Algebraic and Transcendental Numbers

Stéphane Fischler

This text is meant as an introduction to algebraic and transcendental numbers. For a detailed account on this (together with many other related topics), one may refer to [1].

Throughout the text, we denote by $\mathbb{Q}$ (respectively $\mathbb{C}$) the set of rational (respectively complex) numbers, and by log the natural (Napieran) logarithm (whose derivative is the function $x \mapsto \frac{1}{x}$).

1   Algebraic Numbers

1.1   Definitions

To begin with, recall that a complex number α is said to be a *root* of a polynomial $P(X)$ if $P(\alpha) = 0$.

A complex number α is said to be *algebraic* if there is a nonzero polynomial $P(X)$, with integer coefficients, of which α is a root. The set of algebraic numbers is denoted by $\bar{\mathbb{Q}}$. A complex number α which is not algebraic is said to be *transcendental*.

The following numbers are obviously algebraic :

- Rational numbers $\frac{p}{q}$: take $P(X) = qX - p$.

- $\sqrt{2}$: take $P(X) = X^2 - 2$.

- $\sqrt[5]{3}$: take $P(X) = X^5 - 3$.

- $\frac{1+\sqrt{5}}{2}$: take $P(X) = X^2 - X - 1$.

Another example of algebraic number is $\sqrt{2} + \sqrt{3}$: take $P(X) = (X^2 - 5)^2 - 24$ and check, or apply the following Proposition:

Proposition 1.1 *Let α and β be algebraic numbers. Then $\alpha + \beta$, $-\alpha$, $\alpha\beta$ and $\frac{1}{\alpha}$ (if $\alpha \neq 0$) are algebraic.*

N.B. A more abstract formulation of this Proposition is the following: $\bar{\mathbb{Q}}$ is a subfield of $\mathbb{C}$.

Proposition 1.2 *Let α be an algebraic number, and $\beta \in \mathbb{C}$ be a n-th root of α (that is, $\beta^n = \alpha$), where n is a positive integer. Then β is algebraic.*

Using these Propositions, one can construct many algebraic numbers, for instance $\sqrt[3]{17} - 6\sqrt{12 - \sqrt[4]{13}}$. Let us focus, for a while, on the numbers that can be obtained in this way. If α is a root of a polynomial $P(X)$ of degree 2, say $P(X) = aX^2 + bX + c$ with integers a, b, c and $a \neq 0$, then α can be expressed by a formula involving only integers (for instance the coefficients a, b, c), the four usual operations (addition, substraction, multiplication, division) and extractions of square roots (if the discriminant $b^2 - 4ac$ of $P(X)$ is negative, the number i is needed too; but it can be considered as a square root of -1). If α is a root of a polynomial of degree 3 (respectively 4), such a formula exists, using also extractions of third (respectively forth) roots. But for a polynomial of degree at least 5, such a formula does not exist "in general": the roots of a randomly chosen polynomial of degree at least 5, with integer coefficients, can not be expressed by a formula involving only integers, the four usual operations and root extractions.

1.2 Classification of Numbers

Using the previous definitions, we can classify complex numbers according to their *arithmetical nature*:

- Rational numbers,

- Algebraic irrational numbers,

- Transcendental numbers.

Giving examples of rational numbers is easy; for algebraic irrational numbers, it is not so difficult: $\sqrt{2}$, $\frac{\sqrt[5]{7} + \sqrt{2}}{5}$, ... These numbers are obviously algebraic (thanks to the Propositions of Section 1.1), but we have to prove they are irrational. We are going to do this for $\sqrt{2}$.

PROOF that $\sqrt{2}$ is irrational: Argue by contradiction, assuming that $\sqrt{2}$ is an irreducible fraction $\frac{p}{q}$ (that is, p and q are relatively prime positive integers). Then either p or q is odd. Now, we have $2 = \frac{p^2}{q^2}$ i.e. $2q^2 = p^2$, hence p^2 is even, therefore p is even. There is an integer p' such that $p = 2p'$; we can write $2q^2 = (2p')^2$, therefore $q^2 = 2p'^2$. Accordingly q is even, in contradiction with the assumption.

