UNIVERSITY OF NATURAL SCIENCES HO CHI MINH City
http://www.hcmuns.edu.vn/ September 12 – October 4, 2007

Introduction to Diophantine methods: irrationality and transcendence

Michel Waldschmidt,
Professeur, Université P. et M. Curie (Paris VI)
http://www.math.jussieu.fr/∼miw/coursHCMUNS2007.html

Contents

Diophantine approximation is a chapter in number theory which has witnessed outstanding progress together with a number of deep applications during the recent years. The proofs have long been considered as technically difficult. However, we understand better now the underlying ideas, hence it becomes possible to introduce the basic methods and the fundamental tools in a more clear way.

We start with irrationality proofs. Historically, the first ones concerned irrational algebraic numbers, like the square roots of non square positive integers. Next, the theory of continued fraction expansion provided a very useful tool. Among the first proofs of irrationality for numbers which are now known to be transcendental are the ones by H. Lambert and L. Euler, in the XVIIIth century, for the numbers e and π. Later, in 1815, J. Fourier gave a simple proof for the irrationality of e.

We first give this proof by Fourier and explain how J. Liouville extended it in 1840 (four years before his outstanding achievement, where he produced the first examples of transcendental numbers). Such arguments are very nice but quite limited, as we shall see. Next we explain how C. Hermite was able in 1873 to go much further by proving the transcendence of the number e. We introduce these new ideas of Hermite in several steps: first we prove the irrationality of e^r for rational $r \neq 0$ as well as the irrationality of π. Next we relate these simple proofs with Hermite's integral formula, following C.L. Siegel (1929 and 1949). Hermite's arguments led to the theory of Padé Approximants. They also enable Lindemann to settle the problem of the quadrature of the circle in 1882, by proving the transcendence of π.

One of the next important steps in transcendental number theory came with the solution by A.O. Gel'fond and Th. Schneider of the seventh of the 23 problems raised by D. Hilbert at the International Congress of Mathematicians in Paris in 1900: *for algebraic α and β with $\alpha \neq 0$, $\alpha \neq 1$ and β irrational, the number α^β is transcendental.* An example is $2^{\sqrt{2}}$, another less obvious example

is e^π. The proofs of Gel'fond and Schneider came after the study, by G. Pólya, in 1914, of integer valued entire functions, using interpolation formulae going back to Hermite. We introduce these formulae as well as some variants for meromorphic functions due to R. Lagrange (1935) and recently rehabilitated by T. Rivoal (2006) [28].

The end of the course will be devoted to a survey of the most recent irrationality and transcendence results, including results of algebraic independence. We shall also introduce the main conjectures on this topic.

We denote by $\mathbb{Z}$ the ring of rational integers, by $\mathbb{Q}$ the field of rational numbers, by $\mathbb{R}$ the field of real numbers and by $\mathbb{C}$ the field of complex numbers. Given a real number, we want to know whether it is rational or not, that means whether he belongs to $\mathbb{Q}$ or not. The set of irrational numbers $\mathbb{R} \setminus \mathbb{Q}$ has no nice algebraic properties: it is not stable by addition nor by multiplication.

Irrationality is the first step, the second one is transcendence. Given a complex number, one wants to know whether it is algebraic of not. The set of algebraic numbers, which is the set of roots of all non-zero polynomials with rational coefficients, is nothing else than the algebraic closure of $\mathbb{Q}$ into $\mathbb{C}$. We denote it by $\overline{\mathbb{Q}}$. The set of transcendental numbers is defined as $\mathbb{C} \setminus \overline{\mathbb{Q}}$. Since $\overline{\mathbb{Q}}$ is a field, the set of transcendental numbers is not stable by addition nor by multiplication.

1 Irrationality

1.1 Simple proofs of irrationality

The early history of irrationality goes back to the Greek mathematicians Hippasus of Metapontum (around 500 BC) and Theodorus of Cyrene, Eudoxus, Euclid. There are different early references in the Indian civilisation and the Sulba Sutras (around 800-500 BC).

Let us start with the irrationality of the number

$$\sqrt{2} = 1,414\,213\,562\,373\,095\,048\,801\,688\,724\,209\ \ldots$$

One of the most well known proofs is to argue by contradiction as follows: assume $\sqrt{2}$ is rational and write it as a/b where a and b are relatively prime positive rational integers. Then $a^2 = 2b^2$. It follows that a is even. Write $a = 2a'$. From $2a'^2 = b^2$ one deduces that b also is even, contradicting the assumption that a and b were relatively prime.

There are variants of this proof - a number of them are in the nice booklet [27]. For instance using the relation

$$\sqrt{2} = \frac{2 - \sqrt{2}}{\sqrt{2} - 1}$$

with $\sqrt{2} = a/b$ one deduces

$$\sqrt{2} = \frac{2b - a}{a - b}.$$

Now we have $1 < \sqrt{2} < 2$, hence $0 < a-b < b$, which shows that the denominator b of fraction $\sqrt{2} = a/b$ was not minimal.

This argument can be converted into a geometric proof: starting with an isosceles rectangle triangle with sides b and hypothenuse a, one constructs (using ruler and compass if one wishes) another similar triangle with smaller sides $a-b$ and hypothenuse $2b-a$. Such a proof of irrationality is reminiscent of the ancient Greek geometers constructions, and also of the infinite descent of Fermat.

A related but different geometric argument is to start with a rectangle having sides 1 and $1 + \sqrt{2}$. We split it into two unit squares and a smaller rectangle. The length of this second rectangle is 1, its width is $\sqrt{2}-1$, hence its proportion is

$$\frac{1}{\sqrt{2} - 1} = 1 + \sqrt{2}.$$

Therefore the first and second rectangles have the same proportion. Now if we repeat the process and split the small rectangle into two squares (of sides $\sqrt{2} - 1$) and a third tiny rectangle, the proportions of this third rectangle will again be $1 + \sqrt{2}$. This means that the process will not end, each time we shall get two squares and a remaining smaller rectangle having the same proportion.

On the other hand if we start with a rectangle having integer side lengths, if we split it into several squares and if a small rectangle remains, then clearly the small rectangle while have integer side lengths. Therefore the process will not continue forever, it will stop when there is no remaining small rectangle. This proves again the irrationality of $\sqrt{2}$.

In algebraic terms the number $x = 1 + \sqrt{2}$ satisfies

$$x = 2 + \frac{1}{x},$$

hence also

$$x = 2 + \frac{1}{2 + \frac{1}{x}} = 2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{x}}} = \cdots,$$

which yields the *continued fraction expansion* of $1 + \sqrt{2}$. Here is the definition of the continued fraction expansion of a real number.

Given a real number x, the Euclidean division in $\mathbb{R}$ of x by 1 yields a quotient $[x] \in \mathbb{Z}$ (the *integral part of* x) and a remainder $\{x\}$ in the interval $[0, 1)$ (the *fractional part of* x) satisfying

$$x = [x] + \{x\}.$$

Set $a_0 = [x]$. Hence $a_0 \in \mathbb{Z}$. If x is an integer then $x = [x] = a_0$ and $\{x\} = 0$. In this case we just write $x = a_0$ with $a_0 \in \mathbb{Z}$. Otherwise we have $\{x\} > 0$ and

we set $x_1 = 1/\{x\}$ and $a_1 = [x_1]$. Since $\{x\} < 1$ we have $x_1 > 1$ and $a_1 \geq 1$. Also

$$x = a_0 + \frac{1}{a_1 + \{x_1\}}.$$

Again, we consider two cases: if $x_1 \in \mathbb{Z}$ then $\{x_1\} = 0$, $x_1 = a_1$ and

$$x = a_0 + \frac{1}{a_1}$$

with two integers a_0 and a_1, with $a_1 \geq 2$ (recall $x_1 > 1$). Otherwise we can define $x_2 = 1/\{x_1\}$, $a_2 = [x_2]$ and go one step further:

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \{x_2\}}}.$$

Inductively one obtains a relation

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \; a_{n-1} + \cfrac{1}{a_n + \{x_n\}}}}}$$

with $0 \leq \{x_n\} < 1$. The connexion with the geometric proof of irrationality of $\sqrt{2}$ by means of rectangles and squares is now obvious: start with a positive real number x and consider a rectangle of sides 1 and x. Divide this rectangle into unit squares and a second rectangle. Then a_0 is the number of unit squares which occur, while the sides of the second rectangle are 1 and $\{x\}$. If x is not an integer, meaning $\{x\} > 0$, then we split the second rectangle into squares of sides $\{x\}$ plus a third rectangle. The number of squares is now a_1 and the third rectangle has sides $\{x\}$ and $1 - a_1\{x\}$. Going one in the same way, one checks that the number of squares we get at the n-th step is a_n.

This geometric point of view shows that the process stops after finitely many steps (meaning that some $\{x_n\}$ is zero, or equivalently that x_n is in $\mathbb{Z}$) if and only if x is rational.

For simplicity of notation we write

$$x = [a_0; a_1, \ldots, a_n] \quad \text{or} \quad x = [a_0; a_1, \ldots, a_n, \ldots]$$

depending on whether $x_n \in \mathbb{Z}$ for some n or not. This is the *continued fraction expansion of* x. Notice that any irrational number has a unique infinite continued fraction expansion, while for rational numbers, the above construction provides a unique well defined continued fraction which bears the restriction that the last a_n is ≥ 2. But we allow also the representation

$$[a_0; a_1, \ldots, a_n - 1, 1].$$

For instance $11/3 = [3; 1, 2] = [3; 1, 1, 1]$.

We need a further notation for ultimately periodic continued fraction. Assume that x is irrational and that for some integers n_0 and $r > 0$ its continued fraction expansion $[a_0; a_1, \dots, a_n, \dots]$ satisfies

$$a_{n+r} = a_n \quad \text{for any } n \geq n_0.$$

Then we write

$$x = [a_0; a_1, \dots, a_{n_0-1}, \overline{a_{n_0}, a_{n_0+1}, \dots, a_{n_0+r-1}}].$$

For instance

$$\sqrt{2} = [1; 2, 2, 2, \dots] = [1; \overline{2}].$$

References on continued fractions are [10, 29, 19, 22, 5]. An interesting remark [27] on the continued fraction expansion of $\sqrt{2}$ is to relate the A4 paper format 21×29.7 to the fraction expansion

$$\frac{297}{210} = \frac{99}{70} = [1; 2, 2, 2, 2, 2].$$

There is nothing special with the square root of 2: most of the previous argument extend to the proof of irrationality of $\sqrt{n}$ when n is a positive integer which is not the square of an integer. For instance a proof of the irrationality of $\sqrt{n}$ when n is not the square of an integer runs as follows. Write $\sqrt{n} = a/b$ where b is the smallest positive integer such that $b\sqrt{n}$ is an integer. Further, denote by m the integral part of $\sqrt{n}$: this means that m is the positive integer such that $m < \sqrt{n} < m + 1$. The strict inequality $m < \sqrt{n}$ is the assumption that n is not a square. From $0 < \sqrt{n} - m < 1$ one deduces

$$0 < (\sqrt{n} - m)b < b.$$

Now the number $b' = (\sqrt{n} - m)b$ is a positive rational integer, the product $b'\sqrt{n}$ is an integer and $b' < b$, which contradicts the choice of b minimal.

Exercise 1.1. Extend this proof to a proof of the irrationality of $\sqrt[k]{n}$, when n and k are positive integers and n is not the k-th power of an integer.
`Hint.` *Assume that the number $x = \sqrt[k]{n}$ is rational. Then the numbers*

$$x^2, x^3, \dots, x^{k-1}$$

are also rational. Denote by d the least positive integer such that the numbers $dx, dx^2, \dots, dx^{k-1}$ are integers. Further, denote by m the integral part of x and consider the number $d' = (x - m)d$.

The irrationality of $\sqrt{5}$ is equivalent to the irrationality of the *Golden ratio* $\Phi = (1 + \sqrt{5})/2$, root of the polynomial $X^2 - X - 1$, whose continued fraction expansion is

$$\Phi = [1; 1, 1, 1, 1, \dots] = [1, \overline{1}].$$

This expansion follows from the relation

$$\Phi = 1 + \frac{1}{\Phi}\cdot$$

The geometric irrationality proof using rectangles that we described above for $1+\sqrt{2}$ works in a similar way for the Golden ratio: a rectangle of sides Φ and 1 splits into a square and a small rectangle of sides 1 and $\Phi - 1$, hence the first and the second rectangles have the same proportion

$$\Phi = \frac{1}{\Phi - 1}\cdot \tag{1.2}$$

As a consequence the process continues forever with one square and one smaller rectangle with the same proportion. Hence Φ and $\sqrt{5}$ are irrational numbers.

Exercise 1.3. Perform the geometric construction starting with any rectangle of sides 1 and x: split it into a maximal number of squares of sides 1, and if a second smaller rectangle remains repeat the construction: split it into squares as much as possible and continue if a third rectangle remains.
a) Prove that the number of squares in this process is the sequence of integers $(a_n)_{n\geq_0}$ in the continued fraction expansion of x.
b) Start with a unit square. Put on top of it another unit square: you get a rectangle with sides 1 and 2. Next put on the right a square of sides 2, which produces a rectangle with sides 2 and 3. Continue the process as follows: when you reach a rectangle of small side a and large side b, complete it with a square of sides b, so that you get a rectangle with sides b and $a+b$.
Which is the sequence of sides of the rectangles you obtain with this process? Generalizing this idea, deduce a geometrical construction of the rational number having continued fraction expansion

$$[a_0; a_1, \ldots, a_k].$$

Another proof of the same result is to deduce from the equation (1.2) that a relation $\Phi = a/b$ with $0 < b < a$ yields

$$\Phi = \frac{b}{a-b},$$

hence a/b is not a rational fraction with minimal denominator.

Other numbers for which it is easy to prove the irrationality are quotients of logarithms: if m and n are positive integers such that $(\log m)/(\log n)$ is rational, say a/b, then $m^b = n^a$, which means that *m and n are multiplicatively dependent*. Recall that elements $x_1, \ldots, x_r$ in an additive group are *linearly independent* if a relation $a_1x_1 + \cdots + a_rx_r = 0$ with rational integers $a_1, \ldots, a_r$ implies $a_1 = \cdots = a_r = 0$. Similarly, elements $x_1, \ldots, x_r$ in a multiplicative group are *multiplicatively independent* if a relation $x_1^{a_1} \cdots x_r^{a_r} = 1$ with rational integers $a_1, \ldots, a_r$ implies $a_1 = \cdots = a_r = 0$. Therefore a quotient like $(\log 2)/\log 3$, and more generally $(\log m)/\log n$ where m and n are multiplicatively independent positive rational numbers, is irrational.

We have seen that *a real number is rational if and only if its continued fraction expansion is finite*. There is another criterion of irrationality using the b-adic expansion when b is an integer ≥ 2 (for $b = 10$ this is the decimal expansion, for $b = 2$ it is the diadic expansion). Indeed any real number x can be written

$$x = [x] + d_1 b^{-1} + d_2 b^{-2} + \cdots + d_n b^{-n} + \cdots$$

where the integers d_n (the digits of x) are in the range $0 \leq d_n < b$. Again there is unicity of such an expansion apart from the integer multiples of some b^{-n} which have two expansions, one where all sufficiently large digits vanish and one for which all sufficiently large digits are $b - 1$. This is due to the equation

$$b^{-n} = \sum_{k=0}^{n} (b-1) b^{-n-k-1}.$$

Here is the irrationality criterion using such expaansions: fix an integer $b \geq 2$. Then *the real number x is rational if and only if the sequence of digits $(d_n)_{n\geq 1}$ of x in basis b is ultimately periodic.*

Exercise 1.4. Let $b \geq 2$ be an integer. Show that a real number x is rational if and only if the sequence $(d_n)_{n\geq 1}$ of digits of x in the expansion in basis b

$$x = [x] + d_1 b^{-1} + d_2 b^{-2} + \cdots + d_n b^{-n} + \cdots \qquad (0 \leq d_n < b)$$

is ultimately periodic.
Deduce another proof of Lemma 1.24 in § 1.3.5.

One might be tempted to conclude that it should be easy to decide whether a given real number is rational or not. However this is not the case with many constants from analysis, because most often one does not know any expansion, either in continued fraction or in any basis $b \geq 2$. And the fact is that for many such constants the answer is not known. For instance one does not know whether the *Euler–Mascheroni constant*

$$\begin{aligned} \gamma &= \lim_{n\to\infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n \right) \\ &= 0,577\,215\,664\,901\,532\,860\,606\,512\,090\,082\ldots \end{aligned}$$

is rational or not: one expects that it is an irrational number (and even a transcendental number - see later). Other formulas for the same number are

$$\begin{aligned} \gamma &= \sum_{k=1}^{\infty} \left(\frac{1}{k} - \log\left(1 + \frac{1}{k} \right) \right) \\ &= \int_1^{\infty} \left(\frac{1}{[x]} - \frac{1}{x} \right) dx \\ &= -\int_0^1 \int_0^1 \frac{(1-x)dxdy}{(1-xy)\log(xy)}. \end{aligned}$$

Recent papers on that question have been published by J. Sondow [34], they are inspired by F. Beukers' work on Apéry's proof of the irrationality of

$$\zeta(3) = \sum_{n\geq 1} \frac{1}{n^3} = 1,202\,056\,903\,159\,594\,285\,399\,738\,161\,511\ \ldots$$

in 1978. Recall that the values of the *Riemann zeta function*

$$\zeta(s) = \sum_{n\geq 1} n^{-s}$$

was considered by Euler for real s and by Riemann for complex s, the series being convergent for the real part of s greater than 1. Euler proved that the values $\zeta(2k)$ of this function at the even positive integers ($k \in \mathbb{Z}$, $k \geq 1$) are rational multiples of π^{2k}. For instance $\zeta(2) = \pi^2/6$. It is interesting to notice that Euler's proof relates the values $\zeta(2k)$ at the positive even integers with the values of the same function at the odd negative integers, namely $\zeta(1-2k)$. For Euler this involved divergent series, while Riemann defined $\zeta(s)$ for $s \in \mathbb{C}$, $s \neq 1$, by analytic continuation.

