory of Symmetric Polynomials

In order to achieve the proof of the transcendence of π we will use an equation for π via symmetric polynomials. For now we will make remarks about the main properties and relationship between polynomials, symmetric polynomials and elementary symmetric ones.

Definition 4.1.1. *A polynomial $f(X_1, X_2, \dots, X_n)$ in indeterminates $X_1, X_2, \dots, X_n$ is called symmetric if, for all permutations ρ of $\{X_1, X_2, \dots, X_n\}$, we have:*

$$f^{\rho}\{X_1, X_2, \dots, X_n\} = f(X_{\rho(1)}, X_{\rho(2)}, \dots, X_{\rho(n)}) = f(X_1, X_2, \dots, X_n)$$

Lemma 4.1.1. *i) If $f(X_1, X_2, \dots, X_n)$ and $g(X_1, X_2, \dots, X_n)$ are symmetric polynomials in $X_1, X_2, \dots, X_n$ then so are*

$$\begin{gathered} f(X_1, X_2, \dots, X_n) \pm g(X_1, X_2, \dots, X_n) \\ f(X_1, X_2, \dots, X_n) \cdot g(X_1, X_2, \dots, X_n) \end{gathered}$$

ii) If $h(Y_1, Y_2, \dots, Y_m)$ is any polynomial in indeterminates $Y_1, Y_2, \dots, Y_m$ and if $g_1(X_1, X_2, \dots, X_n), \dots, g_m(X_1, X_2, \dots, X_n)$ are symmetric polynomials in $X_1, X_2, \dots, X_n$ then

$$h(g_1(X_1, X_2, \dots, X_n), \dots, g_m(X_1, X_2, \dots, X_n))$$

is also symmetric in $X_1, X_2, \dots, X_n$.

Definition 4.1.2. *The n elementary symmetric functions $\sigma_1, \sigma_2, \dots, \sigma_n$ in indeterminates $X_1, X_2, \dots, X_n$ are the coefficients respectively of the powers $Y^{n-1}, Y^{n-2}, \dots, Y^0$ in the expansion of*

$$(Y + X_1)(Y + X_2) \dots (Y + X_n)$$

that is,

$$\begin{aligned} \sigma_1(X_1, X_2, \dots, X_n) &= X_1 + X_2 + \ldots + X_n, \\ \sigma_1(X_1, X_2, \dots, X_n) &= X_1X_2 + X_1X_3 + \ldots + X_1X_n + \\ &\qquad\qquad + X_2X_3 + \ldots + X_2X_n + \\ &\qquad\qquad\qquad\qquad + X_{n-1}X_n, \\ &\vdots \\ \sigma_n(X_1, X_2, \dots, X_n) &= X_1X_2 \dots X_n. \end{aligned}$$

Notice that $\sigma_k(X_1, \dots, X_n)$ has $\binom{n}{k}$ terms.

Theorem 4.1.1. *Fundamental Theorem on Symmetric Functions*

Every symmetric polynomial g, with coefficients in a field $\mathbb{F}$, in the indeterminates $X_1, X_2, \ldots, X_n$ can be written as a polynomial h with coefficients in $\mathbb{F}$ and degree smaller or equal than the degree of g, in the n elementary symmetric functions.

The proof of this theorem can be found in [10, p.214].

Corollary 4.1.1. *Let $\mathbb{F}$ be a field and let $f(X)$ be a polynomial of degree n with coefficients in $\mathbb{F}$ and with n zeros $\alpha_1, \alpha_2, \ldots, \alpha_n$ in some extension field $\mathbb{E}$ of $\mathbb{F}$. If g is any symmetric polynomial in $X_1, X_2, \ldots X_n$ with coefficients in $\mathbb{F}$ then $g(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}$.*

Proof. Write $f(X) = a_n x^n + \ldots + a_0 = (x - \alpha_1) \ldots (x - \alpha_n)$. By the Fundamental Theorem of Symmetric Functions, $g(X_1, X_2, \ldots, X_n) = h(\sigma_1, \sigma_2, \ldots, \sigma_n)$ where h is a polynomial with coefficients in $\mathbb{F}$. So

$$g(\alpha_1, \alpha_2, \ldots, \alpha_n) = h(\beta_1, \beta_2, \ldots, \beta_n)$$

where $\beta_i = \sigma_i(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for $i = 1, 2, \ldots, n$. But taking into account that $\sigma_i(\alpha_1, \alpha_2, \ldots, \alpha_n) = (-1)^i a_i / a_n$ each of the β's are in $\mathbb{F}$ and thus $g(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is in $\mathbb{F}$. $\square$

The next proposition is one of the results that we will use in the demonstration of the transcendence of π.