We have not given yet any transcendental number; this is easily done using the following result:

Theorem 1.3 (Hermite-Lindemann) *For any nonzero algebraic number α, e^α is transcendental.*

Corollary 1.4 *The numbers e and π are transcendental, and so is any nonzero logarithm of an algebraic number (for instance $\log(2)$, $\log(3)$, ...).*

N.B. A logarithm of a complex number α is a $\lambda \in \mathbb{C}$ such that $\exp(\lambda) = \alpha$. Such a logarithm exists if, and only if, α is nonzero. In this case, if λ is a logarithm of α, the other ones are $\lambda + 2\pi i k$ with integer k. In the special case where α is a positive real number, there is exactly one logarithm of α which is real; we denote it by $\log(\alpha)$. Otherwise (if α is not a positive real number), we shall not use the notation $\log(\alpha)$.

N.B. Hermite proved that e is transcendental in 1873. Nine years later, Lindemann proved that π is transcendental. As a corollary, it is impossible to construct, using only a ruler and a compass, a circle with the same area as a given square; this answers the two thousand year old question of squaring the circle.

Theorem 1.5 (Gel'fond, Schneider, 1934) *Let α and β be algebraic numbers, with $\alpha \neq 0$ and $\beta \notin \mathbb{Q}$.*
  Let λ be a nonzero logarithm of α.
  Then $\exp(\beta\lambda)$ is transcendental.

N.B. If α is a positive real algebraic number, we can take $\lambda = \log(\alpha)$ and write $\alpha^\beta = \exp(\beta\log(\alpha))$.

Corollary 1.6 *The numbers $2^{\sqrt{2}}$ and $\frac{\log(2)}{\log 3}$ are transcendental, and so is $\exp(2\pi i\theta)$ when θ is an irrational algebraic number. For instance, e^π is transcendental.*

1.3 Recent Results and Open Problems

To begin with, nothing is known about the numbers $e + \pi$ and π^e. One conjectures they are both transcendental, but it is not even proved that one of them is irrational !

Euler's constant, defined as the limit as n tends to infinity of $1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n}-\log(n)$, is mysterious too: it is conjectured to be transcendental, but not even known to be irrational.

A bit more is known concerning the values, at integer points, of the Riemann zeta function $\zeta(s)$, defined at integers $s \geq 2$ by the following formula:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \ldots$$

Euler proved that for any positive integer k there is a rational number c_k such that $\zeta(2k) = c_k\pi^{2k}$. For instance, $\zeta(2) = \frac{\pi^2}{6}$ and $\zeta(4) = \frac{\pi^4}{90}$. The arithmetical nature of $\zeta(2k)$ follows at once from Corollary 1.4 and Proposition 1.2: the values of the Riemann ζ function at even integers points are transcendental. As far as odd integer points are concerned, the problem is far more difficult (and far more topical ...):

Theorem 1.7 (Apéry, 1978) *The number $\zeta(3)$ is irrational.*

Theorem 1.8 (Rivoal, 2000) *There are infinitely many odd integers s such that $\zeta(s)$ is irrational.*

Thanks to Theorem 1.8, we know there are infinitely many odd integers s such that $\zeta(s)$ is irrational, but we can not exhibit any such s (except $s = 3$, using Theorem 1.7) ! Only results like the following one are known:

Theorem 1.9 (Rivoal, 2000) *There is an odd integer s, between 5 and 169, such that $\zeta(s)$ is irrational.*

There is a huge difference between what is known (Theorems 1.7 to 1.9) and what is conjectured:

Conjecture 1.10 *For any odd integer $s \geq 3$, the number $\zeta(s)$ is transcendental.*

2   Algebraic Relations

First of all, recall that a polynomial in 2 variables, with integer coefficients, is a sum

$$P(X,Y) = \sum_{i=0}^{d_1} \sum_{j=0}^{d_2} a_{i,j} X^i Y^j$$

with nonnegative integer degrees d_1 and d_2, and integer coefficients $a_{i,j}$ ($0 \leq i \leq d_1$, $0 \leq j \leq d_2$). Of course, the zero polynomial is the one all of which coefficients are zero.