One might be tempted to guess that $\zeta(2k+1)/\pi^{2k+1}$ is a rational number when $k \geq 1$ is a positive integer. However the folklore conjecture is that this is not the case. In fact there are good reasons to conjecture that for any $k \geq 1$ and any non-zero polynomial $P \in \mathbb{Z}[X_0, X_1, \ldots, X_k]$, the number $P(\pi, \zeta(3), \zeta(5), \ldots, \zeta(2k+1))$ is not 0. But one does not know whether

$$\zeta(5) = \sum_{n\geq 1} \frac{1}{n^5} = 1,036\,927\,755\,143\,369\,926\,331\,365\,486\,457\ldots$$

is irrational or not. And there is no proof so far that $\zeta(3)/\pi^3$ is irrational. According to T. Rivoal, among the numbers $\zeta(2n+1)$ with $n \geq 2$, infinitely many are irrational. And W. Zudilin proved that one at least of the four numbers

$$\zeta(5), \zeta(7), \zeta(9), \zeta(11)$$

is irrational. References with more information on this topic are given in the Bourbaki talk [13] by S. Fischler.

A related open question is the arithmetic nature of *Catalan's constant*

$$G = \sum_{n\geq 1} \frac{(-1)^n}{(2n+1)^2} = 0,915\,965\,594\,177\,219\,015\,0\ldots$$

Other open questions can be asked on the values of *Euler's Gamma fonction*

$$\Gamma(z) = e^{-\gamma z} z^{-1} \prod_{n=1}^{\infty} \left(1 + \frac{z}{n}\right)^{-1} e^{z/n} = \int_0^{\infty} e^{-t} t^z \cdot \frac{dt}{t}.$$

As an example we do not know how to prove that the number

$$\Gamma(1/5)\cdots = 4,590\,843\,711\,998\,803\,053\,204\,758\,275\,929\,152\,0\ldots$$

is irrational.

The only rational values of z for which the answer is known (and in fact one knows the transcendence of the Gamma value in these cases) are

$$r \in \left\{ \frac{1}{6}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{5}{6} \right\} \qquad (\text{mod } 1).$$

The number $\Gamma(1/n)$ appears when one computes *periods* of the Fermat curve $X^n + Y^n = Z^n$, and this curve is simpler (in technical terms it has genus ≤ 1) for $n = 2, 3, 4$ and 6. For $n = 5$ the genus is 2 and this is related with the fact that one is not able so far to give the answer for $\Gamma(1/5)$.

The list of similar open problems is endless. For instance, is the number

$$e + \pi = 5,859\,874\,482\,048\,838\,473\,822\,930\,854\,632\ldots$$

rational or not? The answer is not yet known. And the same is true for any number in the following list

$$\log \pi,\ 2^\pi,\ 2^e,\ \pi^e,\ e^e.$$

1.2 Variation on a proof by Fourier (1815)

That e is not quadratic follows from the fact that the continued fraction expansion of e, which was known by L. Euler in 1737 [10] (see also [7]), is not periodic:

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{\ddots}}}}}} = [2;\, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots]$$

Since this expansion is infinite we deduce that e is irrational. The fact that it is not ultimately periodic implies also that e is not a quadratic irrationality, as shown by Lagrange in 1770 – Euler knew already in 1737 that a number with an ultimately period continued fraction expansion is quadratic (see [10, 5, 29]).

Exercise 1.5. a) Let b be a positive integer. Give the continued fraction expansion of the number

$$\frac{-b + \sqrt{b^2 + 4}}{2}.$$

b) Let a and b be two positive integers. Write a degree 2 polynomial with integer coefficients having a root at the real number whose continued fraction expansion is

$$[0; \overline{a, b}].$$

c) Let a, b and c be positive integers. Write a degree 2 polynomial with integer coefficients having a root at the real number whose continued fraction expansion is

$$[0; \overline{a, b, c}].$$

The following easier and well known proof of the irrationality of e was given by J. Fourier in his course at the École Polytechnique in 1815. Later, in 1872 , C. Hermite proved that e is transcendental, while the work of F. Lindemann a dozen of years later led to a proof of the so-called Hermite–Lindemann Theorem: *for any nonzero algebraic number α the number e^α is transcendental.* However for this first section we study only weaker statements which are very easy to prove. We also show that Fourier's argument can be pushed a little bit further than what is usually done, as pointed out by J. Liouville in 1844.

1.2.1 Irrationality of e

We truncate the exponential series giving the value of e at some point N:

$$N!\, e - \sum_{n=0}^{N} \frac{N!}{n!} = \sum_{k\geq 1} \frac{N!}{(N+k)!}\cdot \tag{1.6}$$

The right hand side of (1.6) is a sum of positive numbers, hence is positive (not zero). From the lower bound (for the binomial coefficient)

$$\frac{(N+k)!}{N!k!} \geq N+1 \quad \text{for } k \geq 1,$$

one deduces

$$\sum_{k\geq 1} \frac{N!}{(N+k)!} < \frac{1}{N+1} \sum_{k\geq 1} \frac{N!}{(N+k)!} < \frac{1}{N+1} \sum_{k\geq 1} \frac{1}{k!} = \frac{e-1}{N+1}\cdot$$

Therefore the right hand side of (1.6) tends to 0 when N tends to infinity. In the left hand side, $N!$ and $\sum_{n=0}^{N} N!/n!$ are integers. It follows that $N!e$ is never an integer, hence e is an irrational number.

1.2.2 The number e is not quadratic

.

The fact that e is not a rational number implies that for each $m \geq 1$ the number $e^{1/m}$ is not rational. To prove that e^2 for instance is also irrational is not so easy (see the comment on this point in [1]).

The proof below is essentially the one given by J. Liouville in 1840 [23] which is quoted by Ch. Hermite ("ces travaux de l'illustre géomètre").

To prove that e does not satisfy a quadratic relation $ae^2 + be + c$ with a, b and c rational integers, not all zero, requires some new trick. Indeed if we just

mimic the same argument we get

$$cN! + \sum_{n=0}^{N} (2^n a + b) \frac{N!}{n!} = -\sum_{k\geq 0} \left(2^{N+1+k} a + b\right) \frac{N!}{(N+1+k)!}.$$

The left hand side is a rational integer, but the right hand side tends to infinity (and not 0) with N, so we draw no conclusion.

Instead of this approach we write the quadratic relation as $ae+b+ce^{-1} = 0$. This time it works:

$$bN! + \sum_{n=0}^{N} (a + (-1)^n c) \frac{N!}{n!} = -\sum_{k\geq 0} \left(a + (-1)^{N+1+k} c\right) \frac{N!}{(N+1+k)!}.$$

Again the left hand side is a rational integer, but now the right hand side tends to 0 when N tends to infinity, which is what we expected. However we need a little more work to conclude: we do not yet get the desired conclusion, we only deduce that both sides vanish. Now let us look more closely to the series in the right hand side. Write the two first terms A_N for $k = 0$ and B_N for $k = 1$:

$$\sum_{k\geq 0} \left(a + (-1)^{N+1+k} c\right) \frac{N!}{(N+1+k)!} = A_N + B_N + C_N$$

with

$$\begin{aligned} A_N &= \left(a - (-1)^N c\right) \frac{1}{N+1} \\ B_N &= \left(a + (-1)^N c\right) \frac{1}{(N+1)(N+2)} \\ C_N &= \sum_{k\geq 2} \left(a + (-1)^{N+1+k} c\right) \frac{N!}{(N+1+k)!} \end{aligned}$$

The above proof that the sum $A_N + B_N + C_N$ tends to zero as N tends to infinity shows more: each of the three sequences

$$A_N, \quad (N+1)B_N, \quad (N+1)(N+2)C_N$$

tends to 0 as N tends to infinity. Hence, from the fact that the sum $A_N + B_N + C_N$ vanishes for sufficiently large N, it easily follows that for sufficiently large N, each of the three terms A_N, B_N and C_N vanishes, hence $a - (-1)^N c$ and $a + (-1)^N c$ vanish, therefore $a = c = 0$, and finally $b = 0$.

Exercise 1.7. Let $(a_n)_{n\geq 0}$ be a bounded sequence of rational integers.
a) Prove that the following conditions are equivalent:
(i) The number

$$\vartheta_1 = \sum_{n\geq 0} \frac{a_n}{n!}$$

is rational.
(ii) There exists $N_0 > 0$ such that $a_n = 0$ for all $n \geq N_0$.
b) Prove that these properties are also equivalent to
(iii) The number

$$\vartheta_2 = \sum_{n \geq 0} \frac{a_n 2^n}{n!}$$

is rational.

1.2.3 Irrationality of $e^{\sqrt{2}}$ (Following a suggestion of D.M. Masser)

The trick here is to prove the stronger statement that $\vartheta = e^{\sqrt{2}} + e^{-\sqrt{2}}$ is an irrational number.

Summing the two series

$$e^{\sqrt{2}} = \sum_{n \geq 0} \frac{2^{n/2}}{n!} \quad \text{and} \quad e^{-\sqrt{2}} = \sum_{n \geq 0} (-1)^n \frac{2^{n/2}}{n!}$$

we deduce

$$\vartheta = 2 \sum_{m \geq 0} \frac{2^m}{(2m)!}.$$

Let N be a sufficiently large integer. Then

$$\frac{(2N)!}{2^N} \vartheta - 2 \sum_{m=0}^{N} \frac{(2N)!}{2^{N-m}(2m)!} = 4 \sum_{k \geq 0} \frac{2^k (2N)!}{(2N+2k+2)!}. \tag{1.8}$$

The right hand side of (1.8) is a sum of positive numbers, in particular it is not 0. Moreover the upper bound

$$\frac{(2N)!}{(2N+2k+2)!} \leq \frac{1}{(2N+2)(2k+1)!}$$

shows that the right hand side of (1.8) is bounded by

$$\frac{2}{N+1} \sum_{k \geq 0} \frac{2^k}{(2k+1)!} < \frac{\sqrt{2} e^{\sqrt{2}}}{N+1},$$

hence tends to 0 as N tends to infinity.

It remains to check that the coefficients $(2N)!/2^N$ and $(2N)!/2^{N-m}(2m)!$ $(0 \leq m \leq N)$ which occur in the left hand side of (1.8) are integers. The first one is nothing else than the special case $m = 0$ of the second one. Now for $0 \leq m \leq N$ the quotient

$$\frac{(2N)!}{(2m)!} = (2N)(2N-1)(2N-2) \cdots (2m+2)(2m+1)$$

is the product of $2N-2m$ consecutive integers, $N-m$ of which are even; hence it is a multiple of 2^{N-m}.

The same proof shows that the number $\sqrt{2}(e^{\sqrt{2}}-e^{-\sqrt{2}})$ is also irrational, but the argument does not seem to lead to the conclusion that $e^{\sqrt{2}}$ is not a quadratic number.

1.2.4 The number e^2 is not quadratic

The proof below is the one given by J. Liouville in 1840 [24] . See also [8].

We saw in § 1.2.2 that there was a difficulty to prove that e is not a quadratic number if we were to follow too closely Fourier's initial idea. Considering e^{-1} provided the clue. Now we prove that e^2 is not a quadratic number by truncating the series at carefully selected places. Consider a relation $ae^4+be^2+c=0$ with rational integer coefficients a, b and c. Write $ae^2+b+ce^{-2}=0$. Hence

$$\frac{N!b}{2^{N-1}}+\sum_{n=0}^{N}\left(a+(-1)^n c\right)\frac{N!}{2^{N-n-1}n!}=-\sum_{k\geq 0}\left(a+(-1)^{N+1+k}c\right)\frac{2^k N!}{(N+1+k)!}.$$

Like in § 1.2.2, the right hand side tends to 0 as N tends to infinity, and if the two first terms of the series vanish for some value of N, then we conclude $a=c=0$. What remains to be proved is that the numbers

$$\frac{N!}{2^{N-n-1}n!},\quad (0\leq n\leq N)$$

are integers. For $n=0$ this is the coefficient of b, namely $2^{-N+1}N!$. The fact that these numbers are integers is not true for all values of N, it is not true even for all sufficiently large N; but we do not need so much, it suffices that they are integers for infinitely many N, and that much is true.

The exponent $v_p(N!)$ of p in the prime decomposition of $N!$ is given by the (finite) sum (see for instance [16])

$$v_p(N!)=\sum_{j\geq 1}\left[\frac{N}{p^j}\right]. \tag{1.9}$$

Using the trivial upper bound $[m/p^j]\leq m/p^j$ we deduce the upper bound

$$v_p(n!)\leq\frac{n}{p-1}$$

for all $n\geq 0$. In particular $v_2(n!)\leq n$. On the other hand, when N is a power of p, say $N=p^t$, then (1.9) yields

$$v_p(N!)=p^{t-1}+p^{t-2}+\cdots+p+1=\frac{p^t-1}{p-1}=\frac{N-1}{p-1}.$$

Therefore when N is a power of 2 the number $N!$ is divisible by 2^{N-1} and we have, for $0\leq m\leq N$,

$$v_2(N!/n!)\geq N-n-1,$$

which means that the numbers $N!/2^{N-n-1}n!$ are integers.

1.2.5 The number $e^{\sqrt{3}}$ is irrational

Set $\vartheta = e^{\sqrt{3}} + e^{-\sqrt{3}}$. From the series expansion of the exponential function we derive

$$\frac{(2N)!}{3^{N-1}}\vartheta - 2\sum_{m=0}^{N}\frac{(2N)!}{(2m)!3^{N-m-1}} = 2\sum_{k\geq 0}\frac{3^k(2N)!}{(2N+2k+2)!}.$$

Take N of the form $(3^t+1)/2$ for some sufficiently large integer t. We deduce from (1.9) with $p=3$

$$v_3((2N)!) = \frac{3^t-1}{2} = N-1, \quad v_3((2m)!) \leq m, \quad (0 \leq m \leq N)$$

hence $v_3((2N)!/(2m)!) \geq N-m-1$.

1.2.6 Is-it possible to go further?

The same argument does not seem to yield the irrationality of e^3. The range of applications of this method is limited. The main ideas allowing to go further have been introduced by Charles Hermite. These new ideas are basic for the development of transcendental number theory which we shall discuss later.

1.2.7 A geometrical proof of the irrationality of e

The following proof of the irrationality of e is due to Jonathan Sondow [34]. Start with an interval I_1 of length 1. We are going to construct inductively a sequence of intervals $(I_n)_{n\geq 1}$, where for each n the interval I_n is obtained by splitting I_{n-1} into n intervals of the same length and keeping only one such piece. Hence the length of I_n will be $1/n!$.

In order to have the origin of I_n as

$$1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}$$

we start with $I_1 = [2,3]$. For $n \geq 2$, split I_{n-1} into n intervals and keep the second one: this is I_n. Hence

$$\begin{aligned}
I_1 &= \left[1 + \frac{1}{1!}\,,\, 1 + \frac{2}{1!}\right] = [2,3],\\
I_2 &= \left[1 + \frac{1}{1!} + \frac{1}{2!}\,,\, 1 + \frac{1}{1!} + \frac{2}{2!}\right] = \left[\frac{5}{2!}\,,\, \frac{6}{2!}\right],\\
I_3 &= \left[1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!}\,,\, 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{2}{3!}\right] = \left[\frac{16}{3!}\,,\, \frac{17}{3!}\right].
\end{aligned}$$

The origin of I_n is

$$1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} = \frac{a_n}{n!},$$

the length is $1/n!$, hence the endpoint of I_n is $(a_n+1)/n!$. Also for $n \geq 1$ we have $a_{n+1} = (n+1)a_n + 1$.

The number e is the intersection of all these intervals, hence it lies in the interior of each I_n, and therefore it cannot be written as $a/n!$ with $a \in \mathbb{Z}$.

Since

$$\frac{p}{q} = \frac{(q-1)!\,p}{q!},$$

the irrationality of e follows.