Proposition 4.1.1. *Let $\mathbb{F}$ be a field and let $t(X)$ be a polynomial of degree n with coefficients in $\mathbb{F}$ and with n zeros $\alpha_1, \alpha_2, \ldots, \alpha_n$ in some extension field $\mathbb{E}$ of $\mathbb{F}$. Assume that k is an integer between 1 and n, and let*

$$\gamma_1, \gamma_2, \ldots, \gamma_m$$

be all the sums of exactly k of the α's. Then there is a monic polynomial $t_k(X)$ of degree m with coefficients in $\mathbb{F}$ which has $\gamma_1, \gamma_2, \ldots, \gamma_m$ as its zeros.

Proof. We define $t_k(X) = (X - \gamma_1)(X - \gamma_2) \ldots (X - \gamma_m)$. We must prove that each of its coefficients is in $\mathbb{F}$. Now, each of the coefficients of $t_k(X)$ is a symmetric polynomial evaluated at $(\gamma_1, \gamma_2, \ldots, \gamma_m)$. It is sufficient then to prove that, if h is any symmetric polynomial in m indeterminates and with coefficients in $\mathbb{F}$ then $h(\gamma_1, \gamma_2, \ldots, \gamma_m)$ is in $\mathbb{F}$.

Let h be any symmetric polynomial in m indeterminates and with coefficients in $\mathbb{F}$. We introduce now n indeterminates $X_1, X_2, \ldots, X_n$ and let $Y_1, Y_2, \ldots, Y_m$ denote all the sums of exactly k of the X's. Then $h(Y_1, Y_2, \ldots, Y_m)$ can be expanded out to give a polynomial $g(X_1, X_2, \ldots, X_n)$ in the X's:

$$h(Y_1, Y_2, \ldots, Y_m) = g(X_1, X_2, \ldots, X_n)$$

It is easy to see that if we permute the X's we also permute the Y's since a sum of k X's remains such a sum after permutation of the X's, and every such sum comes from another such sum after permutation. Thus $g(X_1, X_2, \ldots, X_n)$ is a symmetric function in $X_1, X_2, \ldots, X_n$ and has its coefficients in $\mathbb{F}$. Finally, from the connection between the Y's and X's and between the γ's and α's, we have

$$h(\gamma_1, \gamma_2, \ldots, \gamma_m) = g(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

which is in $\mathbb{F}$ by the *Corollary* 4.1.1. $\square$

4.2 π is transcendental

We arrived to the highpoint of this work and this is representeded by the transcendence of π, the second common number found as being transcendental. In fact this is a generalization of the Hermite's method made by Lindemann who give the proof of the transcendence of maybe the most famous number i history, π.

Theorem 4.2.1. ***Number π is transcendental.***

Proof. This proof is by contradiction. We suppose the opposite: π is not transcendental, so it is algebraic. Hence π is a zero of a non-zero polynomial over $\mathbb{Q}$. Since the imaginary unit $i \in \mathbb{C}$ is an algebraic number we have that $i\pi$ is also algebraic.

Let $t(X)$ be a monic polynomial with rational coefficients such that $t(i\pi) = 0$. The *Fundamental Theorem of Algebra* tells us that $t(X)$ factors completely over $\mathbb{C}$ so that:

$$t(X) = (X - \alpha_1)(X - \alpha_2) \cdot \ldots \cdot (X - \alpha_n) \tag{4.1}$$

where $\alpha_1 = i\pi, \alpha_2, \ldots, \alpha_n$ are all complex numbers.