Two complex numbers α and β are said to be *algebraically dependent* if there is a nonzero polynomial $P(X,Y)$ in 2 variables, with integer coefficients, such that $P(\alpha,\beta) = 0$. Otherwise, α and β are said to be *algebraically independent*.

For instance, the numbers e and $e+2$ (respectively $\sqrt{\pi}$ and $\pi^2 - 2\pi + \sqrt[4]{3}$) are algebraically dependent : take $P(X,Y) = Y - X - 2$ (respectively $P(X,Y) = (Y - X^4 - 2X^2)^4 - 3$).

N.B. If $\alpha \in \bar{\mathbb{Q}}$ and $\beta \in \mathbb{C}$ then α and β are algebraically dependent (take $P(X,Y) = Q(X)$ where Q is a nonzero polynomial, with integer coefficients, a root of which is α). Accordingly, two numbers can be algebraically independent only if both are transcendental.

As pointed out in Section 1.3, it is an open problem to prove that no polynomial $P(X,Y)$ of the shape $qX + qY - p$ (with nonzero integers p and q) satisfies $P(e,\pi) = 0$. A stronger conjecture is the following:

Conjecture 2.1 *The numbers e and π are algebraically independent.*

However, the same question with π and e^π has been answered:

Theorem 2.2 (Nesterenko, 1996) *The numbers π and e^π are algebraically independent.*

Concerning logarithms of algebraic numbers, $\log(2)$ and $\log(3)$ are conjectured to be algebraically independent. A more general conjecture is the following: if λ and λ' are algebraically dependent logarithms of algebraic numbers, then λ and λ' are linearly dependent over $\mathbb{Q}$. The conclusion means there are integers a and b, not both zero, such that $a\lambda + b\lambda' = 0$. If $\alpha = \exp(\lambda)$ and $\beta = \exp(\lambda')$, this implies $\alpha^a \beta^b = 1$. For instance, if α and β are distinct prime numbers, this conclusion can not hold: the logarithms of two distinct prime numbers are conjectured to be algebraically dependent.

As far as the Riemann ζ function is concerned, the following conjecture may be stated, but it is out of reach nowadays since it is much stronger than Conjecture 1.10:

Conjecture 2.3 *Let s and s' be distinct odd integers, greater than or equal to 3. Then $\zeta(s)$ and $\zeta(s')$ are algebraically independent.*

3   Rational Approximations

3.1   General Results

In this section, we consider a real number α, assumed to be irrational. We try to find rational numbers $\frac{p}{q}$ which are close to α; the integers p and q are, in the sequel, assumed

4

to be relatively prime, and q positive (that is, we choose the fraction $\frac{p}{q}$ to be irreducible). The quality of approximation of α by $\frac{p}{q}$ is measured by a real number t, greater than or equal to 1; the larger t, the better the approximation:

DEFINITION An *approximation of α to order t* is a rational number $\frac{p}{q}$ such that

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{q^t}$$

For example, $\frac{22}{7} = 3.142857\ldots$ is an approximation of $\pi = 3.141592\ldots$ to order 3.2 since $0 \leq \frac{22}{7} - \pi \leq \frac{1}{7^{3.2}}$. An approximation of α to high order is a rational number which is very close to α and has denominator not too large. For instance, $\frac{3141}{1000} = 3.141$ is closer to π than $\frac{22}{7}$, but is an approximation of π only to order 1.07 because 1000 is much larger than 7.

DEFINITION An irrational real number α is said to be *approximable to order t* if there are infinitely many rational approximations of α to order t.