As pointed out by Sondow in [34], the proof shows that for any integer $n > 1$,

$$\frac{1}{(n+1)!} < \min_{m\in\mathbb{Z}} \left|e - \frac{m}{n!}\right| < \frac{1}{n!}.$$

The *Smarandache function* is defined as follows: $S(q)$ is the least positive integer such that $S(q)!$ is a multiple of q:

$$S(1) = 1,\ S(2) = 2,\ S(3) = 3,\ S(4) = 4,\ S(5) = 5,\ S(6) = 3\ldots$$

Hence $S(n) \leq n$ or all $n \geq 1$, $S(p) = p$ for p prime and $S(n!) = n$. From his proof Sondow [34] deduces an irrationality measure for e: *for any* $p/q \in \mathbb{Q}$,

$$\left|e - \frac{p}{q}\right| > \frac{1}{(S(q)+1)!}.$$

1.3 Irrationality Criteria

The main tool in Diophantine approximation is the basic property that *any non-zero integer has absolute value at least* 1. There are many consequences of this fact. The first one we consider here is the following:
If ϑ is a rational number, there is a positive constant $c = c(\vartheta)$ such that, for any rational number p/q with $p/q \neq \vartheta$,

$$\left|\vartheta - \frac{p}{q}\right| \geq \frac{c}{q}. \tag{1.10}$$

This result is obvious: if $\vartheta = a/b$ then an admissible value for c is $1/b$, because the non-zero integer $aq - bp$ has absolute value at least 1.

This property is characteristic of rational numbers: a rational number cannot be well approximated by other rational numbers, while an irrational number can be well approximated by rational numbers.

We now give several such criteria. The first one was used implicitly in § 1.2.

1.3.1 Statement of the first criterion

Lemma 1.11. *Let ϑ be a real number. The following conditions are equivalent*
(i) *ϑ is irrational.*

(ii) *For any* $\epsilon > 0$ *there exists* $p/q \in \mathbb{Q}$ *such that*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{\epsilon}{q}.$$

(iii) *For any real number* $Q > 1$ *there exists an integer* q *in the range* $1 \leq q < Q$ *and a rational integer* p *such that*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{1}{qQ}.$$

(iv) *There exist infinitely many* $p/q \in \mathbb{Q}$ *such that*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{1}{q^2}.$$

So far we needed only (ii)⇒(i), which is the easiest part, as we just checked in (1.10).

According to this implication, in order to prove that some number is irrational, it is sufficient (and in fact also necessary) to produce good rational approximations. Lemma 1.11 tells us that an irrational real number ϑ has very good *friends* among the rational numbers, the sharp inequality (iv) shows indeed that ϑ is well approximated by rational numbers (and a sharper version of (iv) will be proved in Lemma 1.14 below). Conversely, the proof we just gave shows that a rational number has *no good friend*, apart from himself. Hence in this world of rational approximation it suffices to have one good friend (not counting oneself) to guarantee that one has many very good friends.

1.3.2 Proof of Dirichlet's Theorem (i)⇒(iii) in the criterion 1.11

The implications (iii)⇒(iv)⇒(ii)⇒(i) in Lemma 1.11 are easy. It only remains to prove (i)⇒(iii), which is a Theorem due to Dirichlet. For this we shall use the *box* or *pigeon hole* principle.

Proof of (i)⇒(iii). Let $Q > 1$ 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 $N \geq 2$.

For $x \in \mathbb{R}$ write $x = [x] + \{x\}$ with $[x] \in \mathbb{Z}$ (integral part of x) and $0 \leq \{x\} < 1$ (fractional part of x). Let $\vartheta \in \mathbb{R} \setminus \mathbb{Q}$. Consider the subset E of the unit interval $[0, 1]$ which consists of the $N + 1$ elements

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

Since ϑ is irrational, these $N+1$ elements are pairwise distinct. Split the interval $[0, 1]$ into N intervals

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

One at least of these N intervals, say I_{j_0}, contains at least two elements of E. Apart from 0 and 1, all elements $\{q\vartheta\}$ in E with $1 \leq q \leq N-1$ are irrational, hence belong to the union of the *open* intervals $(j/N,\ (j+1)/N)$ with $0 \leq j \leq N-1$.

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 $\{q\vartheta\}$ with $1 \leq q \leq N-1$. Set $p = [q\vartheta] + 1$. Then we have $1 \leq q \leq N-1 < Q$ and

$$p - q\vartheta = [q\vartheta] + 1 - [q\vartheta] - \{q\vartheta\} = 1 - \{q\vartheta\}, \quad \text{hence} \quad 0 < p - q\vartheta < \frac{1}{N} \leq \frac{1}{Q}.$$

Otherwise we have $0 \leq j_0 \leq N-2$ and I_{j_0} contains two elements $\{q_1\vartheta\}$ and $\{q_2\vartheta\}$ with $0 \leq q_1 < q_2 \leq N-1$. Set

$$q = q_2 - q_1, \quad p = [q_2\vartheta] - [q_1\vartheta].$$

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

$$|q\vartheta - p| = |\{q_2\vartheta\} - \{q_1\vartheta\}| < 1/N \leq 1/Q.$$

□

There are other proofs of (i)⇒(iii) – for instance one can use Minkowski's Theorem in the geometry of numbers, which is more powerful than Dirichlet's box principle. We shall come back to this point in section § 2.2.7.

Exercise 1.12. This exercise extends the irrationality criterion Lemma 1.11 by replacing $\mathbb{Q}$ by $\mathbb{Q}(i)$. The elements in $\mathbb{Q}(i)$ are called the *Gaussian numbers*, the elements in $\mathbb{Z}(i)$ are called the *Gaussian integers*. The elements of $\mathbb{Q}(i)$ will be written p/q with $p \in \mathbb{Z}[i]$ and $q \in \mathbb{Z}$, $q > 0$.

Let ϑ be a complex number. Check that the following conditions are equivalent.
(i) $\vartheta \notin \mathbb{Q}(i)$.
(ii) For any $\epsilon > 0$ there exists $p/q \in \mathbb{Q}(i)$ such that

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{\epsilon}{q}.$$

(iii) For any rational integer $N \geq 1$ there exists a rational integer q in the range $1 \leq q \leq N^2$ and a Gaussian integer p such that

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{\sqrt{2}}{qN}.$$

(iv) There exist infinitely many Gaussian numbers $p/q \in \mathbb{Q}(i)$ such that

$$\left|\vartheta - \frac{p}{q}\right| < \frac{\sqrt{2}}{q^{3/2}}.$$

1.3.3 Irrationality of at least one number

We shall use the following variant of Lemma 1.11 later.

Lemma 1.13. *Let $\vartheta_1, \dots, \vartheta_m$ be real numbers. The following conditions are equivalent*
(i) *One at least of $\vartheta_1, \dots, \vartheta_m$ is irrational.*
(ii) *For any $\epsilon > 0$ there exist $p_1, \dots, p_m, q$ in $\mathbb{Z}$ with $q > 0$ such that*

$$0 < \max_{1 \le i \le m} \left| \vartheta_i - \frac{p_i}{q} \right| < \frac{\epsilon}{q}.$$

(iii) *For any integer $Q > 1$ there exists $p_1, \dots, p_m, q$ in $\mathbb{Z}$ such that $1 \le q \le Q^m$ and*

$$0 < \max_{1 \le i \le m} \left| \vartheta_i - \frac{p_i}{q} \right| \le \frac{1}{qQ}.$$

(iv) *There is an infinite set of $q \in \mathbb{Z}$, $q > 0$, for which there there exist $p_1, \dots, p_m$ in $\mathbb{Z}$ satisfying*

$$0 < \max_{1 \le i \le m} \left| \vartheta_i - \frac{p_i}{q} \right| < \frac{1}{q^{1+1/m}}.$$

Proof. The proofs of (iii)⇒(iv)⇒(ii)⇒(i) are easy.

For (i)⇒(iii) we use Dirichlet's box principle [1] like in the proof of Lemma 1.11. Consider the $Q^m + 1$ elements

$$\xi_q = \big(\{q\vartheta_1\}, \dots, \{q\vartheta_m\}\big) \quad (q = 0, 1, \dots, Q^m)$$

in the unit cube $[0, 1)^m$ of $\mathbb{R}^m$. Split this unit cube into Q^m cubes having sides of lengths $1/Q$. One at least of these small cubes contains at least two ξ_q, say ξ_{q_1} and ξ_{q_2}, with $0 \le q_2 < q_1 \le Q^m$. Set $q = q_1 - q_2$ and take for p_i the nearest integer to ϑ_i, $1 \le i \le m$. This completes the proof of Lemma 1.13.

□

1.3.4 Hurwitz Theorem

The following result improves the implication (i)⇒(iv) of Lemma 1.11.

Lemma 1.14. *Let ϑ be a real number. The following conditions are equivalent*
(i) *ϑ is irrational.*
(ii) *There exist infinitely many $p/q \in \mathbb{Q}$ such that*

$$0 < \left| \vartheta - \frac{p}{q} \right| < \frac{1}{\sqrt{5}q^2}.$$

[1] An alternative arguments relies on geometry of numbers - see section § 2.2.7 and W.M. Schmidt's lecture notes - as a consequence it is not necessary to assume that Q is an integer, and the strict inequality $q < Q^m$ can be achieved.

Of course the implication (ii)⇒(i) in Lemma 1.14 is weaker than the implication (iv)⇒(i) in Lemma 1.11. What is new is the converse.

Classical proofs of the equivalence between (i) and (iv) involve either continued fractions or Farey series. We give here a proof which does not involve continued fractions, but they occur implicitly.

Lemma 1.15. *Let ϑ be a real irrational number. Then there exists infinitely many pairs $(p/q, r/s)$ of irreducible fractions such that*

$$\frac{p}{q} < \vartheta < \frac{r}{s} \quad \textit{and} \quad qr - ps = 1.$$

In this statement and the next ones it is sufficient to prove inequalities $\leq$ in place of $<$: the strict inequalities are plain from the irrationality of ϑ.

Proof. First let H be a positive integer. Among the irreducible rational fractions a/b with $1 \leq b \leq H$, select one for which $|\vartheta - a/b|$ is minimal. If $a/b < \vartheta$ rename a/b as p/q, while if $a/b > \vartheta$, then rename a/b as r/s.

First consider the case where $a/b < \vartheta$, hence $a/b = p/q$. Since $\gcd(p, q) = 1$, using Euclidean's algorithm, one deduces (Bézout's Theorem) that there exist $(r, s) \in \mathbb{Z}^2$ such that $qr - sp = 1$ with $1 \leq s < q$ and $|r| < |p|$. Since $1 \leq s < q \leq H$, from the choice of a/b it follows that

$$\left|\vartheta - \frac{p}{q}\right| \leq \left|\vartheta - \frac{r}{s}\right|$$

hence r/s does not belong to the interval $[p/q, \vartheta]$. Since $qr - sp > 0$ we also have $p/q < r/s$, hence $\vartheta < r/s$.

In the second case where $a/b > \vartheta$ and $r/s = a/b$ we solve $qr - sp = 1$ by Euclidean algorithm with $1 \leq q < s$ and $|p| < r$, and the argument is similar.

We now complete the proof of infinitely many such pairs. Once we have a finite set of such pairs $(p/q, r/s)$, we use the fact that there is a rational number closer to ϑ than any of these rational fractions. We use the previous argument with $H = \max\{|a|, b\}$. This way we produce a new pair $(p/q, r/s)$ of rational numbers which is none of the previous ones (because one at least of the two rational numbers p/q, r/s is a better approximation than the previous ones). Hence this construction yields infinitely many pairs, as claimed.

□

Lemma 1.16. *Let ϑ be a real irrational number. Assume $(p/q, r/s)$ are irreducible fractions such that*

$$\frac{p}{q} < \vartheta < \frac{r}{s} \quad \textit{and} \quad qr - ps = 1.$$

Then

$$\min\left\{q^2\left(\vartheta - \frac{p}{q}\right)\ ,\ s^2\left(\frac{r}{s} - \vartheta\right)\right\} < \frac{1}{2}.$$

Proof. Define

$$\delta = \min\left\{q^2\left(\vartheta - \frac{p}{q}\right)\ ,\ s^2\left(\frac{r}{s} - \vartheta\right)\right\}.$$

From

$$\frac{\delta}{q^2} \leq \vartheta - \frac{p}{q} \quad \text{and} \quad \frac{\delta}{s^2} \leq \frac{r}{s} - \vartheta$$

one deduces that the number $t = s/q$ satisfies

$$t + \frac{1}{t} \leq \frac{1}{\delta}.$$

Since the minimum of the function $t \mapsto t + 1/t$ is 2 and since $t \neq 1$, we deduce $\delta < 1/2$.

□

Remark. *The inequality $t + (1/t) \geq 2$ for all $t > 0$ with equality if and only if $t = 1$ is equivalent to the arithmetico-geometric inequality*

$$\sqrt{xy} \leq \frac{x+y}{2},$$

when x and y are positive real numbers, with equality if and only if $x = y$. The correspondance between both estimates is $t = \sqrt{x/y}$.

From Lemmas 1.15 and 1.16 it follows that for $\vartheta \in \mathbb{R}\setminus\mathbb{Q}$, there exist infinitely many $p/q \in \mathbb{Q}$ such that

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

A further step is required in order to complete the proof of Lemma 1.14.

Lemma 1.17. *Let ϑ be a real irrational number. Assume $(p/q, r/s)$ are irreducible fractions such that*

$$\frac{p}{q} < \vartheta < \frac{r}{s} \quad \textit{and} \quad qr - ps = 1.$$

Define $u = p + r$ and $v = q + s$. Then

$$\min\left\{q^2\left(\vartheta - \frac{p}{q}\right)\ ,\ s^2\left(\frac{r}{s} - \vartheta\right)\ ,\ v^2\left|\vartheta - \frac{u}{v}\right|\right\} < \frac{1}{\sqrt{5}}.$$

Proof. First notice that $qu - pv = 1$ and $rv - su = 1$. Hence

$$\frac{p}{q} < \frac{u}{v} < \frac{r}{s}.$$

We repeat the proof of lemma 1.16 ; we distinguish two cases according to whether u/v is larger or smaller than ϑ. Since both cases are quite similar, let us assume $\vartheta < u/v$. The proof of lemma 1.16 shows that

$$\frac{s}{q} + \frac{q}{s} \leq \frac{1}{\delta} \quad \text{and} \quad \frac{v}{q} + \frac{q}{v} \leq \frac{1}{\delta}.$$

Hence each of the four numbers s/q, q/s, v/q, q/v satisfies $t + 1/t \leq 1/\delta$. Now the function $t \mapsto t+1/t$ is decreasing on the interval $(0, 1)$ and increasing on the interval $(1, +\infty)$. It follows that our four numbers all lie in the interval $(1/x, x)$, where x is the root > 1 of the equation $x+1/x = 1/\delta$. The two roots x and $1/x$ of the quadratic polynomial $X^2 - (1/\delta)X + 1$ are at a mutual distance equal to the square root of the discriminant $\Delta = (1/\delta)^2 - 4$ of this polynomial. Now

$$\frac{v}{q} - \frac{s}{q} = 1,$$

hence the length $\sqrt{\Delta}$ of the interval $(1/x, x)$ is ≥ 1 and therefore $\delta \geq 1/\sqrt{5}$. This completes the proof of Lemma 1.17. □

We now show that Lemma 1.14 is optimal.

Denote again by $\Phi = 1.6180339887499\ldots$ the Golden ratio, which is the root > 1 of the polynomial $X^2 - X - 1$. The discriminant of this polynomial is 5. Recall also the definition of the Fibonacci sequence $(F_n)_{n\geq 0}$:

$$F_0 = 0,\ F_1 = 1,\ F_n = F_{n-1} + F_{n-2} \quad (n \geq 2).$$

Lemma 1.18. *For any $q \geq 1$ and any $p \in \mathbb{Z}$,*

$$\left|\Phi - \frac{p}{q}\right| > \frac{1}{\sqrt{5}q^2 + (q/2)}.$$

On the other hand

$$\lim_{n\to\infty} F_{n-1}^2 \left|\Phi - \frac{F_n}{F_{n-1}}\right| = \frac{1}{\sqrt{5}}.$$

Proof. It suffices to prove the lower bound when p is the nearest integer to $q\Phi$. From $X^2 - X - 1 = (X - \Phi)(X + \Phi^{-1})$ we deduce

$$p^2 - pq - q^2 = q^2 \left(\frac{p}{q} - \Phi\right)\left(\frac{p}{q} + \Phi^{-1}\right).$$

The left hand side is a non-zero rational integer, hence has absolute value at least 1. We now bound the absolute value of the right hand side from above. Since $p < q\Phi + (1/2)$ and $\Phi + \Phi^{-1} = \sqrt{5}$ we have

$$\frac{p}{q} + \Phi^{-1} \leq \sqrt{5} + \frac{1}{2q}.$$

Hence

$$1 \leq q^2 \left|\frac{p}{q} - \Phi\right| \left(\sqrt{5} + \frac{1}{2q}\right)$$

The first part of Lemma 1.18 follows.

The real vector space of sequences $(v_n)_{n\geq 0}$ satisfying $v_n = v_{n-1} + v_{n-2}$ has dimension 2, a basis is given by the two sequences $(\Phi^n)_{n\geq 0}$ and $((-\Phi^{-1})^n)_{n\geq 0}$. From this one easily deduces the formula

$$F_n = \frac{1}{\sqrt{5}}(\Phi^n - (-1)^n \Phi^{-n})$$

due to A. De Moivre (1730), L. Euler (1765) and J.P.M. Binet (1843). It follows that F_n is the nearest integer to

$$\frac{1}{\sqrt{5}}\Phi^n,$$

hence the sequence $(u_n)_{n\geq 2}$ of quotients of Fibonacci numbers

$$u_n = F_n/F_{n-1}$$

satisfies $\lim_{n\to\infty} u_n = \Phi$.