On the other hand, from the Euler formula for complex numbers we know that:

$$e^{x+iy} = e^x(\cos y + i \sin y) \overset{x=0, y=\pi}{\Longrightarrow} \quad e^{i\pi} + 1 = 0 \tag{4.2}$$

so we have:

$$(e^{\alpha_1} + 1)(e^{\alpha_2} + 1) \cdot \ldots \cdot (e^{\alpha_n} + 1) = 0 \tag{4.3}$$

The product in (4.3) can be written out as a sum of 2^n terms of the form e^γ where γ is a sum of one or more α's and a single term equal to 1: the product of all the 1's in (4.3). Thus (4.3) can be rewritten as

$$e^{\gamma_1} + e^{\gamma_2} + \ldots + e^{\gamma_N} + 1 = 0 \qquad \textit{where } N = 2^n - 1 \tag{4.4}$$

Now using the *Proposition* 4.1.1 we have the next results:

(i) there is a monic polynomial $t_1(X)$ with rational coefficients which has all the α's as zeros.

(ii) there is a monic polynomial $t_2(X)$ with rational coefficients which has all the sums of two α's as zeros. And so on, finishing with:

(iii) there is a monic polynomial $t_n(X)$ with rational coefficients which has all the sums of n α's as zeros.

So if

$$T(X) = t_1(X)t_2(X)\dots t_n(X)$$

then $T(X)$ is a monic polynomial with rational coefficients which has all the N γ's as it zeros. This means that

$$T(X) = (X - \gamma_1)(X - \gamma_2)\dots(X - \gamma_N) \tag{4.5}$$

It may happen that some of these sums of α's are zero. We don't have a way to know it, so we can allow for it by rewrite the *eq.*(4.4) like:

$$e^{\beta_1} + e^{\beta_2} + \dots + e^{\beta_r} + k = 0 \tag{4.6}$$

where $k \in \mathbb{Z}, k \neq 0$ and the β's are all the nonzero γ's. So the *eq.*(4.5) becomes:

$$T(X) = X^{k-1}(X - \beta_1)\dots(X - \beta_r) \tag{4.7}$$

and has rational coefficients. Then dividing by X^{k-1}

$$\frac{T(X)}{X^{k-1}} = (X - \beta_1)\dots(X - \beta_r) \tag{4.8}$$

is also a polynomial with rational coefficients. Finally we can multiply it by a suitable integer $c \neq 0$, in order to cancel out all denominators to obtain a polynomial $\theta(X)$ over $\mathbb{Z}$.

$$\theta(X) = cX^r + c_1X^{r-1} + \dots + c_r \qquad \textit{where } c_r \neq 0 \textit{ since none of the } \beta'\textit{s is 0.}$$

Define

$$f(x) = \frac{c^s x^{p-1}[\theta(x)]^p}{(p-1)!}$$

where $s = rp - 1$ and p is any prime number. Define also:

$$F(x) = f(x) + f'(x) + \dots + f^{(s+p)}(x)$$

and note that $f^{(s+p+l)}(x) = 0 \quad \forall\, l > 0$. Now we will use the same remark of Adolf Hurwitz as in the proof of the transcendence of e :

$$\begin{aligned} \frac{d}{dx}[e^{-x}F(x)] = e^{-x}\left(f'(x) + f''(x) + \dots + f^{(s+p)}(x) + f^{(s+p+1)}(x)\right) - \\ - e^{-x}\left(f(x) + f'(x) + \dots + f^{(s+p)}(x)\right) \\ = -e^{-x}f(x) \end{aligned}$$

Consequently if we integrate on both sides between 0 and x, we obtain

$$\int_0^x \frac{d}{dy}[e^{-y}F(y)] = \int_0^x -e^{-y}f(y)dy$$

In order to calculate the integral we will make a substitution: $y = \tau x$ and we will multiply in both sides by e^x, so we obtain:

$$F(x) - e^x F(0) = -x \int_0^1 e^{(1-\tau)x} f(\tau x) d\tau$$

Observe that x is now a constant. Let it range over $\beta_1, \beta_2, \dots \beta_r$ and add the resulting equations, we get

$$\sum_{j=1}^{r} F(\beta_j) + kF(0) = -\sum_{j=1}^{r} \beta_j \int_0^1 e^{(1-\tau)\beta_j} f(\tau \beta_j) d\tau \qquad (4.9)$$

since, from eq. (4.6): $-\sum_{j=1}^{r} e^{\beta_j} = k.$

We remember that we shall achieve a contradiction, at this point we will start the reasoning to get it since this result gives it and it.
We will analise both sides of *eq.*(4.9), in the same way that we did in the proof of the transcendence of e.