N.B. In this definition, we ask for infinitely many good rational approximations. In this way, for any positive ε there is such an approximation (and, actually, infinitely many) between $\alpha - \varepsilon$ and $\alpha + \varepsilon$.

Proposition 3.1 *Every irrational real number α is approximable to order 1.*

PROOF of Proposition 3.1: Let q be any positive integer. There is an integer p such that $\frac{p}{q} \leq \alpha < \frac{p+1}{q}$. Then $\left| \alpha - \frac{p}{q} \right| \leq \frac{p+1}{q} - \frac{p}{q} = \frac{1}{q}$, thereby proving Proposition 3.1.

Of course, if $t \geq t' \geq 1$ are real numbers and $\frac{p}{q}$ is an approximation of α to order t, then $\frac{p}{q}$ is also an approximation of α to order t'. Accordingly, every number approximable to order t is also approximable to order t'. Therefore the following theorem is stronger than Proposition 3.1 (for a proof, see [1], §11.1):

Theorem 3.2 *Every irrational real number α is approximable to order 2.*

In view of this Theorem, it is natural to wonder whether a given number α is approximable to some order $t > 2$.

3.2   Approximations of Algebraic Numbers

Let us begin with the number $\alpha = \sqrt{2}$, which is irrational (see Section 1.2):

Theorem 3.3 *The number $\sqrt{2}$ is not approximable to any order $t > 2$.*

PROOF of Theorem 3.3: Let $\frac{p}{q}$ be a rational number (written as an irreducible fraction) such that $\left| \sqrt{2} - \frac{p}{q} \right| \leq \frac{1}{q^t}$, where t is a real number greater than 2. Then we have $\sqrt{2} - 1 \leq \frac{p}{q} \leq \sqrt{2} + 1$. We shall consider the rational number $r = \frac{p^2}{q^2} - 2$; it is nonzero since $\sqrt{2}$ is irrational.

On the one hand, we have $|r| = \frac{|p^2 - 2q^2|}{q^2} \geq \frac{1}{q^2}$ because any positive integer is greater than or equal to 1. On the other hand, we have $|r| = \left| \frac{p}{q} + \sqrt{2} \right| \cdot \left| \frac{p}{q} - \sqrt{2} \right| \leq \frac{2\sqrt{2}+1}{q^t}$. By

comparison, we get $\frac{1}{q^2} \leq \frac{2\sqrt{2}+1}{q^t}$, that is $q \leq (2\sqrt{2}+1)^{\frac{1}{t-2}}$. We have proved that q can take only finitely many values; for each value of q, p can take only finitely many values under the assumption $|\sqrt{2} - \frac{p}{q}| \leq \frac{1}{q^t}$. Consequently, $\sqrt{2}$ admits only finitely many rational approximations to order t, thereby proving Theorem 3.3.

Following the same lines, we shall prove the following generalization of Theorem 3.3:

Theorem 3.4 (Liouville, 1844) *Let α be a root of a nonzero polynomial $P(X)$, of degree d, with integer coefficients. Assume α is irrational. Then α is not approximable to any order t greater than d.*

PROOF of Theorem 3.4: Choose a positive real number δ, with $\delta \leq 1$, such that the only root of $P(X)$ in the interval $[\alpha - \delta, \alpha + \delta]$ is α (this is possible since $P(X)$ has only finitely many real roots). Let M be a positive real number such that $|P'(x)| \leq M$ for all $x \in [\alpha - \delta, \alpha + \delta]$ (such a M exists because the function P' is continuous).

Let $\frac{p}{q}$ be an approximation of α to order t, with $t > d$. We shall find an upper bound for q; with this aim in view, let us distinguish between two cases.

In the first case, $\frac{p}{q}$ does not belong to the interval $[\alpha - \delta, \alpha + \delta]$. Then $\delta \leq |\alpha - \frac{p}{q}| \leq \frac{1}{q^t}$, that is $q \leq \delta^{-\frac{1}{t}}$.