By induction one easily checks

$$F_n^2 - F_nF_{n-1} - F_{n-1}^2 = (-1)^n$$

for $n \geq 1$. The left hand side is $F_{n-1}^2(u_n - \Phi)(u_n + \Phi^{-1})$, as we already saw. Hence

$$F_{n-1}^2|\Phi - u_n| = \frac{1}{\Phi^{-1} + u_n},$$

and the limit of the right hand side is $1/(\Phi + \Phi^{-1}) = 1/\sqrt{5}$. The result follows. □

Remark. *The sequence $u_n = F_n/F_{n-1}$ is also defined by*

$$u_2 = 2,\ u_n = 1 + \frac{1}{u_{n-1}},\quad (n \geq 3).$$

Hence

$$u_n = 1 + \frac{1}{1 + \dfrac{1}{u_{n-2}}} = 1 + \frac{1}{1 + \dfrac{1}{1 + \dfrac{1}{u_{n-3}}}} = \cdots$$

Remark. *It is known (see for instance [29] p. 25) that if k is a positive integer, if an irrational real number ϑ has a continued fraction expansion $[a_0; a_1, a_2, \dots]$ with $a_n \geq k$ for infinitely many n, then*

$$\liminf_{q\to\infty} q^2 \left|\vartheta - \frac{p}{q}\right| \leq \frac{1}{\sqrt{4 + k^2}}.$$

This proof of Lemma 1.18 can be extended by replacing $X^2 - X - 1$ by any irreducible polynomial with integer coefficients. Recall that the ring $\mathbb{Z}[X]$ is factorial, its irreducible elements of positive degree are the non-constant polynomials with integer coefficients which are irreducible in $\mathbb{Q}[X]$ (i.e. not a product of two non-constant polynomials in $\mathbb{Q}[X]$) and have content 1. The *content* of a polynomial in $\mathbb{Z}[X]$ is the greatest common divisor of its coefficients.

The *minimal polynomial* of an algebraic number α is the unique irreducible polynomial $P \in \mathbb{Z}[X]$ which vanishes at α and has a positive leading coefficient.

The next lemma ([29] p. 6 Lemma 2E) is a variant of Liouville's inequality that we shall study more throughly later.

Lemma 1.19. *Let α be a real algebraic number of degree $d \geq 2$ and minimal polynomial $P \in \mathbb{Z}[X]$. Define $c = |P'(\alpha)|$. Let $\epsilon > 0$. Then there exists an integer q_0 such that, for any $p/q \in \mathbb{Q}$ with $q \geq q_0$,*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{(c+\epsilon)q^d}.$$

Proof. Let q be a sufficiently large positive integer and let p be the nearest integer to α. In particular

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{2}.$$

Denote a_0 the leading coefficient of P and by $\alpha_1, \ldots, \alpha_d$ its the roots with $\alpha_1 = \alpha$. Hence

$$P(X) = a_0(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_d)$$

and

$$q^d P(p/q) = a_0 q^d \prod_{i=1}^{d} \left(\frac{p}{q} - \alpha_i\right). \tag{1.20}$$

Also

$$P'(\alpha) = a_0 \prod_{i=2}^{d} (\alpha - \alpha_i).$$

The left hand side of (1.20) is a rational integer. It is not zero because P is irreducible of degree ≥ 2. For $i \geq 2$ we use the estimate

$$\left|\alpha_i - \frac{p}{q}\right| \leq |\alpha_i - \alpha| + \frac{1}{2q}.$$

We deduce

$$1 \leq q^d a_0 \left|\alpha - \frac{p}{q}\right| \prod_{i=2}^{d} \left(|\alpha_i - \alpha| + \frac{1}{2q}\right).$$

For sufficiently large q the right hand side is bounded from above by

$$q^d \left|\alpha - \frac{p}{q}\right| (|P'(\alpha)| + \epsilon).$$

□

If α is a real root of a quadratic polynomial $P(X) = aX^2 + bX + c$, then $P'(\alpha) = 2a\alpha + b$ is a square root of the discriminant of P. So Hurwitz Lemma 1.14 is optimal for all quadratic numbers having a minimal polynomial of discriminant 5. Incidentally, this shows that 5 is the smallest positive discriminant of an irreducible quadratic polynomial in $\mathbb{Z}[X]$ (of course it is easily checked directly that if a, b, c are three rational integers with $a > 0$ and $b^2 - 4ac$ positive and not a perfect square in $\mathbb{Z}$, then $b^2 - 4ac \geq 5$).

It follows that for the numbers of the form $(a\Phi + b)/(c\Phi + d)$ with integers a, b, c, d having $ad - bc = \pm 1$, one cannot replace in Lemma 1.14 the number $\sqrt{5}$ by a larger number.

If one omits these irrational numbers in the field generated by the Golden ratio, then Hurwitz showed that one can replace $\sqrt{5}$ by $2\sqrt{2}$, and again this is optimal. This is the beginning of the so-called *Markoff* [2] *spectrum* $\sqrt{5}$, $\sqrt{8}$, $\sqrt{221}/5$, $\sqrt{1517}/13$, ... which tends to $1/3$ and is obtained as follows. First consider the set of integers m for which the *Markoff equation*

$$m^2 + m_1^2 + m_2^2 = 3mm_1m_2$$

has a solution in positive integers (m_1, m_2) with $0 < m_1 \leq m_2 \leq m$. The infinite increasing sequence of these integers m starts with

$$1,\ 2,\ 5,\ 13,\ 29,\ 34,\ 89,\ 169,\ 194,\ 233,\ 433,\ 610,\ 985,\ 1325,\ 1597, \ldots \quad (1.21)$$

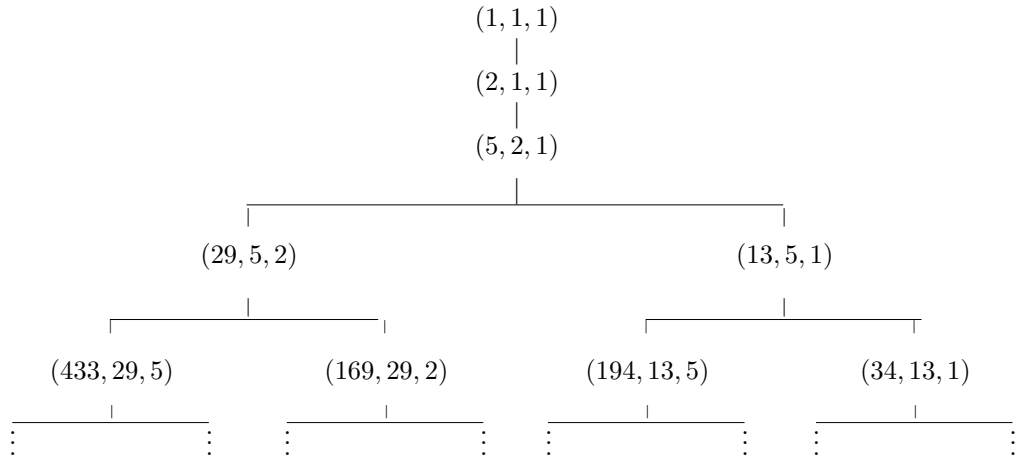
and there is an easy and well known algorithm to construct it (see for instance [36]): apart from $(1, 1, 1)$ and $(2, 1, 1)$, for any solution (m, m_1, m_2) there are three exactly solutions sharing two components with (m, m_1, m_2), namely

$$(m', m_1, m_2), \quad (m, m_1', m_2), \quad (m, m_1, m_2'),$$

where

$$m' = 3m_1m_2 - m, \quad m_1' = 3mm_2 - m_1, \quad m_2' = 3mm_1 - m_2.$$

This produces the *Markoff tree*



For each m in the Markoff sequence (1.21), we define

$$\mu_m = \frac{\sqrt{9m^2 - 4}}{m}.$$

[2] His name is spelled *Markov* in probability theory.

Then there is an explicit quadratic form $f_m(x,y)$ such that $f_m(x,1)=0$ and there is a root α_m of f_m for which

$$\limsup_{q\in\mathbb{Z},\ q\to\infty} (q\|q\alpha_m\|) = \frac{1}{\mu_m},$$

where $\|\cdot\|$ denotes the distance too the nearest integer:

$$\|x\| = \min_{m\in\mathbb{Z}} |x-m| = \min\big\{\{x\}\,;\,1-\{x\}\big\}.$$

The sequence of $(m, f_m, \alpha_m, \mu_m)$ starts as follows,

m	1	2	5	13
$f_m(x,1)$	x^2+x-1	x^2+2x-1	$5x^2+11x-5$	$13x^2+29x-13$
α_m	$[0;\overline{1}]$	$[0;\overline{2}]$	$[0;\overline{2211}]$	$[0;\overline{221111}]$
μ_m	$\sqrt{5}$	$\sqrt{8}$	$\sqrt{221}/5$	$\sqrt{1517}/13$

The third row gives the continued fraction expansion for α_m.

Exercise 1.22. Check that any solution (m, m_1, m_2) of Markoff's equation (1.21) is in Markoff's tree.

1.3.5 Irrationality of series studied by Liouville and Fredholm

The implication (ii)⇒(i) in lemma 1.11 was used implicitely in § 1.1. We give here another application.

Several methods are available to investigate the arithmetic nature of numbers of the form

$$\sum_{n\geq 0} a^{-n^2} \quad \text{and} \quad \sum_{n\geq 0} a^{-2^n} \tag{1.23}$$

where a is a positive integer.

There is apparently a confusion in the litterature between these two series. The name *Fredholm series* is often wrongly attributed to the power series

$$\sum_{n\geq 0} z^{2^n}.$$

However Fredholm studied rather the series

$$\sum_{n\geq 0} z^{n^2}$$

(see the book [2] by Allouche & Shallit, Notes on chapter 13, page 403 as well as Shallit's paper [31]).

The series $\sum_{n\geq 0} z^{n^2}$ was explicitly quoted by Liouville (see for instance [11]). We shall come back to this question later (where we discuss Nesterenko's result in 1995 according to which this number is transcendental). Right now we only prove the irrationality of the numbers (1.23) for $a \in \mathbb{Z}$, $a \geq 2$ by means of Lemma 1.11. More generally we replace the sequences $(n^2)_{n\geq 0}$ and $(2^n)_{n\geq 0}$ by more general ones: one requires that they grow and tend to infinity sufficiently fast.

Lemma 1.24. *Let $(u_n)_{n\geq 0}$ be an increasing sequence of positive numbers. Assume there exists $c > 0$ such that, for all sufficiently large n,*

$$u_n - u_{n-1} \geq cn.$$

Let $a \in \mathbb{Z}$, $a \geq 2$. Then the number

$$\vartheta = \sum_{n\geq 0} a^{-u_n}$$

is irrational.

Proof. Let $\epsilon > 0$. Let N be a sufficiently large integer. Set

$$q_N = a^{u_N}, \quad p_N = \sum_{n=0}^{N} a^{u_N - u_n} \quad \text{and} \quad R_N = q_N\vartheta - p_N.$$

Then p_N and q_N are rational integers, while

$$R_N = \sum_{k=1}^{\infty} a^{u_N - u_{N+k}}$$

is > 0.

By induction on $k \geq 1$ one checks

$$u_{N+k} \geq u_N + ckN + v_k \quad \text{where} \quad v_k := c\frac{k(k-1)}{2}.$$

Therefore

$$u_{N+k} - u_N - cN \geq (k-1)cN + v_k \geq v_k$$

and

$$0 < R_N \leq a^{-cN} \sum_{k\geq 1} a^{-v_k}.$$

Hence R_N tends to 0 as N tends to infinity and Lemma 1.11 shows that ϑ is irrational. □

Exercise 1.25. Let $b \geq 2$ be an integer. Let $(a_n)_{n\geq 0}$ be a bounded sequence of rational integers and $(u_n)_{n\geq 0}$ an increasing sequence of positive numbers. Assume there exists $c > 0$ and $n_0 \geq 0$ such that, for all $n \geq n_0$,

$$u_{n+1} - u_n \geq cn.$$

a) Deduce, for all $k \geq 1$ and $n \geq n_0$,

$$u_{n+k} - u_n \geq cnk + c \cdot \frac{k(k-1)}{2}.$$

b) Show that the number

$$\vartheta = \sum_{n\geq 0} a_n b^{-u_n}$$

is irrational if and only if the set $\{n \geq 0 \ ; \ a_n \neq 0\}$ is infinite.
c) Deduce another proof of Lemma 1.24 in § 1.3.5.

1.3.6 A further irrationality criterion

Lemma 1.26. *Let ϑ be a real number. The following conditions are equivalent*
(i) *ϑ is irrational.*
(ii) *For any $\epsilon > 0$ there exists p/q and r/s in $\mathbb{Q}$ such that*

$$\frac{p}{q} < \vartheta < \frac{r}{s}, \quad qr - ps = 1$$

and

$$\max\{q\vartheta - p \ ; \ r - s\vartheta\} < \epsilon.$$

(iii) *There exist infinitely many pairs $(p/q, r/s)$ of rational numbers such that*

$$\frac{p}{q} < \vartheta < \frac{r}{s}, \quad qr - ps = 1$$

and

$$\max\{q(q\vartheta - p) \ ; \ s(r - s\vartheta)\} < 1.$$

Proof. The implications (iii)⇒(ii)⇒(i) are easy. For (i)⇒(iii) we use the arguments in the proof of Lemma 1.15, but we use also an auxiliary result from the theory of continued fractions.

Since ϑ is irrational, Hurwitz Lemma 1.14 shows that there are infinitely many p/q such that

$$\left|\vartheta - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

We shall use the fact that such a p/q is a so-called *best approximation to ϑ*: this means that for any $a/b \in \mathbb{Q}$ with $1 \leq b \leq q$ and $a/b \neq p/q$, we have

$$\left|\vartheta - \frac{a}{b}\right| > \left|\vartheta - \frac{p}{q}\right|.$$

Assume first $p/q < \vartheta$. Let r/s be defined by $qr - ps = 1$ and $1 \leq s < q$, $|r| < |p|$. We have

$$0 < \frac{r}{s} - \vartheta < \frac{r}{s} - \frac{p}{q} = \frac{1}{qs} \leq \frac{1}{s^2}.$$

Next assume $p/q > \vartheta$. In this case rename it r/s and define p/q by $qr - ps = 1$ and $1 \leq q < s$, $|p| < |r|$.

Finally repeat the argument in the proof of Lemma 1.15 to get an infinite set of approximations. Lemma 1.26 follows. □

1.4 Irrationality of e^r and π, following Nesterenko

The proofs given in subsection 1.2 of the irrationality of e^r for several rational values of r (namely $r \in \{1/a, 2/a, \sqrt{2}/a, \sqrt{3}/a \ ; \ a \in \mathbb{Z}, \ a \neq 0\}$) are similar: the idea is to start from the expansion of the exponential function, to truncate it and to deduce rational approximations to e^r. In terms of the exponential function this amounts to approximate e^z by a polynomial. The main idea, due to C. Hermite [17], is to approximate e^z by rational functions $A(z)/B(z)$. The word "approximate" has the following meaning (Hermite-Padé): an analytic function is well approximated by a rational function $A(z)/B(z)$ (where A and B are polynomial) if the difference $B(z)f(z) - A(z)$ has a zero at the origin of high multiplicity.

When we just truncate the series expansion of the exponential function, we approximate e^z by a polynomial in z with rational coefficients; when we substitute $z = a$ where a is a positive integer, this polynomial produces a rational number, but the denominator of this number is quite large (unless $a = \pm 1$). A trick gave the result also for $a = \pm 2$, but definitely for a a larger prime number for instance there is a problem: if we multiply by the denominator then the "remainder" is by no means small. To produce a sufficiently large gap in the power expansion of $B(z)e^z$ will solve the problem.

Our first goal in this section is to prove the irrationality of e^r when r is a non-zero rational number. Next we show how a slight modification implies the irrationality of π.

1.4.1 Irrationality of e^r for $r \in \mathbb{Q}$

If $r = a/b$ is a rational number such that e^r is also rational, then $e^{|a|}$ is also rational, and therefore the irrationality of e^r for any non-zero rational number r follows from the irrationality of e^a for any positive integer a. We shall approximate the exponential function e^z by a rational function $A(z)/B(z)$ and show that $A(a)/B(a)$ is a good rational approximation to e^a, sufficiently good in fact so that one may use Lemma 1.11.

Write

$$e^z = \sum_{k \geq 0} \frac{z^k}{k!}.$$

We wish to multiply this series by a polynomial so that the Taylor expansion at the origin of the product $B(z)e^z$ has a large gap: the polynomial preceding the gap will be $A(z)$, the remainder $R(z) = B(z)e^z - A(z)$ will have a zero of high multiplicity at the origin.

In order to create such a gap, we shall use the differential equation of the exponential function - hence we introduce derivatives.