First of all, we remember the definition of $f(x)$:

$$\begin{aligned} f(x) &= \frac{c^s x^{p-1}[\theta(x)]^p}{(p-1)!} \\ &= \frac{c^s}{(p-1)} x^{p-1}(x-\beta_1)^p \dots (x-\beta_r)^p, \qquad c \in \mathbb{Z} \end{aligned}$$

Now we will look to the left side of *eq.*(4.9) and we claim that for all sufficiently large p this left side is a non-zero integer. To prove the claim let's observe that

$$\sum_{j=1}^{r} f^{(t)}(\beta_j) = 0 \qquad \textit{when} \quad 0 \le t < p.$$

since if we derive f less than p times, each obtained factor contains at least one term $(x - \beta_j)$, $\forall j = 1, \dots, r$, so if we make the substitution $x = \beta_j$, the result is 0, $\forall j = 1, \dots, r$.

For the cases where $t \geqslant p$ we will use the next lemma:

Lemma 4.2.1. *Let be $f(x)$ a polynomial with integer coefficients. The coefficients of the j-derivative of $f(x)$ are divisibe by $j!$.*

We can assume $f(x)$ is a monomial, then the key point of the proof of this lemma raises in the fact that:

$$\frac{k!}{(k-j)!}\, x^{k-j} \quad = \quad j! \underbrace{\binom{k}{j}}_{\in \mathbb{Z}} x^{k-j}.$$

for each summand of $f(x)$.

In our case we use the lemma with the $t-$derivate of $(p-1)!f(x)$, whose coefficients are divisible by $p!$ since $t \geqslant p$. For the study of our $f(x)$, we will let appart for now the c^s term and define:

$$f_0(x) = \frac{1}{(p-1)!} x^{p-1}(x-\beta_1)^p \ldots (x-\beta_r)^p$$

.So, each derivative of order p or higher has a factor p and degree at most s. Now, let us consider

$$\sum_{j=1}^{r} f_0^{(t)}(\beta_j) \text{ with } t \geqslant p$$

Moreover this sum is symmetric respect to the β_j's and its coefficients are divisible by p. Since $\theta(x) = cx^r + c_1x^{r-1} + \ldots + c_r$ is the polynomial which has the β's like its zeros, we can use the elementary symmetric functions to provide the relationship between the zeros of $\theta(x)$ and its coefficients: in particular, the quotients $\frac{c_i}{c}$ are the elementary symmetric functions evaluated in the β_j's.

Now if we apply the FTSF(*Fundamental Theorem on Symmetric Functions*) to

$$\sum_{j=1}^{r} f_0^{(t)}(x_j)$$

we obtain the existence of a new polynomial $q(x)$ with coefficients in $\mathbb{Z}$ of degree lower than s, such that:

$$\sum_{j=1}^{r} f_0^{(t)}(x_j) = q(s_1^r(x), \ldots, s_r^r(x))$$

where s_i^r are the elementary symmetric polynomials in r variables. Evaluating now x_j at β and multiplying by c^s we get:

$$\sum_{j=1}^{r} f^{(t)}(\beta_j) = \underbrace{c^s\, q\left(\frac{c_1}{c}, \ldots, \frac{c_{r-1}}{c}\right)}_{\in\mathbb{Z},\ \text{multiple of } p}$$

In conclusion,

$$\sum_{j=1}^{r} f^{(t)}(\beta_j) = pk_t, \qquad\qquad t = p, p+1, \ldots, p+s$$

where the k_t are integers. It follows that

$$\sum_{j=1}^{r} F(\beta_j) = p \sum_{t=p}^{n+s} k_t$$

In order to complete the proof that the left side of *eq.*(4.9) is a non-zero integer, we now look at $kF(0)$. From the definition of $f(x)$ and earliest comments it is clear that

$$\begin{aligned} f^{(t)}(0) &= 0, & &\text{for } t \leq p-2 \\ f^{(t)}(0) &= c^s c_r^p, & &\text{for } t = p-1 \\ f^{(t)}(0) &= pl_t, & &\text{for } p \leq t \leq p+s \end{aligned}$$

for suitable $l_t \in \mathbb{Z}$. Consequently the left-hand side of the *eq.*(4.9) is

$$mp + kc^s c_r^p \qquad \text{for some } m \in \mathbb{Z}.$$

Now it remains to see that this integer is not 0. From *eq.*(4.6) we have that $k \neq 0$. Same happen for c and c_r since c is the leading coefficient of $\theta(x)$ and c_r is the independent term of $\theta(x)$ which zeros are all different of 0.
So since the value of p is not fixed yet, if we take p with enough high value, the left-hand side of *eq.*(4.9) is a non-zero integer.