In the second case $\frac{p}{q}$ is between $\alpha - \delta$ and $\alpha + \delta$. Then $\frac{p}{q}$ is not a root of $P(X)$ (since the only root in this interval is the irrational number α). Therefore, if we let $P(X) = a_d X^d + \ldots + a_1 X + a_0$, we have:

$$|P(\frac{p}{q})| = \frac{|a_d p^d + \ldots + a_1 p q^{d-1} + a_0 q^d|}{q^d} \geq \frac{1}{q^d} \tag{1}$$

since the numerator is a positive integer. On the other hand, there is a real number c, between α and $\frac{p}{q}$, such that $P(\frac{p}{q}) = P(\frac{p}{q}) - P(\alpha) = P'(c)(\frac{p}{q} - \alpha)$. Since c belongs to the interval $[\alpha - \delta, \alpha + \delta]$, we obtain $|P(\frac{p}{q})| \leq \frac{M}{q^t}$. By comparison with (1), this yields $q \leq M^{\frac{1}{t-d}}$.

In both cases, we have found an upper bound for q. Therefore q can take only finitely many values; so does p, because $\frac{|p|}{q} \leq |\alpha| + 1$. This concludes the proof of Theorem 3.4.

Theorem 3.4 has been strengthened to give the following result:

Theorem 3.5 (Roth, 1955) *Let α be an irrational algebraic number. Then α is not approximable to any order $t > 2$.*

N.B. Using Theorems 3.4 and 3.5, some numbers can be proved to be transcendental. This is how Liouville has constructed, for the first time, a transcendental number: he proved that $\alpha = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ is approximable to all orders t.

3.3 Approximations of Other Classical Numbers

If an irrational real number α is chosen "randomly", then it is not approximable to any order $t > 2$. Even without knowing exactly what this "randomly" means, it may seem natural that π (for instance) behaves like a randomly chosen number, with respect to rational approximations. This is a reason why the following statement is conjectured:

Conjecture 3.6 *The numbers π, $\log(2)$ and $\zeta(3)$ are not approximable to any order $t > 2$.*

N.B. The numbers $\zeta(s)$, for odd integers $s \geq 5$, are also conjectured not to be approximable to any order $t > 2$; but no statement can be proved in this direction before these $\zeta(s)$ are shown to be irrational.

Towards Conjecture 3.6, only partial results are known.

Theorem 3.7 (Rukhadze, 1987) *The number $\log(2)$ is not approximable to any order $t > 3.893$.*

N.B. Theorem 3.7 is (as far as I know) the best known result up to now (except for a refinement, due to Hata in 1990, in which 3.893 is replaced with 3.892). But many weaker results had been obtained before, for instance by Baker, Danilov, Alladi and Robinson, Chudnovsky, Nikishin, Rhin. Of course, the same remark applies to the following two results.

Theorem 3.8 (Hata, 1993) *The number π is not approximable to any order $t > 8.017$.*

Theorem 3.9 (Viola-Rhin, 2000) *The number $\zeta(3)$ is not approximable to any order $t > 5.514$.*

A classical number which does not appear in Conjecture 3.6 is e; indeed, the following very precise result can be proved using the continued fraction expansion of e:

Theorem 3.10 (Davis, 1978) *Let c be a positive real number, and consider the equation*

$$\mid e - \frac{p}{q} \mid \leq c \, \frac{\log(\log(q))}{q^2 \log(q)} \tag{2}$$

If $c > \frac{1}{2}$ (respectively $c < \frac{1}{2}$) then infinitely many (respectively only finitely many) rational numbers $\frac{p}{q}$ satisfy Equation (2) with $q \geq 2$.

Corollary 3.11 *The number e is not approximable to any order $t > 2$.*

References

[1] G.H. Hardy, E.M. Wright, *An introduction to the theory of numbers*, fifth edition, Oxford University Press, 1983.

Stéphane Fischler
Département de Mathématiques et Applications
École Normale Supérieure
45, rue d'Ulm
75230 Paris Cedex 05, France
fischler@clipper.ens.fr