We first explain how to produce, from an analytic function whose Taylor development at the origin is

$$f(z) = \sum_{k\geq 0} a_k z^k, \tag{1.27}$$

another analytic function with one given Taylor coefficient, say the coefficient of z^m, is zero. The coefficient of z^m for f is $f^{(m)}(0) = a^m/m!$. The same number a_m occurs when one computes the Taylor coefficient of z^{m-1} for the derivative f' of f, it is also the Taylor coefficient of z^m in the development of $zf'(z)$:

$$(zf')^{(m)}(0) = \frac{a^m}{(m-1)!}\cdot$$

Hence the coefficient of z^m in the Taylor development of $zf'(z) - mf(z)$ is 0, which is what we wanted.

It is the same thing to write

$$zf'(z) = \sum_{k\geq 0} ka_k z^k$$

so that

$$zf'(z) - mf(z) = \sum_{k\geq 0}(k-m)a_k z^k.$$

Now we want that several consecutive Taylor coefficients cancel. It will be convenient to introduce derivative operators.

We start with $D = d/dz$. As usual D^2 denotes $D \circ D$ and $D^m = D^{m-1} \circ D$ for $m \geq 2$. The derivation D and the multiplication by z do not commute:

$$D(zf) = f + zD(f),$$

relation which we write $Dz = 1 + zD$. From this relation it follows that the non-commutative ring generated by z and D over $\mathbb{C}$ is also the ring of polynomials in D with coefficients in $\mathbb{C}[z]$. In this ring $\mathbb{C}[z][D]$ there is an element which will be very useful for us, namely $\delta = zd/dz$. It satisfies $\delta(z^k) = kz^k$. To any polynomial $T \in \mathbb{C}[X]$ one associate the derivative operator $T(\delta)$.

By induction on m one checks $\delta^m z^k = k^m z^k$ for all $m \geq 0$. By linearity, one deduces that if T is a polynomial with complex coefficients, then

$$T(\delta)z^k = T(k)z^k.$$

For our function f with the Taylor development (1.27) we have

$$T(\delta)f(z) = \sum_{k\geq 0} a_k T(k) z^k.$$

Hence if we want a function with a Taylor expansion having 0 as coefficient of z^k, it suffices to consider $T(\delta)f(z)$ where T is a polynomial satisfying $T(k) = 0$. For instance if n_0 and n_1 are two non-negative integers and if we take

$$T(X) = (X - n_0 - 1)(X - n_0 - 2)\cdots(X - n_0 - n_1),$$

then the series $T(\delta)f(z)$ can be written $A(z) + R(z)$ with

$$A(z) = \sum_{k=0}^{n_0} T(k) a_k z^k$$

and

$$R(z) = \sum_{k\geq n_0+n_1+1} T(k) a_k z^k.$$

This means that in the Taylor expansion at the origin of $T(\delta)f(z)$, all coefficients of $z^{n_0+1}, z^{n_0+2}, \ldots, z^{n_0+n_1}$ are 0.

Let $n_0 \geq 0$, $n_1 \geq 0$ be two integers. Define $N = n_0 + n_1$ and

$$T(X) = (X - n_0 - 1)(X - n_0 - 2)\cdots(X - N).$$

Since T is monic of degree n_1 with integer coefficients, it follows from the differential equation of the exponential function

$$\delta(e^z) = ze^z$$

that there is a polynomial $B \in \mathbb{Z}[z]$, which is monic of degree n_1, such that $T(\delta)e^z = B(z)e^z$.

Set

$$A(z) = \sum_{k=0}^{n_0} T(k)\frac{z^k}{k!} \quad \text{and} \quad R(z) = \sum_{k\geq N+1} T(k)\frac{z^k}{k!}\cdot$$

Then

$$B(z)e^z = A(z) + R(z),$$

where A is a polynomial with rational coefficients of degree n_0 and leading coefficient

$$\frac{T(n_0)}{n_0!} = (-1)^{n_1}\frac{n_1!}{n_0!}\cdot$$

Also the analytic function R has a zero of multiplicity $\geq N + 1$ at the origin.

We can explicit these formulae for A and R. For $0 \leq k \leq n_0$ we have

$$\begin{aligned} T(k) &= (k - n_0 - 1)(k - n_0 - 2)\cdots(k - N) \\ &= (-1)^{n_1}(N - k)\cdots(n_0 + 2 - k)(n_0 + 1 - k) \\ &= (-1)^{n_1}\frac{(N-k)!}{(n_0-k)!}\cdot \end{aligned}$$

For $k \geq N+1$ we write in a similar way

$$T(k) = (k-n_0-1)(k-n_0-2)\cdots(k-N) = \frac{(k-n_0-1)!}{(k-N-1)!}.$$

Hence we have proved:

Proposition 1.28 (Hermite's formulae for the exponential function)**.** *Let $n_0 \geq 0$, $n_1 \geq 0$ be two integers. Define $N = n_0 + n_1$. Set*

$$A(z) = (-1)^{n_1} \sum_{k=0}^{n_0} \frac{(N-k)!}{(n_0-k)!k!} \cdot z^k \quad \text{and} \quad R(z) = \sum_{k \geq N+1} \frac{(k-n_0-1)!}{(k-N-1)!} \cdot z^k.$$

Finally, define $B \in \mathbb{Z}[z]$ by the condition

$$(\delta - n_0 + 1)(\delta - n_0 + 2)\cdots(\delta - N)e^z = B(z)e^z.$$

Then

$$B(z)e^z = A(z) + R(z).$$

Further, B is a monic polynomial with integer coefficients of degree n_1, A is a polynomial with rational coefficients of degree n_0 and leading coefficient $(-1)^{n_1} n_1!/n_0!$, and the analytic function R has a zero of multiplicity $N+1$ at the origin.
Furthermore, if $n_1 \geq n_0$, then the coefficients of A are integers.

Proof. It remains only to check the last assertion on the integrality of the coefficients of A for $n_1 \geq n_0$. Indeed when $n_1 \geq n_0$ each coefficient of the polynomial A is an integral multiple of a binomial coefficient:

$$\frac{(N-k)!}{(n_0-k)!k!} = (N-k)(N-k-1)\cdots(n_0+1) \cdot \frac{n_0!}{(n_0-k)!k!}$$

for $0 \leq k \leq n_0$. Hence $A \in \mathbb{Z}[z]$. □

We now restrict to the case $n_0 = n_1$ and we set $n = n_0 = n_1$. We write also

$$T_n(z) = (z-n-1)(z-n-2)\cdots(z-2n)$$

and we denote by A_n, B_n and R_n the Hermite polynomials and the remainder in Hermite's Proposition 1.28.

Remark. *For $n_1 < n_0$ the leading coefficient of A is not an integer, but the polynomial $n_0!A$ always has integer coefficients.*

Lemma 1.29. *Let $z \in \mathbb{C}$. Then*

$$|R_n(z)| \leq \frac{|z|^{2n+1}}{n!} e^{|z|}.$$

In particular the sequence $(R_n(z))_{n \geq 0}$ tends to 0 as n tends to infinity.

Proof. We have

$$R_n(z) = \sum_{k \geq 2n+1} \frac{(k-n-1)!}{(k-2n-1)!k!} \cdot z^k = \sum_{\ell \geq 0} \frac{(\ell+n)!}{(\ell+2n+1)!} \cdot \frac{|z|^{\ell+2n+1}}{\ell!}.$$

The trivial upper bound

$$\prod_{j=n+1}^{n+\ell} j \leq \prod_{j=n+1}^{n+\ell} (j+n+1)$$

is equivalent to

$$\frac{(\ell+n)!}{(\ell+2n+1)!} \leq \frac{n!}{(2n+1)!},$$

hence

$$|R_n(z)| \leq \frac{n!|z|^{2n+1}}{(2n+1)!} \sum_{\ell \geq 0} \frac{|z|^\ell}{\ell!}.$$

We bound $n!/(2n+1)!$ by $n!$: Lemma 1.29 follows. □

We are now able to complete the proof of the irrationality of e^r for $\in \mathbb{Q}$, $r \neq 0$.

Let $r = a/b$ be a non-zero rational number. Assume first r is positive. Set $s = e^r$ and replace z by $a = br$ in the previous formulae; we deduce

$$B_n(a)s^b - A_n(a) = R_n(a).$$

All coefficients in R_n are positive, hence $R_n(a) > 0$. Therefore $B_n(a)s^b - A_n(a) \neq 0$. Since $R_n(a)$ tends to 0 when n tends to infinity and since $B_n(a)$ and $A_n(a)$ are rational integers, we may use the implication (ii)⇒(i) in Lemma 1.11: we deduce that the number s^b is irrational. As we already saw this readily implies that $s = e^r$ and $s^{-1} = e^{-r}$ are irrational.

1.4.2 Irrationality of π

The proof of the irrationality of $\log s$ for s a positive rational number given in § 1.4.1 can be extended to the case $s = -1$ in such a way that one deduces the irrationality of the number π (this result was first proved by H. Lambert in 1761 [20], using continued fraction expansion for the tangent function).

Assume π is a rational number, $\pi = a/b$. Substitute $z = ia = i\pi b$ in the previous formulae. Notice that $e^z = (-1)^b$:

$$B_n(ia)(-1)^b - A_n(ia) = R_n(ia),$$

and that the two complex numbers $A_n(ia)$ and $B_n(ia)$ are in $\mathbb{Z}[i]$. The left hand side is in $\mathbb{Z}[i]$, the right hand side tends to 0 as n tends to infinity, hence both sides are 0.

In the proof of § 1.4.1 we used the positivity of the coefficients of R_n and we deduced that $R_n(a)$ was not 0 (this is the so-called "zero estimate" in transcendental number theory). Here we need another argument.

The last step of the proof of the irrationality of π is achieved by using two consecutive indices n and $n+1$. We eliminate e^z among the two relations

$$B_n(z)e^z - A_n(z) = R_n(z) \quad \text{and} \quad B_{n+1}(z)e^z - A_{n+1}(z) = R_{n+1}(z).$$

We deduce that the polynomial

$$\Delta_n = B_n A_{n+1} - B_{n+1} A_n \tag{1.30}$$

can be written

$$\Delta_n = -B_n R_{n+1} + B_{n+1} R_n. \tag{1.31}$$

As we have seen, the polynomial B_n is monic of degree n; the polynomial A_n also has degree n, its highest degree term is $(-1)^n z^n$. It follows from (1.30) that Δ_n is a polynomial of degree $2n+1$ and highest degree term $(-1)^n 2z^{2n+1}$. On the other hand since R_n has a zero of multiplicity at least $2n+1$, the relation (1.31) shows that it is the same for Δ_n. Consequently

$$\Delta_n(z) = (-1)^n 2z^{2n+1}.$$

We deduce that Δ_n does not vanish outside 0. From (1.31) we deduce that R_n and R_{n+1} have no common zero apart from 0. This completes the proof of the irrationality of π.

1.4.3 Hermite's integral formula for the remainder

For $h \geq 0$, the h-th derivative $D^h R(z)$ of the remainder in Proposition 2.9 is given by

$$D^h R(z) = \sum_{k \geq N+1} \frac{(k-n_0-1)!}{(k-N-1)!} \cdot \frac{z^{k-h}}{(k-h)!}.$$

In particular for $h = n_0 + 1$ the formula becomes

$$D^{n_0+1} R = \sum_{k \geq N+1} \frac{z^{k-n_0-1}}{(k-N-1)!} = z^{n_1} e^z. \tag{1.32}$$

This relations determines R since R has a zero of multiplicity $\geq n_0 + 1$ at the origin. When we restrict the operator of $D = d/dz$ to the functions vanishing at the origin, it has an inverse which is the operator J defined by

$$J(\varphi) = \int_0^z \varphi(t)dt.$$

Following [33], we can compute the iterates of J:

Lemma 1.33. *For $n \geq 0$,*

$$J^{n+1}\varphi = \frac{1}{n!}\int_0^z (z-t)^n \varphi(t)dt.$$

Proof. The formula is valid for $n = 0$. We first check it for $n = 1$. The derivative of the function

$$\int_0^z (z-t)\varphi(t)dt = z\int_0^z \varphi(t)dt - \int_0^z t\varphi(t)dt$$

is

$$\int_0^z \varphi(t)dt + z\varphi(z) - z\varphi(z) = \int_0^z \varphi(t)dt.$$

We now proceed by induction. The derivative of the function of z

$$\frac{1}{n!}\int_0^z (z-t)^n\varphi(t)dt = \sum_{k=0}^{n} \frac{(-1)^{n-k}}{k!(n-k)!}\cdot z^k \int_0^z t^{n-k}\varphi(t)dt$$

is

$$\sum_{k=0}^{n} \frac{(-1)^{n-k}}{k!(n-k)!}\left(kz^{k-1}\int_0^z t^{n-k}\varphi(t)dt + z^n\varphi(z)\right).$$

Since

$$\sum_{k=0}^{n} \frac{(-1)^{n-k}}{k!(n-k)!} = 0,$$

the right hand side is nothing else than

$$\sum_{k=1}^{n} \frac{(-1)^{n-k}}{(k-1)!(n-k)!}\cdot z^{k-1}\int_0^z t^{n-k}\varphi(t)dt = \frac{1}{(n-1)!}\int_0^z (z-t)^{n-1}\varphi(t)dt.$$

□

From (1.32) and 1.33 it plainly follows:

Lemma 1.34. *The remainder $R(z)$ in Hermite's fomula with parameters n_0 and n_1 is given by*

$$R(z) = \frac{1}{n_0!}\int_0^z (z-t)^{n_0} t^{n_1} e^t dt.$$

1.4.4 Hermite's identity

The next formula is one of the many disguises of Hermite's identity.

Lemma 1.35. *Let f be a polynomial of degree $\leq N$. Define*

$$F = f + Df + D^2 + \cdots + D^N f.$$

Then for $z \in \mathbb{C}$

$$\int_0^z e^{-t} f(t)dt = F(0) - e^{-z}F(z).$$

We can also write the definition of F as

$$F = (1-D)^{-1} f \quad \text{where} \quad (1-D)^{-1} = \sum_{k \geq 0} D^k.$$

The series in the right hand side is infinite, but when we apply the operator to a polynomial only finitely many $D^k f$ are not 0: when f is a polynomial of degree $\leq N$ then $D^k f = 0$ for $k > N$.

Proof. More generally, if f is a complex function which is analytic at the origin and N is a positive integer, if we set

$$F = f + Df + D^2 + \cdots + D^N f,$$

then the derivative of $e^{-t}F(t)$ is $-e^{-t}f(t) + e^{-t}D^{N+1}f(t)$. □

We shall come back to such formulae in section § 2.1.3.

2 Transcendence

2.1 Hermite's Method

In 1873 C. Hermite [17] proved that the number e is transcendental. In his paper he explains in a very clear way how he found his proof. He starts with an analogy between simultaneous diophantine approximation of real numbers on the one hand and analytic complex functions of one variable on the other. He first solves the analytic problem by constructing explicitly what is now called Padé approximants for the exponential function. In fact there are two types of such approximants, they are now called type I and type II, and what Hermite did in 1873 was to compute Padé approximants of type II. He also found those of type I in 1873 and studied them later in 1893. K. Mahler was the first in the mid's 1930 to relate the properties of the two types of Padé's approximants and to use those of type I in order to get a new proof of Hermite's transcendence Theorem (and also of the generalisation by Lindemann and Weierstraß as well as quantitative refinements). See [11] Chap. 2 § 3.

In the analogy with number theory, Padé approximants of type II are related with the simultaneous approximation of real numbers $\vartheta_1, \ldots, \vartheta_m$ by rational numbers p_i/q with the same denominator q (one does not require that the fractions are irreducible), which means that we wish to bound from below

$$\max_{1 \leq i \leq m} \left| \vartheta_i - \frac{p_i}{q} \right|$$

in terms of q, while type I is related with the study of lower bounds for linear combinations

$$|a_0 + a_1\vartheta_1 + \cdots + a_m\vartheta_m|$$

when $a_0, \ldots, a_m$ are rational integers, not all of which are 0, in terms of the number $\max_{0 \leq i \leq m} |a_i|$.

After Hermite's seminal work, F. Lindemann was able to extend the argument and to prove the transcendence of π (hence he solved the old greek problem of the quadrature of the circle: *it is not possible using ruler and compass to draw a square and a circle having the same area*). This extension led to the so-called Hermite-Lindemann's Theorem:

Theorem 2.1 (Hermite–Lindemann)**.** *Let α be a non zero complex algebraic number. Let $\log \alpha$ be any non-zero logarithm of α. Then $\log \alpha$ is transcendental.*

Equivalently, let β be a non-zero algebraic number. Then e^β is transcendental.

Recall that any non-zero complex number z has complex logarithms: these are the solutions $\ell \in \mathbb{C}$ of the equation $e^\ell = z$. If ℓ is one of them, then all solutions ℓ to this equation $e^\ell = z$ are $\ell + 2ik\pi$ with $k \in \mathbb{Z}$. The only non-zero complex of which 0 is a logarithm is 1.

The equivalence between both statements in Theorem 2.1 is easily seen by setting $e^\beta = \alpha$: one can phrase the result by saying that for any non-zero complex number β, one at least of the two numbers β, e^β is transcendental.