The last part of the proof represents the analysis of the right-hand side of *eq.*(4.9). We claim, like in the proof for e, that this right-hand term tends to 0 as p tends to $+\infty$.

In order to proove the claim, we will treat the sum by terms, so we will choose one of the β's:

$$\left| +\beta_j \int_0^1 e^{(1-\lambda)\beta_j} |f(\lambda\beta_j)| d\lambda \right| \tag{4.10}$$

Let's look to $|f(\lambda\beta_j)|$:

$$|f(\lambda\beta_j)| \leq \left| \frac{c^s}{(p-1)!} (\lambda\beta_j)^{p-1} \theta(\lambda\beta_j)^p \right| \leq \frac{|c|^s}{(p-1)!} |\beta_j|^{p-1} |\theta(\lambda\beta_j)|^p \underbrace{\leq}_{\substack{\theta(\lambda\beta_j) \leq m(j) \\ \textit{where } m(j) = \sup_{0\leq\lambda\leq 1} |\theta(\lambda\beta_j)|}} \tag{4.11}$$

$$\leq \frac{|c|^s}{(p-1)!} |\beta_j|^{p-1} |m(j)^p$$

Then, returning to the (4.10):

$$\left| +\beta_j \int_0^1 e^{(1-\lambda)\beta_j} |f(\lambda\beta_j)| d\lambda \right| \leq \frac{|\beta_j|^p |c|^s}{(p-1)!} \, m(j)^p \int_0^1 e^{(1-\lambda)\beta_j} d\lambda \underbrace{\leq}_{\substack{e^{(1-\lambda)\beta_j} \leq B \\ \textit{where } B = \sup_{0\leq\lambda\leq 1} e^{(1-\lambda)\beta_j}}} \tag{4.12}$$

$$\begin{aligned} &\leq \frac{|\beta_j|^p |c|^s}{(p-1)!} \, m(j)^p B = \\ &= \frac{1}{|\beta_j| m(j)} \, (|c|^s B) \, \frac{[|\beta_j| \;\; m(j)]^{p-1}}{(p-1)!} \end{aligned}$$

If we define $y = |\beta_j| m(j)$ then we have:

$$= \frac{1}{|\beta_j| m(j)} \left(|c|^s B\right) \frac{y^{p-1}}{(p-1)!} \tag{4.13}$$

Remark: We observe that *eq.*(4.11) and *eq.*(4.12) occur since both of the functions, the exponential and $\theta(x)$ are continous functions in a compact space: $[0, 1]$ so they have a supreme.

Turning back to (4.13) we can underestimate the first part since the last one: $\frac{y^{p-1}}{(p-1)!}$ tends to 0 as p tends to ∞ so we can now observe that for enough large p the right-hand side of *eq.*(4.9) tends to 0.
This contradicts the fact that the left-hand side of the equality is a non-zero integer and so π is transcendental.
□

5 History, continuing with the impossibilities.

On the beggining of this work, we started with the classical geometry problems, but we did not proove the impossibility of such constructions. The main point for the three problems is to describe which numbers are constructible with straightedge and compass.

First of all we will give an algebraic expression to what we can do using the straightedge and the compass with the rules laid down by the ancient greeks, who imagined the straightedge as being free of any markings, so it is not allowed to measure distances or to transfer lengths.

Given line segments of lengths α and β , we can construct line segments of length:

$$\alpha\beta, \quad \frac{\alpha}{\beta}, \quad \sqrt{\alpha}$$

For details constructions and steps look forward to Chapter 5 of [3].

5.1 Constructible numbers

We continue making a reminder about the constructible numbers :

Definition 5.1.1. *Let $\gamma \in \mathbb{R}$ be a real number. Then γ is said to be constructible if we can construct points P_i and P_j whose distance apart is $|\gamma|$ performing a finite number of operations of addition, substraction, multiplication, division or square root.*

Theorem 5.1.1. *The set CON of all constructible numbers is a subfield of $\mathbb{R}$. Furthermore*

a) all rational numbers are in CON, and *b) if α is in CON and $\alpha > 0$ then $\sqrt{\alpha} \in$ CON.*

The plain of the proof is the next one:

1. From segments of lengths $|\alpha|$ and $|\beta|$ we can construct segments of lengths $\alpha + \beta$ and $|\alpha - \beta|$ since with the compass we can transfer lengths.
2. We can also construct segments of lengths $|\alpha\beta|$ and $|\frac{\alpha}{\beta}|$
3. Since we are given a segment of length 1 we can construct segments of lengths $1 + 1 = 2,\ 2 + 1 = 3$ and so on, from which we can construct segments of length equal to any positive integer. Hencewe can construct a segment of length equal to any desired rational number $\frac{m}{n}$ since $m, n \in \mathbb{N}$.
4. Finally we know that $\sqrt{\alpha}$ is constructible. (see [3, p.87])

Corollary 5.1.1. *Successive Square Roots Give Constructibles*
A real number $\gamma \in \mathbb{R}$ is constructible if there exist positive real numbers $\gamma_1, \gamma_2, \ldots, \gamma_n$ such that:

$$\begin{aligned} \gamma_1 \in \mathbb{F}_1 \ \text{ where }\ \mathbb{F}_1 &= \mathbb{Q}, \\ \gamma_2 \in \mathbb{F}_2 \ \text{ where }\ \mathbb{F}_2 &= \mathbb{F}_1(\sqrt{\gamma_1}), \\ &\vdots \\ \gamma_n \in \mathbb{F}_n \ \text{ where }\ \mathbb{F}_n &= \mathbb{F}_{n-1}(\sqrt{\gamma_{n-1}}), \\ &\text{and, finally,} \\ \gamma \in \mathbb{F}_{n+1} \ \text{ where }\ \mathbb{F}_{n+1} &= \mathbb{F}_n(\sqrt{\gamma_n}), \end{aligned}$$

Notice that there is a tower of fields

$$\mathbb{Q} \subseteq \mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \ldots \subseteq \mathbb{F}_n \subseteq \mathbb{F}_{n+1}$$

Theorem 5.1.2. *All Constructible Come From Square Roots*
If the real number $\gamma \in \mathbb{R}$ is constructible, then there exist positive real numbers $\gamma_1, \gamma_2, \ldots, \gamma_n$ such that:

$$\begin{aligned} \gamma_1 \in \mathbb{F}_1 \ \text{ where }\ \mathbb{F}_1 &= \mathbb{Q}, \\ \gamma_2 \in \mathbb{F}_2 \ \text{ where }\ \mathbb{F}_2 &= \mathbb{F}_1(\sqrt{\gamma_1}), \\ &\vdots \\ \gamma_n \in \mathbb{F}_n \ \text{ where }\ \mathbb{F}_n &= \mathbb{F}_{n-1}(\sqrt{\gamma_{n-1}}), \\ &\text{and, finally,} \\ \gamma \in \mathbb{F}_{n+1} \ \text{ where }\ \mathbb{F}_{n+1} &= \mathbb{F}_n(\sqrt{\gamma_n}), \end{aligned}$$

The proof of this theorem is given in [3, p.110].

Now we will apply the Theorem 5.1.2 to show that many numbers are not constructible, in fact that every constructible number must be algebraic.

Theorem 5.1.3. *Degree of a Constructible Number Theorem*
If a real number $\gamma \in \mathbb{R}$ is constructible, then $\gamma \in \overline{\mathbb{Q}}$ is algebraic over $\mathbb{Q}$ and deg$(\gamma, \mathbb{Q}) = 2^s$ for some integer $s \geq 0$.

Proof. Let γ be constructible and let $\gamma_1, \gamma_2, \ldots, \gamma_n$ be as in the *All Constructible Come From Square Roots* Theorem. But $\forall i \in \{1, \ldots, n\}$, the number $\sqrt{\gamma_i}$ is a zero of the polynomial $X^2 - \gamma_i$ which is in $\mathbb{F}_i[X]$ since $\gamma_i \in \mathbb{F}_i$. Hence by the definition of the irreductible polynomial of γ_i over $\mathbb{F}_i$ we have that

$$\deg(\sqrt{\gamma_i}, \mathbb{F}_i) = 1 \text{ or } 2$$

and since $\mathbb{F}_{i+1} = \mathbb{F}_i(\sqrt{\gamma_i})$ it follows from Theorem 3.2.4 that

$$[\mathbb{F}_{i+1} : \mathbb{F}_i] = 1 \text{ or } 2 \qquad (1 \leq i \leq n).$$