After the proofs by Hermite and Lindemann, a number of authors in the XIX-th century worked out variants of the argument. The main goal was apparently to get the shorter possible proof, and most often the reason for which it works is by no means so clear as in Hermite's original version. One can find in the literature such short proofs (see for instance [26]), the connexion with Hermite's arguments are most often not so transparent. So we shall come back to the origin and try to explain what is going on.

We concentrate now on Hermite's proof for the transcendence of e. The goal is to prove that for any positive integer m, the numbers $1, e, e^2, \ldots, e^m$ are linearly independent over $\mathbb{Q}$.

2.1.1 Criterion of linear independence

We first state a criterion for linear independence. This is a generalisation (from personal notes of Michel Laurent after a course he gave in Marseille) of one of the previous criteria for irrationality, namely Lemma 1.26. Most often in mathematics there is sort of an entropy: when a statement provides a necessary and sufficient condition, and when one of the two implication is easy while the other requires more work, then it is the difficult part which is most useful. Here we have a counterexample to this claim (which does not belong to mathematics but rather to social science): in the criterion 2.2 below, one of the implications is easy while the other is deeper; but it turns out that it is the easy one which is required in transcendence proofs. So we state the statement and prove the easy part now, we postpone the reverse to a later section where we introduce some tools from geometry of numbers and give further consequences of these tools.

Let $\vartheta_1, \ldots, \vartheta_m$ be real numbers and a_0, $a_1, \ldots, a_m$ rational integers, not all of which are 0. Our goal is to prove that the number

$$L = a_0 + a_1\vartheta_1 + \cdots + a_m\vartheta_m$$

is not 0.

The idea is to approximate simultaneously $\vartheta_1, \dots, \vartheta_m$ by rational numbers $p_1/q, \dots, p_m/q$ with the same denominator $q > 0$.

Let $q, p_1, \dots, p_m$ be rational integers with $q > 0$. For $1 \le k \le m$ set

$$\epsilon_k = q\vartheta_k - p_k.$$

Then $qL = M + R$ with

$$M = a_0 q + a_1 p_1 + \cdots + a_m p_m \in \mathbb{Z} \quad \text{and} \quad R = a_1\epsilon_1 + \cdots + a_m\epsilon_m \in \mathbb{R}.$$

If $M \neq 0$ and $|R| < 1$ we deduce $L \neq 0$.

One of the main difficulties is often to check $M \neq 0$. This question gives rise to the so-called *zero estimates* or *non-vanishing lemmas*. In the present situation, we wish to find a $m+1$–tuple $(q, p_1, \dots, p_m)$ giving a simultaneous rational approximation to $(\vartheta_1, \dots, \vartheta_m)$, but we also require that it lies outside the hyperplane $a_0x_0 + a_1x_1 + \cdots + a_mp_m = 0$ of $\mathbb{Q}^{m+1}$. Since this needs to be checked for all hyperplanes, the solution is to construct not only one tuple $(q, p_1, \dots, p_m)$ in $\mathbb{Z}^{m+1} \setminus \{0\}$, but $m+1$ such tuples which are linearly independent. This yields $m+1$ pairs (M_k, R_k), $k = 0, \dots, m$ in place of a single pair (M, R), and from $(a_0, \dots, a_m) \neq 0$ one deduces that one at least of $M_0, \dots, M_m$ is not 0.

It turns out that nothing is lossed by using such arguments: existence of linearly independent simultaneous rational approximations for $\vartheta_1, \dots, \vartheta_m$ are characteristic of linearly independent numbers $1, \vartheta_1, \dots, \vartheta_m$. As we just said earlier, we shall use only the easy part of the next lemma 2.2.

Lemma 2.2. *Let $\underline{\vartheta} = (\vartheta_1, \dots, \vartheta_m) \in \mathbb{R}^m$. Then the following conditions are equivalent.*
(i) The numbers $1, \vartheta_1, \dots, \vartheta_m$ are linearly independent over $\mathbb{Q}$.
(ii) For any $\epsilon > 0$ there exist $m+1$ linearly independent elements $\underline{b}_0, \underline{b}_1, \dots, \underline{b}_m$ in $\mathbb{Z}^{m+1}$, say

$$\underline{b}_i = (q_i, p_{1i}, \dots, p_{mi}), \quad (0 \le i \le m)$$

with $q_i > 0$, such that

$$\max_{1 \le k \le m} \left| \vartheta_k - \frac{p_{ki}}{q_i} \right| \le \frac{\epsilon}{q_i}, \quad (0 \le i \le m). \tag{2.3}$$

In (ii) there is no non-vanishing condition. For $m = 1$ this criterion is not identical to the irrationality criterion: in Lemma 1.11, we required for each ϵ one approximation p/q distinct from θ. Here we need two linearly independent approximations: hence, if θ is rational, one at least of them is not the trivial one.

The condition on linear independence of the elements $\underline{b}_0, \underline{b}_1, \dots, \underline{b}_m$ means that the determinant

$$\begin{vmatrix} q_0 & p_{10} & \cdots & p_{m0} \\ \vdots & \vdots & \ddots & \vdots \\ q_m & p_{1m} & \cdots & p_{mm} \end{vmatrix}$$

is not 0.

For $0 \le i \le m$, set

$$\underline{r}_i = \left(\frac{p_{1i}}{q_i}, \dots, \frac{p_{mi}}{q_i} \right) \in \mathbb{Q}^m.$$

Further define, for $\underline{x} = (x_1, \dots, x_m) \in \mathbb{R}^m$

$$|\underline{x}| = \max_{1 \le i \le m} |x_i|.$$

Also for $\underline{x} = (x_1, \dots, x_m) \in \mathbb{R}^m$ and $\underline{x} = (x_1, \dots, x_m) \in \mathbb{R}^m$ set

$$\underline{x} - \underline{y} = (x_1 - y_1, \dots, x_m - y_m),$$

so that

$$|\underline{x} - \underline{y}| = \max_{1 \le i \le m} |x_i - y_i|.$$

Then the relation (2.3) in Lemma 2.2 can be written

$$|\underline{\vartheta} - \underline{r}_i| \le \frac{\epsilon}{q_i}, \quad (0 \le i \le m).$$

We shall prove a more explicit version of (ii)⇒(i): we check that *any tuple* $(q, p_1, \dots, p_m) \in \mathbb{Z}^{m+1}$ *producing a tuple* $(p_1/q, \dots, p_m/q) \in \mathbb{Q}^m$ *of sufficiently good rational approximations to* $\underline{\vartheta}$ *satisfies the same linear dependence relations as* $1, \vartheta_1, \dots, \vartheta_m$.

Lemma 2.4. *Let* $\vartheta_1, \dots, \vartheta_m$ *be real numbers. Assume that the numbers* $1, \vartheta_1, \dots, \vartheta_m$ *are linearly dependent over* $\mathbb{Q}$*: let* $a, b_1, \dots, b_m$ *be rational integers, not all of which are zero, satisfying*

$$a + b_1\vartheta_1 + \cdots + b_m\vartheta_m = 0.$$

Let $\epsilon > 0$ *satisfy* $\sum_{k=1}^m |b_k] > 1/\epsilon$. *Assume further that* $(q, p_1, \dots, p_m) \in \mathbb{Z}^{m+1}$ *satisfies* $q > 0$ *and*

$$\max_{1 \le k \le m} |q\vartheta_k - p_k| \le \epsilon.$$

Then

$$aq + b_1p_1 + \cdots + b_mp_m = 0.$$

Proof. In the relation

$$qa + \sum_{k=1}^m b_kp_k = -\sum_{k=1}^m b_k(q\vartheta_k - p_k),$$

the right hand side has absolute value less than 1 and the left hand side is a rational integer, so it is 0.

□

Proof of (ii)⇒(i) in Lemma 2.2. By assumption (ii) we have $m+1$ linearly independent elements $\underline{b}_i \in \mathbb{Z}^{m+1}$ such that the corresponding rational approximation satisfy the assumptions of Lemma 2.4. For each non-zero linear form

$$aX_0 + b_1X_1 + \cdots + b_mX_m = 0$$

one at least of the $L(\underline{b}_i)$ is not 0. Hence

$$a + b_1\vartheta_1 + \cdots + b_m\vartheta_m \neq 0.$$

□

Proof of (i)⇒(ii) in Lemma 2.2. Let $\epsilon > 0$. Assume (i) holds. By Dirichlet's box principle (Lemma 1.7), there exists $\underline{b} = (q, p_1, \ldots, p_m) \in \mathbb{Z}^{m+1}$ with $q > 0$ such that

$$\max_{1\leq k\leq m} \left|\vartheta_k - \frac{p_k}{q}\right| \leq \frac{\epsilon}{q}.$$

Consider the subset $E_\epsilon \subset \mathbb{Z}^{m+1}$ of these tuples. We show that the $\mathbb{Q}$-vector subspace V_ϵ of $\mathbb{Q}^{m+1}$ spanned by E_ϵ is $\mathbb{Q}^{m+1}$. It will follow that there are $m+1$ linearly independent elements in E_ϵ.

If $V_\epsilon \neq \mathbb{Q}^{m+1}$, then there is a hyperplane $a_0z_0 + a_1z_1 + \cdots + a_mz_m = 0$ containing E_ϵ. Any $\underline{b} = (q, p_1, \ldots, p_m)$ in E_ϵ has

$$a_0q + a_1p_1 + \cdots + a_mp_m = 0.$$

For each $n \geq 1/\epsilon$, let $\underline{b} = (q_n, p_{1n}, \ldots, p_{mn}) \in E_\epsilon$ satisfy

$$\max_{1\leq k\leq m} \left|\vartheta_k - \frac{p_{kn}}{q_n}\right| \leq \frac{1}{nq_n}.$$

Then

$$-a_0 + a_1\theta_1 + \cdots + a_m\theta_m = \sum_{k=1}^{m} a_k\left(\theta_k - \frac{p_{kn}}{q_n}\right).$$

Hence

$$|-a_0 + a_1\theta_1 + \cdots + a_m\theta_m| \leq \frac{1}{nq_n}\sum_{k=1}^{m}|a_k|.$$

The right hand side tends to 0 as n tends to infinity, hence the left hand side vanishes, and $1, \vartheta_1, \ldots, \vartheta_m$ are $\mathbb{Q}$–linearly dependent, which contradicts (i).

□

2.1.2 Padé approximants

Henri Eugène Padé (1863–1953), who was a student of Charles Hermite (1822–1901), gave his name to the following objects.

Lemma 2.5. *Let $f_1, \dots, f_m$ be analytic functions of one complex variable near the origin. Let $n_0, n_1, \dots, n_m$ be non-negative integers. Set*

$$N = n_0 + n_1 + \cdots + n_m.$$

Then there exists a tuple $(Q, P_1, \dots, P_m)$ of polynomials in $\mathbb{C}[X]$ satisfying the following properties:
(i) The polynomial Q is not zero, it has degree $\leq N - n_0$.
(ii) For $1 \leq \mu \leq m$, the polynomial P_μ has degree $\leq N - n_\mu$.
(iii) For $1 \leq \mu \leq m$, the function $x \mapsto Q(x)f_\mu(x) - P_\mu(x)$ has a zero at the origin of multiplicity $\geq N + 1$.

Definition. *A tuple $(Q, P_1, \dots, P_m)$ of polynomials in $\mathbb{C}[X]$ satisfying the condition of Lemma 2.5 is called a* Padé system of the second type for $(f_1, \dots, f_m)$ attached to the parameters $n_0, n_1, \dots, n_m$.

Proof. The polynomial Q of Lemma 2.5 should have degree $\leq N - n_0$, so we have to find (or rather to prove the existence) its $N - n_0 + 1$ coefficients, not all being zero. We consider these coefficients as unknowns. The property we require is that for $1 \leq \mu \leq m$, the Taylor expansion at the origin of $Q(z)f_\mu(z)$ has zero coefficients for $z^{N-n_\mu+1}, z^{N-n_\mu+1}, \dots, z^N$. If this property holds for $1 \leq \mu \leq m$, we shall define P_μ by truncating the Taylor series at the origin of $Q(z)f_\mu(z)$ at the rank z^{N-n_μ}, hence P_μ will have degree $\leq N - n_\mu$, while the remainder $Q(z)f_\mu(z) - P_\mu(z)$ will have a mutiplicity $\geq N + 1$ at the origin.

Now for each given μ the condition we stated amounts to require that our unknowns (the coefficients of Q) satisfy n_μ homogeneous linear relations, namely

$$\left(\frac{d}{dx}\right)^k [Q(x)f_\mu(x)]_{x=0} = 0 \quad \text{for} \quad N - n_\mu < k \leq N.$$

Therefore altogether we get $n_1 + \cdots + n_m = N - n_0$ homogeneous linear equations, and since the number $N - n_0 + 1$ of unknowns (the coefficients of Q) is larger, linear algebra tells us that a non-trivial solution exists.

□

There is no unicity, because of the homogeneity of the problem: the set of solutions (together with the trivial solution 0) is a vector space over $\mathbb{C}$, and Lemma 2.5 tells us that it has positive dimension. In the case where this dimension is 1 (which means that there is unicity up to a multiplicative factor), the system of approximants is called *perfect*. An example is with $m = 1$ and $f(z) = e^z$, as shown by Hermite's work.

Exercise 2.6. Let $f_1, \dots, f_m$ be analytic functions of one complex variable near the origin. Let $d_0, d_1, \dots, d_m$ be non-negative integers. Set

$$M = d_0 + d_1 + \cdots + d_m + m.$$

a) Show that there exists a tuple $(A_0, \dots, A_m)$ of polynomials in $\mathbb{C}[X]$, not all of which are zero, where A_i has degree $\leq d_i$, such that the function

$$A_0 + A_1 f_1 + \cdots + A_m f_m$$

has a zero at the origin of multiplicity $\geq M$.
These are the Padé approximants of type I.
b) Give an explicit solution (A_0, A_1) in the case $m = 1$ and $f_1(z) = e^z$.

Most often it is not easy to find explicit solutions: we only know their existence. As we are going to show, Hermite succeeded to produce explicit solutions for the systems of Padé approximants of the functions $(e^x, e^{2x}, \ldots, e^{mx})$.

Exercise 2.7.

2.1.3 Hermite's identity

Let us come back to the problem which was considered in § 1.4.1 and solved by Hermite (Proposition 1.28):

Given two integers $n_0 \geq 0$, $n_1 \geq 0$, find two polynomials A and B with A of degree $\leq n_0$ and B of degree $\leq n_1$ such that the function $R(z) = B(z)e^z - A(z)$ has a zero at the origin of multiplicity $\geq N + 1$ with $N = n_0 + n_1$.

From § 1.4.3 one easily deduces that *there is a non-trivial solution, and it is unique if one requires B to be monic. Moreover B has degree n_1 and R has multiplicity exactly $N + 1$ at the origin.*

Indeed, since A has degree $\leq n_0$, the $(n_0 + 1)$-th derivative of R is

$$D^{n_0+1}R = D^{n_0+1}(B(z)e^z),$$

hence it is the product of e^z with a polynomial of the same degree as the degree of B and same leading coefficient. Now R has a zero at the origin of multiplicity $\geq n_0 + n_1 + 1$, hence $D^{n_0+1}R(z)$ has a zero of multiplicity $\geq n_1$ at the origin. Therefore $D^{n_0+1}R = cz^{n_1}e^z$ where c is the leading coefficient of B. Since $D^{n_0+1}R$ has a zero of multiplicity exactly n_1, it follows that R has a zero at the origin of multiplicity exactly $N + 1$. Finally R is the unique function satisfying $D^{n_0+1}R = cz^{n_1}e^z$ with a zero of multiplicity $\geq n_0$ at 0. According to Lemma 1.33, this implies that the unique solution R for which $c = 1$ is given by the formula of Lemma 1.34:

$$R(z) = \frac{1}{n_0!}\int_0^z (z-t)^{n_0}t^{n_1}e^t dt.$$

Hence Padé system for the exponential function is perfect.

Our goal is to generalize these results.