Now if we reconsider the tower of fields:

$$\mathbb{Q} \subseteq \mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \ldots \subseteq \mathbb{F}_n \subseteq \mathbb{F}_{n+1}$$

we know that

$$\begin{aligned}[F_{n+1} : \mathbb{Q}] &= [F_{n+1} : \mathbb{F}_n][F_n : \mathbb{F}_{n-1}] \ldots [F_2 : \mathbb{F}_1] \\ &= 2^u, \ \text{ for some integer } u \geq 0\end{aligned}$$

So $\gamma \in \mathbb{F}_{n+1}$ is algebraic over $\mathbb{Q}$. Also, by considering the tower

$$\mathbb{Q} \subseteq \mathbb{Q}(\gamma) \subseteq \mathbb{F}_{n+1}$$

we see that $\deg(\gamma, \mathbb{Q})$ is a factor of $[\mathbb{F}_{n+1} : \mathbb{Q}]$. Hence

$$\deg(\gamma, \mathbb{Q}) = 2^s$$

for some integer $s \geq 0$. □

Now, we get back on the classical problems already discussed and we give a reasoning of the impossiblity of each one. The reasoning consists in see that if the constructions were possible, then:

- there would exist a constructible number which is not algebraic, or
- there would exists a constructible number which is algebraic but whose degree over $\mathbb{Q}$ is not a power of 2.

We recall that the most difficult problem, the one of squaring the circle, is proved in the previous chapter where it is evidentiated that π is transcendental.
So we will see now the other two problems, which do not need of the transcendence of any number and are easier to prove.

Dubling the cube

If the cube could be doubled, then the number $\sqrt[3]{2}$ would be a constructible number. But:

$X^3 - 2$ has $\sqrt[3]{2}$ as a zero and it is monic.
Now, the only possible zeros in $\mathbb{Q}$ are $\{\pm 1, \pm 2\}$, none of which is solution.
This polynomial has degree 3 so we obtain that it is irreducible over $\mathbb{Q}$ and:

$$\operatorname{irr}(\sqrt[3]{2}, \mathbb{Q}) = X^3 - 2$$

and so:

$$\deg(\sqrt[3]{2}, \mathbb{Q}) = 3$$

which is not a power of 2. This shows that $\sqrt[3]{2}$ is not a constructible number, and so the cube cannot be doubled.

Trisecting an arbitrary angle

Here we remained at the point to prove that $\cos 20°$ is a non constructible number.

To do so, we recall the trigonometric formula:

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta.$$

Proof. This formula derives from using:

$$\begin{aligned} \cos(A+B) &= \cos A \cos B - \sin A \sin B \\ \sin(A+B) &= \sin A \cos B + \cos A \sin B \end{aligned} \tag{5.1}$$

Replacing A and B by a single value θ in (5.1) we obtain:

$$\begin{aligned} \cos 2\theta &= \cos^2\theta - \sin^2\theta \\ \sin 2\theta &= 2\sin\theta\cos\theta \end{aligned} \tag{5.2}$$

Nex if we replace A by 2θ and B by θ in the first equation of (5.1), we get:

$$\cos 3\theta = \cos 2\theta \cos\theta - \sin 2\theta \sin\theta \tag{5.3}$$

Now, using (5.2) and the identity $cos^2\theta + \sin^2\theta = 1$, we obtain

$$\begin{aligned} \cos 3\theta &= (\cos^2\theta - \sin^2\theta)\cos\theta - (2\sin\theta\cos\theta)\sin\theta \\ &= \cos^3\theta - 3\sin^2\theta\cos\theta \\ &= 4cos^3\theta - 3\cos\theta \end{aligned} \tag{5.4}$$

□

If we use now $\theta = \cos 20°$, we get:

$$\begin{aligned} & \cos 60° = 4\cos^3 20° - 3\cos 20° \\ \text{if we set: } x = \cos 20° \text{ then: } \quad & \frac{1}{2} = 4x^3 - 3x \qquad (5.5) \\ \text{or what is the same: } \quad & 8x^3 - 6x - 1 = 0 \end{aligned}$$

At this point we know that $\cos 20°$ is a root . In order to go on we know that the only possible rational roots are $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$. Since none of these eight possibilities is an actual root, we obtain that $\cos 20°$ is an irrational number and that polynomial $f(x) = 8x^3 - 6x - 1$ is irreducible in $\mathbb{Q}[x]$.
Finally applying Theorem 5.1.3 we obtain that $\cos 20°$ is not a constructible number because the degree of the polynomial $f(x) = 8x^3 - 6x - 1$ is not a power of 2.

6 Conclusions and future work

All the understanding about transcendental numbers realized during this study is generated by the fresh ideas of Liouville about the approximation of irrationals by rationals and of Hermite who studied the exponential function. Then, within a decade Lindemann succeeded in generalizing Hermite's method. [11]

In fact, the two preceding cases: e and π are special cases of a much more general result which Lindemann sketched in his original memoir of 1882 and which was later proved by Karl Weierstrass. [12]

Theorem. *Lindemann Theorem*

The number e^α is transcendental for any non-zero algebraic number α.

So we can observe that an immediate consequence is the transcendence of π.

Then a good way to continue this work would be studying the Lindemann-Weierstrass Theorem:

Theorem. *Lindemann-Weierstrass Theorem*

Let $\alpha_0, \alpha_1 \dots, \alpha_n$ be $n+1a$ distinc algebraic numbers. Then

$$e^{\alpha_0}, e^{\alpha_1}, \dots, e^{\alpha_n}$$

are linearly independent over the algebraic numbers. That is, if $\beta_1, \dots, \beta_n$ are non-zero algebraic numbers, then:

$$\beta_0 e^{\alpha_0}, \beta_1 e^{\alpha_1} + \dots + \beta_n e^{\alpha_n} \neq 0.$$

This theorem represents a very important result, knowing that numbers are linearly independent over algebraic numbers leads to extremely powerful and important results about transcendental numbers.

Nowadays, the rhythm is accelerated and many new information is achieved. The next point that I would study to go on with the transcendence would be the seventh problem of the famous 23 problems proposed by David Hilbert in 1900. There he proposed that mathematicians attempt to establish the transcendence of an algebraic number to an irrational, algebraic power. Partial solutions to this problem were given by A. O. Gelfond in 1929, R. O. Kuzmin in 1930, and K. Boehle in 1933. In 1934 the complete solution was obtained independently by A. O. Gelfond and by Th. Schneider. The partial solutions were based on ideas reminiscent of the nineteenth proofs for the transcendence of e and for the transcendence of pi, both of the general solutions relied on a new idea that opened the way for the development of a theory of transcendental numbers.

References

[1] Peter M.Neumann, (2011). *The mathematical writings of Évariste Galois*, Switzerland: European Mathematical Society Publishing House.

[2] Ian Stewart; (2015), Fourth Edition. *Galois Theory*. CRC Press.

[3] Arthur Jones.; Sidney A.Morris.; Kenneth R. Pearson.; (1991). *Abstarct Algebra and Famous Impossibilities*. New-York: Springer-Verlag.

[4] Jorg Bewersdorff. (2006). *Galois Theory for Beginners. A Historical Perspective.* Rhode Island: American MAthematical Society.

[5] Ivan Niven. (1961). *Numbers: Rational and Irrational*. USA: Random House and The L. W. Singer Company.

[6] Carl B. Boyer. (1991). *History of Mathematics*. USA: John Wiley & Sons, INC..

[7] Dorrie Heinrich. (1965). *100 Great Problems of Elementary MAthematics. Their history and solution*. New York: Dover Publications, INC. .

[8] School of Mathematics and Statistics University of St Andrews, Scotland. MacTutor History of Mathematics archive. Date of consultation on: 26 june 2016. Available at:

`http://www-groups.dcs.st-and.ac.uk/history/Biographies/Wantzel.html`

[9] Komaravolu Chandrashekhar. (1968). *Introduction to Analytic Number Theory.* Berlin-Heidelberg: Springer-Verlag

[10] Paul Garrett. (2007). *Abstract Algebra*. Minneapolis.

[11] Alan Baker. (1975). *Transcendental Number Theory.* Great Britain: Cambridge University Press.

[12] Edward B. Burger,; Robert Tubbs. (2004). *Making Transcendence Transparent.* USA: Springer.