Let f be a polynomial. Hermite's Lemma 1.35 gives a formula for

$$\int_0^z e^{-t}f(t)dt$$

for $z \in \mathbb{C}$. A change of variables leads to a formula for

$$\int_0^u e^{-xt}f(t)dt$$

when x and u are complex numbers. Here, in place of using Lemma 1.35, we repeat the proof. Integrate by part $e^{-xt}f(t)$ between 0 and u:

$$\int_0^u e^{-xt}f(t)dt = -\left[\frac{1}{x}e^{-xt}f(t)\right]_0^u + \frac{1}{x}\int_0^u e^{-xt}f'(t)dt.$$

By induction we deduce

$$\int_0^u e^{-xt}f(t)dt = -\sum_{k=0}^{m}\left[\frac{1}{x^{k+1}}e^{-xt}D^kf(t)\right]_0^u + \frac{1}{x^{m+1}}\int_0^u e^{-xt}D^{m+1}f(t)dt.$$

Let N be an upper bound for the degree of f. For $m = N$ the last integral vanishes and

$$\begin{aligned}\int_0^u e^{-xt}f(t)dt &= -\sum_{k=0}^{N}\left[\frac{1}{x^{k+1}}e^{-xt}D^kf(t)\right]_0^u \\ &= \sum_{k=0}^{N}\frac{1}{x^{k+1}}D^kf(0) - e^{-xu}\sum_{k=0}^{N}\frac{1}{x^{k+1}}D^kf(u).\end{aligned}$$

Multipling by $x^{N+1}e^{ux}$ yields:

Lemma 2.8. *Let f be a polynomial of degree $\leq N$ and let x, u be complex numbers. Then*

$$e^{xu}\sum_{k=0}^{N}x^{N-k}D^kf(0) = \sum_{k=0}^{N}x^{N-k}D^kf(u) + x^{N+1}e^{xu}\int_0^u e^{-xt}f(t)dt.$$

With the notation of Lemma 2.8, the function

$$x \mapsto \int_0^u e^{-xt}f(t)dt$$

is analytic at $x = 0$, hence its product with x^{N+1} has a mutiplicity $\geq N+1$ at the origin. Moreover

$$Q(x) = \sum_{k=0}^{N}x^{N-k}D^kf(0) \quad \text{and} \quad P(x) = \sum_{k=0}^{N}x^{N-k}D^kf(u)$$

are polynomials in x.

If the polynomial f has a zero of multiplicity $\geq n_0$ at the origin, then Q has degree $\leq N - n_0$. If the polynomial f has a zero of multiplicity $\geq n_1$ at u, then P has degree $\leq N - n_1$.

For instance in the case $u = 1$, $N = n_0 + n_1$, $f(t) = t^{n_0}(t-1)^{n_1}$, the two polynomials

$$Q(x) = \sum_{k=n_0}^{N}x^{N-k}D^kf(0) \quad \text{and} \quad P(x) = \sum_{k=n_1}^{N}x^{N-k}D^kf(1)$$

satisfy the properties which were required in section §1.4.1 (see Proposition 1.28), namely $R(z) = Q(z)e^z - P(z)$ has a zero of multiplicity $> n_0 + n_1$ at the origin, P has degree $\leq n_0$ and Q has degree $\leq n_1$.

Lemma 2.8 is a powerful tool to go much further.

Proposition 2.9. *Let m be a positive integer, $n_0, \ldots, n_m$ be non-negative integers. Set $N = n_0 + \cdots + n_m$. Define the polynomial $f \in \mathbb{Z}[t]$ of degree N by*

$$f(t) = t^{n_0}(t-1)^{n_1} \cdots (t-m)^{n_m}.$$

Further set, for $1 \leq \mu \leq m$,

$$Q(x) = \sum_{k=n_0}^{N} x^{N-k} D^k f(0), \quad P_\mu(x) = \sum_{k=n_\mu}^{N} x^{N-k} D^k f(\mu)$$

and

$$R_\mu(x) = x^{N+1} e^{x\mu} \int_0^\mu e^{-xt} f(t) dt.$$

Then the polynomial Q has exact degree $N - n_0$, while P_μ has exact degree $N - n_\mu$, and R_μ is an analytic function having at the origin a multiplicity $\geq N + 1$. Further, for $1 \leq \mu \leq m$,

$$Q(x)e^{\mu x} - P_\mu(x) = R_\mu(x).$$

Hence $(Q, P_1, \ldots, P_m)$ is a Padé system of the second type for the m-tuple of functions $(e^x, e^{2x}, \ldots, e^{mx})$, attached to the parameters $n_0, n_1, \ldots, n_m$. Furthermore, the polynomials $(1/n_0!)Q$ and $(1/n_\mu!)P_\mu$ for $1 \leq \mu \leq m$ have integral coefficients.

These polynomials $Q, P_1, \ldots, P_m$ are called the *Hermite-Padé polynomials attached to the parameters $n_0, n_1, \ldots, n_m$*.

Proof. The coefficient of x^{N-n_0} in the polynomial Q is $D^{n_0} f(0)$, so it is not zero since f has mutiplicity exactly n_0 at the origin. Similarly for $1 \leq \mu \leq m$ the coefficient of x^{N-n_μ} in P_μ is $D^{n_0} f(\mu) \neq 0$.

The assertion on the integrality of the coefficients follows from the next lemma.

Lemma 2.10. *Let f be a polynomial with integer coefficients and let k be a non-negative integer. Then the polynomial $(1/k!)D^k f$ has integer coefficients.*

Proof. If $f(X) = \sum_{n \geq 0} a_n X^n$ then

$$\frac{1}{k!} D^k f = \sum_{n \geq 0} a_n \binom{n}{k} X^n \quad \text{with} \quad \binom{n}{k} = \frac{n!}{k!(n-k)!},$$

and the binomial coefficients are rational integers. □

From Lemma 2.10 it follows that for any polynomial $f \in \mathbb{Z}[X]$ and for any integers k and n with $n \geq k$, the polynomial $(1/k!)D^n f$ also belongs to $\mathbb{Z}[X]$. This completes the proof of Proposition 2.9.

□

In order to complete the proof of the transcendence of e, we shall substitute 1 to x in the relations

$$Q(x)e^{\mu x} = P_\mu(x) + R_\mu(x)$$

and deduce simultaneous rational approximations $(p_1/q, p_2/q, \ldots, p_m/q)$ to the numbers $e, e^2, \ldots, e^m$. In order to use Lemma 2.2, we need to have independent such approximations. This is a subtle point which Hermite did not find easy to overcome, according to his owns comments in [17]. The following approach is due to K. Mahler, we can view it as an extension of the simple non-vanishing argument used in § 1.4.2 for the irrationality of π.

We fix integers $n_0, \ldots, n_1$, all ≥ 1. For $j = 0, 1, \ldots, m$ we denote by $Q_j, P_{j1}, \ldots, P_{jm}$ the Hermite-Padé polynomials attached to the parameters

$$n_0 - \delta_{j0}, n_1 - \delta_{j1}, \ldots, n_m - \delta_{jm},$$

where δ_{ji} is Kronecker's symbol

$$\delta_{ji} = \begin{cases} 1 & \text{if } j = i, \\ 0 & \text{if } j \neq i. \end{cases}$$

These parameters are said to be *contiguous* to $n_0, n_1, \ldots, n_m$. They are the rows of the matrix

$$\begin{pmatrix} n_0 - 1 & n_1 & n_2 & \cdots & n_m \\ n_0 & n_1 - 1 & n_2 & \cdots & n_m \\ \vdots & \vdots & \ddots & \vdots & \\ n_0 & n_1 & n_2 & \cdots & n_m - 1 \end{pmatrix}.$$

Proposition 2.11. *There exists a non-zero constant c such that the determinant*

$$\Delta(x) = \begin{vmatrix} Q_0 & P_{10} & \cdots & P_{m0} \\ \vdots & \vdots & \ddots & \vdots \\ Q_m & P_{1m} & \cdots & P_{mm} \end{vmatrix}$$

is the monomial cx^{mN}.

Proof. The matrix of degrees of the entries in the determinant defining Δ is

$$\begin{pmatrix} N - n_0 & N - n_1 - 1 & \cdots & N - n_m - 1 \\ N - n_0 - 1 & N - n_1 & \cdots & N - n_m - 1 \\ \vdots & \vdots & \ddots & \vdots \\ N - n_0 - 1 & N - n_1 - 1 & \cdots & N - n_m \end{pmatrix}.$$

Therefore Δ is a polynomial of exact degree $N-n_0+N-n_1+\cdots+N-n_m = mN$, the leading coefficient arising from the diagonal. This leading coefficient is $c = c_0c_1\cdots c_m$, where c_0 is the leading coefficient of Q_0 and c_μ is the leading coefficient of $P_{\mu\mu}$, $1 \le \mu \le m$.

It remains to check that Δ has a multiplicity at least mN at the origin. Linear combinations of the columns yield

$$\Delta(x) = \begin{vmatrix} Q_0 & P_{10} - e^x Q_0 & \cdots & P_{m0} - e^{mx} Q_0 \\ \vdots & \vdots & \ddots & \vdots \\ Q_m & P_{1m} - e^x Q_m & \cdots & P_{mm} - e^{mx} Q_m \end{vmatrix}.$$

Each $P_{\mu j} - e^{\mu x} Q_j$, $1 \le \mu \le m$, $0 \le j \le m$, has multiplicity at least N at the origin, because for each contiguous triple ($1 \le j \le m$) we have

$$\sum_{i=0}^{m} (n_i - \delta_{ji}) = n_0 + n_1 + \cdots + n_m - 1 = N - 1.$$

Looking at the multiplicity at the origin, we can write

$$\Delta(x) = \begin{vmatrix} Q_0 & \mathcal{O}(x^N) & \cdots & \mathcal{O}(x^N) \\ \vdots & \vdots & \ddots & \vdots \\ Q_m & \mathcal{O}(x^N) & \cdots & \mathcal{O}(x^N) \end{vmatrix}.$$

This completes the proof of Proposition 2.11. □

Now we fix a sufficiently large integer n and we use the previous results for $n_0 = n_1 = \cdots = n_m = n$ with $N = (m+1)n$. We define, for $0 \le j \le m$, the integers $q_j, p_{1j}, \ldots, p_{nj}$ by

$$n! q_j = Q_j(1),\ n! p_{\mu j} = P_{\mu j}(1), \quad (1 \le \mu \le m).$$

Proposition 2.12. *There exists a constant $\kappa > 0$ independent on n such that for $1 \le \mu \le m$ and $0 \le j \le m$,*

$$|q_i e^\mu - p_{\mu j}| \le \frac{\kappa^n}{n!}.$$

Further, the determinant

$$\begin{vmatrix} q_0 & p_{10} & \cdots & p_{m0} \\ \vdots & \vdots & \ddots & \vdots \\ q_m & p_{1m} & \cdots & p_{mm} \end{vmatrix}$$

is not zero.

Proof. Recall Hermite's formulae in Proposition 2.9:

$$Q_j(x)e^{\mu x} - P_{\mu j}(X) = x^{mn} e^{\mu x} \int_0^\mu e^{-xt} f_j(t)\,dt, \quad (1 \le \mu \le m,\ 0 \le j \le m),$$

where

$$f_j(t) = (t-j)^{-1}\big(t(t-1)\cdots(t-m)\big)^n$$
$$= (t-j)^{n-1}\prod_{\substack{1\le i\le m\\ i\neq j}}(t-i)^n.$$

We substitute 1 to x and we divide by $n!$:

$$q_j e^\mu - p_{\mu j} = \frac{1}{n!}\big(Q_j(1)e^\mu - P_{\mu j}(1)\big) = \frac{e^\mu}{n!}\int_0^\mu e^{-t}f_j(t)dt.$$

Now the integral is bounded from above by

$$\int_0^\mu e^{-t}|f_j(t)|dt \le m\sup_{0\le t\le m}|f_j(t)| \le m^{1+(m+1)n}.$$

Finally the determinant in the statement of Proposition 2.12 is $\Delta(1)/n!^{m+1}$, where Δ is the determinant of Proposition 2.11. Hence it does not vanish since $\Delta(1)\neq 0$.

□

Since $\kappa^n/n!$ tends to 0 as n tends to infinity, we may apply the criterion for linear independence Lemma 2.2. Therefore the numbers $1, e, e^2, \ldots, e^m$ are linearly independent, and since this is true for all integers m, Hermite's Theorem on the transcendence of e follows.

Exercise 2.13. Using Hermite's method as explained in § 2.1, prove that for any non-zero $r \in \mathbb{Q}(i)$, the number e^r is transcendental.

Exercise 2.14. Let m be a positive integer and $\epsilon > 0$ a real number. Show that there exists $q_0 > 0$ such that, for any $q \ge q_0$ and for any tuple $(q, p_1, \ldots, p_m)$ of rational integers with $q > q_0$,

$$\max_{1\le\mu\le m}\left|e^\mu - \frac{p_\mu}{q}\right| \ge \frac{1}{q^{1+(1/m)+\epsilon}}.$$

Is it possible to improve the exponent by replacing $1+(1/m)$ with a smaller number?

`Hint.` Consider Hermite's proof of the transcendence of e (§ 2.1.3), especially Proposition 2.12. First check (for instance using Cauchy's formulae)

$$\max_{0\le j\le m}\frac{1}{k!}|D^k f_j(\mu)| \le c_1^n,$$

where c_1 is a positive real number which does not depend on n. Next, check that the numbers p_j and $q_{\mu j}$ satisfy

$$\max\{q_j, |p_{\mu j}|\} \le (n!)^m c_2^m$$

for $1 \le \mu \le m$ and $0 \le j \le n$, where again $c_2 > 0$ does not depend on n.
Then repeat the proof of Hermite in § 2.1 with n satisfying

$$(n!)^m c_3^{-2mn} \le q < \big((n+1)!\big)^m c_3^{-2m(n+1)},$$

where $c_3 > 0$ is a suitable constant independent on n. One does not need to compute c_1, c_2 and c_3 in terms of m, one only needs to show their existence so that the proof yields the desired estimate.

2.2 Transcendental numbers: historical survey

We already stated Hermite's Theorem on the transcendence of e, Lindemann's Theorem on the transcendence of π and Hermite-Lindemann's Theorem on the transcendence of $\log \alpha$ and e^β for non-zero algebraic numbers α and β (with the proviso $\log \alpha \neq 0$) – see Theorem 2.1. We complete the history of the theory in the XIX-th century, and then discuss the development in the XX-th century.

References are [12] and [11].

2.2.1 Transcendental numbers before 1900: Liouville, Hermite, Lindemann, Weierstraß

The next corollary of Lemma 1.19 was proved by J. Liouville in 1844: this his how he constructed the first examples of transcendental numbers. His first explicit examples were given by continued fractions, next he gave further examples with series like

$$\theta_a = \sum_{n \ge 0} a^{-n!} \tag{2.15}$$

for any integer $a \ge 2$.

Lemma 2.16. *For any algebraic number α, there exist two constants c and d such that, for any rational number $p/q \neq \alpha$,*

$$\left|\alpha - \frac{p}{q}\right| \ge \frac{c}{q^d}.$$

It follows also from Lemma 1.19 that in Lemma 2.16, one can take for d the degree of α (that is the degree of the minimal polynomial of α).

Exercise 2.17. Denote by $P \in \mathbb{Z}[X]$ the minimal polynomial of α.
a) Prove this result with d the degree of P and κ given by

$$\kappa = \max\big\{1\ ;\ \max_{|t-\alpha|\le 1} |P'(t)|\big\}.$$

b) Check also that the same estimate is true with again d the degree of P and κ given by

$$\kappa = a_0 \prod_{i=2}^{d} (|\alpha_j - \alpha| + 1),$$

where a_0 is the leading coefficient and $\alpha_1, \dots, \alpha_d$ the roots of P with $\alpha_1 = \alpha$:

$$P(X) = a_0(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_d).$$

`Hint:` *For both parts of this exercise one may distinguish two cases, whether* $|\alpha - (p/q)|$ *is* ≥ 1 *or* < 1.

Definition. *A real number* θ *is a* Liouville number *if for any* $\kappa > 0$ *there exists* $p/q \in \mathbb{Q}$ *with* $q \geq 2$ *and*

$$0 < \left|\alpha - \frac{p}{q}\right| \leq \frac{c}{q^\kappa}.$$

It follows from Lemma 2.16 that Liouville numbers are transcendental. In dynamical systems one says that an irrational real number *satisfies a Diophantine condition* if is not Liouville: this means that there exists a constant $\kappa > 0$ such that, for any $p/q \in \mathbb{Q}$ with sufficiently large q,

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^\kappa}.$$

Let us check that the numbers (2.15) are Liouville numbers: let $a \geq 2$ be an integer and $\kappa > 0$ a real number. For sufficiently large N, set

$$q = a^{N!}, \quad p = \sum_{n=0}^{N} a^{N!-n!}.$$

Then we have

$$0 < \theta_a - \frac{p}{q} = \sum_{k \geq 1} \frac{1}{a^{(N+k)!-N!}}.$$

For $k \geq 1$ we use the crude estimate

$$(N+k)! - N! \geq N!N(N+1) \cdot (N+k-1) \geq N!\big(N + (k-1)!\big),$$

which yields

$$0 < \theta_a - \frac{p}{q} \leq \frac{e}{q^N}.$$

We shall discuss the development of this topic in the next subsection.

After the contributions of Ch. Hermite in 1873, F. Lindemann in 1882 and the Theorem of Hermite Lindemann 2.1, K. Weierstraß completed in 1888 the proof of a claim by Lindemann:

Theorem 2.18 (Lindemann–Weierstraß – first form)**.** *Let* $\alpha_1, \dots, \alpha_m$ *be algebraic numbers which are pairwise distinct:* $\alpha_i \neq \alpha_j$ *for* $i \neq j$*. Then the numbers* $e^{\alpha_1}, \dots, e^{\alpha_m}$ *are linearly independent over* $\mathbb{Q}$*.*

It is easy to checked that Theorem 2.18 is equivalent to the next statement:

Theorem 2.19 (Lindemann–Weierstraß – second form)**.** *Let* $\beta_1, \dots, \beta_n$ *be algebraic numbers which are linearly independent over* $\mathbb{Q}$*. Then the numbers* $e^{\beta_1}, \dots, e^{\beta_n}$ *are algebraically independent over* $\mathbb{Q}$*.*

Now the algebraic independence of complex numbers over $\mathbb{Q}$ is equivalent to the algebraic independence over the field $\overline{\mathbb{Q}}$ of algebraic numbers. Therefore Theorem 2.18 is also equivalent to the next statement:

Theorem 2.20 (Lindemann–Weierstraß – third form)**.** *Let $\alpha_1, \ldots, \alpha_m$ be algebraic numbers which are pairwise distinct. Then the numbers $e^{\alpha_1}, \ldots, e^{\alpha_m}$ are linearly independent over $\overline{\mathbb{Q}}$.*

This does not cover all the history of transcendental numbers in the XIX-th Century. In particular the work of Cantor is another main contribution which gave rise to many development in the XX-th Century.

2.2.2 Diophantine approximation and applications

Diophantine approximation is the study of the approximation of real or complex numbers by rational or algebraic numbers. It has its early sources in astronomy, with the study of movement of the celestials bodies, and in the computations of π.

The number π occurs more or less explicitly in a number of ancient documents from different civilisations. In the Bible there is an implicit value 3. The Rhind Papyrus around 2000 BC gives an approximate value $2^8/3^4 = 3.1604\ldots$

In the early times in India, ancient Hindu and Jaina mathematicians considered this question. Sometimes between the 8th and the 4th century, the Indian sacred texts Sulvasūtras from Baudhāyana give $3,088$. Also in India, around 500 BC, Suryaprajnapati (a Jaina mathematician) gives $\sqrt{10} = 3.162\ldots$

The value of π was studied in ancient Greece (especially by Archimedes around 2500 BC), also in China where the approximation $355/113 = 3.1415929\ldots$ was known. In the Vth Century AC Aryabhaṭīya, Āryabhaṭa I had the approximation 3.1416 and he suggested that π might be irrational. One century later Bhāskara I suggests a negative solution to the problem of squaring the circle. In the XIIth century Bhāskarācārya (Bhāskara II) has the approximation $3927/1250 = 3.1416$.

It is remarkable that Madhava (1380–1420) knew a series which gave him 11 exact decimals 3.14159265359 (while Viète in 1579 had 9 decimals only). A number of other mathematicians in Europa studied this question (including Leibniz and Gregory).

Getting sharp rational approximations is now easy using the continued fraction expansion of $\pi = 3.1415926535898\ldots$ which starts with

$$\pi = [3;\ 7,\ 15,\ 1,\ 292,\ 1,\ 1,\ 1,\ 2,\ 1,\ 3,\ 1,\ 14,\ 2,\ 1,\ 1\ldots]$$

The sequence of rational approximations we get by truncating this expansion is

$$3,\ \frac{22}{7},\ \frac{333}{106},\ \frac{355}{113},\ \ldots$$

Computation of billions of decimals of π have been performed: it serves as a test for computers, and produces also good candidates for random sequences, even if proofs are not available that such sequences satisfy the required properties.

Another type of approximation for π is due to Ramanujan:

$$\frac{63}{25}\left(\frac{17+15\sqrt{5}}{7+15\sqrt{5}}\right) = 3.141\,592\,653\quad 805\ldots$$

which is a root of $P(x) = 168\,125\,x^2 - 792\,225x + 829\,521$. Of course we know from Lindemann's Theorem that such estimate will not produce an exact value, since

$$\pi = 3.141\,592\,653\ \ 589\ldots$$

is not root of a polynomial with integer coefficients.

One recent (1997) formula for π produces efficiently its digits in base 16:

$$\pi = \sum_{n\geq 0}\left(\frac{4}{8n+1} - \frac{2}{8n+4} - \frac{1}{8n+5} - \frac{1}{8n+6}\right)2^{-4n}.$$

For computing a number with a sharp accuracy, one wishes to get many decimals (or binary digits) with a number of operations as small as possible. As we have seen for Diophantine questions, the cost is measured by the denominator q: one investigates how well ξ can be approximated in terms of q. So the notion of *complexity* is very different in these two points of view.

Diophantine approximation occurs in many different disguises (a very good reference here is [30]). It plays a crucial role in the question of small divisors and dynamical systems, introduced by H. Poincaré. See in particular [40]. In the study of the periods of Saturn orbits (Cassini divisions), Diophantine approximation is also there. It plays a role in the question of the stability of the solar system, in resonance in astronomy, in the problems of engrenages, in quasi-cristals, in the acoustic of concert halls, in calendars (bissextile years).

We give now an example of application of the question of rational approximations to $\log_2 3$ to musical scales.

The successive harmonics of a note of frequency n are the vibrations with frequencies $2n$, $3n$, $4n$, $5n$, ... with decreasing intensity. The successive octaves of a note of frequency n are vibrations with frequencies $2n$, $4n$, $8n$, $16n\ldots$

Using octaves, one replaces each note by a note with frequency in a given interval, say $[n, 2n)$. The classical choice in Hertz is $[264, 528)$. For simplicity we take rather $[1, 2)$. Hence a note with frequency f is replaced by a note with frequency r with $1 \leq r < 2$, where

$$f = 2^a r, \qquad a = [\log_2 f] \in \mathbb{Z}, \quad r = 2^{\{\log_2 f\}} \in [1, 2).$$

For instance a note with frequency 3 (which is a harmonic of 1) is at the octave of a note with frequency $3/2$. The musical interval $[1, 3/2]$ is called *fifth*, the ratio of the endpoints of the interval is $3/2$.

The musical interval $[3/2, 2]$ is *the fourth*, with ratio $4/3$.

The successive fifths are the notes in the interval $[1, 2]$, which are at the octave of notes with frequency

$$1,\ 3,\ 9,\ 27,\ 81\ldots$$

namely:

$$1,\ 3/2,\ 9/8,\ 27/16,\ 81/64\ldots$$

We shall never come back to the initial value 1, since the Diophantine equation $3^a = 2^b$ has no solution in positive integers a, b. We cannot solve exactly the equation $2^a = 3^b$ in positive rational integers a and b, but we can look for powers of 2 which are close to powers of 3.

There are just three solutions to the equation $3^x - 2^y = \pm 1$ in positive integers x and y, namely $3 - 2 = 1$, $4 - 3 = 1$ and $9 - 8 = 1$. This question leads to the study of so-called *exponential Diophantine equations*, which include the Catalan's equation $x^p - y^q = 1$ where x,y, p and q are unknowns in $\mathbb{Z}$ all ≥ 2 (this was solved recently, the only solution is $3^2 - 2^3 = 1$, as suggested in 1844 by E. Catalan, the same year when Liouville produced the first examples of transcendental numbers). A generalisation of this question is a conjecture of Pillai, according to which *for any fixed positive $k \in \mathbb{Z}$ there are only finitely many x,y, p and q in $\mathbb{Z}$, all ≥ 2, with $x^p - y^q = k$.* It is easy to check that Pillai's conjecture is equivalent to the fact that *in the increasing sequence $(u_n)_{n\geq 1}$ of* perfect powers (namely integers of the form a^b with $a \geq 1$ and $b \geq 2$), *the difference between two consecutive terms $u_{n+1} - u_n$ tends to infinity.*

Instead of looking at Diophantine equations, one can consider rather the question of approximating 3^a by 2^b from another point of view. The fact that the equation $3^a = 2^b$ has no solution in positive integers a, b means that the logarithm in basis 2 of 3:

$$\log_2 3 = (\log 3)/\log 2 = 1.58496250072\ldots,$$

which is the solution x of the equation $2^x = 3$, is irrational. Powers of 2 which are close to powers of 3 correspond to rational approximations a/b to $\log_2 3$:

$$\log_2 3 \simeq a/b, \qquad 2^a \simeq 3^b.$$

Hence it is natural to consider the continued fraction expansion

$$\log_2 3 = [1; 1, 1, 2, 2, 3, 1, 5,\ \ldots]$$

The first approximations we obtain by truncating this expansion are

$$[1] = 1,\ [1;1] = 2,\ [1;1,1] = \frac{3}{2},\ [1;1,1,2] = \frac{8}{5} = 1.6.$$

This last approximation suggest to consider $a = 3$ and $b = 5$:

$$2^8 = 256 \quad \text{is not too far from} \quad 3^5 = 243.$$

The approximation of $(3/2)^5 = 7.593\ldots$ by 2^3 means that 5 *fifths produces almost to* 3 *octaves.*

The next approximation is

$$[1;1,1,2,2] = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{2}}}} = \frac{19}{12} = 1.5833\ldots$$

It is related to the fact that 2^{19} is close to 3^{12}:

$$2^{19} = 524\,288 \simeq 3^{12} = 531\,441, \quad (3/2)^{12} = 129.74\ldots \text{ is close to } 2^7 = 128.$$

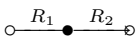
In music it means that *twelve fifths is a bit more than seven octaves.* The *comma of Pythagoras* is $3^{12}/2^{19} = 1,01364$. It produces an error of about 1.36%, which most people cannot ear.

A further remarkable Diophantine approximation is

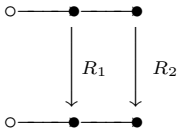
$$5^3 = 125 \simeq 2^7 = 128, \quad (5/4)^3 = 1.953 \simeq 2.$$

meaning that *three thirds* (ratio 5/4) *produce almost one octave.* This approximation can be written $2^{10} = 1024 \simeq 10^3$. It plays an important role in computers (kilo octets), of course, but also in acoustic: multiplying the intensity of a sound by 10 means adding 10 decibels. Multiplying the intensity by k, amounts to add d decibels with $10^d = k^{10}$. Since $2^{10} \simeq 10^3$, doubling the intensity, is close to adding 3 decibels.

A further example of application of continued fractions given in [30] deals with *electric networks.* The resistance of a network in series



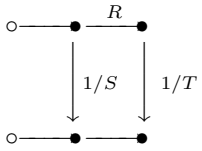
is the sum $R_1 + R_2$. The resistance R of the parallel network



satisfies

$$\frac{1}{R} = \frac{1}{R_1} + \frac{1}{R_2}.$$

The resistance U of the circuit



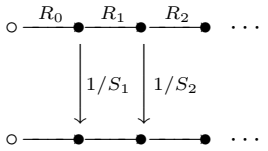
is given by

$$U = \cfrac{1}{S + \cfrac{1}{R + \cfrac{1}{T}}}.$$

The resistance of the following network is given by a continued fraction

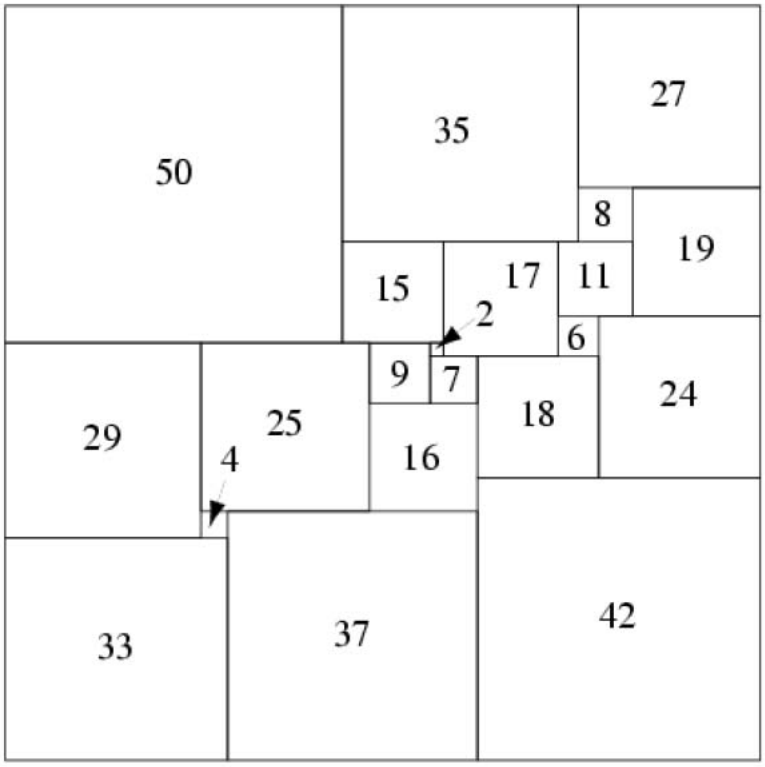
$$[R_0; S_1, R_1, S_2, R_2 \ldots]$$

for the circuit



For instance when $R_i = S_j = 1$ we get the quotients of consecutive Fibonacci numbers.

This fact provides a connexion between electric networks, and continued fractions, it has a surprising consequence on the problem of *decomposition of a square into squares* (squaring the square!): electric networks and continued fractions were used to find the first solution to the problem of decomposing a geometric integer square into distinct integer squares.



21-*square perfect square*

There is a unique simple perfect square of order 21 (the lowest possible order), discovered in 1978 by A. J. W. Duijvestijn (Bouwkamp and Duijvestijn 1992). It is composed of 21 squares with total side length 112, and is illustrated above.

We conclude this list of applications of Diophantine questions with a connexion between a problem raised by K. Mahler in 1967 and theoretical computer science.

Mahler notices that an integer power of e is never an integer, since e is transcendental. He asks whether there exists an absolute constant $c > 0$ such that, for a and b positive integers,

$$|e^b - a| > a^{-c}?$$

This is not yet solved. Mahler's conjecture arises by considering the numbers $\log a - b_a$ for $a = 1, \ldots, A$, where b_a is the nearest integer to $\log a$, for growing values of A, and assuming that these numbers are evenly distributed in the interval $(-1/2, 1/2)$. Instead we could consider the numbers $e^b - a_b$ for $b = 1, \ldots, B$, where a_b is the nearest integer to e^b , for growing values of B, and assume that these numbers are evenly distributed in the interval $(-1/2, 1/2)$. For this reason I suggested that Mahler's conjecture may not be the best possible estimate and that the following stronger estimate would be valid:

$$|e^b - a| > b^{-c}.$$

But this is not true, as pointed out to me by Iam Ho on September 27, 2007: if a denotes the integral part of e^b, then we have

$$0 < e^b - a < 1, \qquad 0 < a(b - \log a) < e^b - a < e^b(b - \log a),$$

hence

$$0 < b - \log a < \frac{e^b - a}{a} < \frac{1}{a}\cdot$$

The question of a lower bound for $|e^b - a|$ was considered first by K. Mahler (1953, 1967), then by M. Mignotte (1974), and more recently by F. Wielonsky (1997). The sharpest known estimate on Mahler's problem is

$$|e^b - a| > b^{-20b}.$$

In a joint work with Yu.V. Nesterenko [25] in 1996, we considered an extension of this question when a and b are rational numbers. A refinement of our estimate has been obtained by S. Khemira in 2005 and is currently being sharpened in a joint work of S. Khemira and P. Voutier.

Define $H(p/q) = \max\{|p|,\, q\}$. Then for a and b in $\mathbb{Q}$ with $b \neq 0$, the estimate is

$$|e^b - a| \geq \exp\{-1, 3 \cdot 10^5 (\log A)(\log B)\}$$

where $A = \max\{H(a),\ A_0\}$, $B = \max\{H(b),\ 2\}$. The numerical value of the absolute constant A_0 will be explicitly computed.

There is a connexion with the question of *exact rounding of the elementary functions* in theoretical computer science. A reference to the *Arénaire project in Computer Arithmetic* is
http://www.ens-lyon.fr/LIP/Arenaire/

This team works on validated scientific computing: arithmetic. reliability, accuracy, and speed. Their goal is to improve the available arithmetic on computers, processors, dedicated or embedded chips, and they want to achieve more accurate results or getting them more quickly. This has implication in power consumption as well as reliability of numerical software.

Further applications of Diophantine Approximation include (see [18]): equidistribution modulo 1, discrepancy, numerical integration, interpolation, approximate solutions to integral and differential equations.

2.2.3 Diophantine approximation and Diophantine Equations

There are deep connexions between diophantine approximation and Diophantine equations. In this section we show how continued fractions expansions are used for solving the equation:

$$x^2 - dy^2 = \pm 1 \tag{2.21}$$

(where the unknowns x, y are in $\mathbb{Z}$) which is named Pell's equation. Later we shall consider other examples.

There is a natural ordering among the solutions, by increasing x (or y, it amounts to the same). Since we are looking at positive solutions there is a smallest one, called the *fundamental solution*, say (x_1, y_1).

From $x_1^2 - dy_1^2 = \pm 1$ it readily follows that the sequence of pairs of integers (x_n, y_n) defined by

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$$

satisfies also $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$ hence

$$x_n^2 - dy_n^2 = \pm 1.$$

If the fundamental solution has $x_1^2 - dy_1^2 = 1$, then all x_n, y_n also have $x_n^2 - dy_n^2 = 1$, while if $x_1^2 - dy_1^2 = -1$, then for all n we have $x_n^2 - dy_n^2 = (-1)^n$. In the second case (x_2, y_2) is the fundamental solution of the equation $x_1^2 - dy_1^2 = 1$.

Let us check that all solutions of the Pell's equation are the (x_n, y_n) with $n \geq 0$ (with $n = 0$ giving the trivial solution $(1, 0)$). Consider the following subset of $\mathbb{R}^2$:

$$G = \left\{ (\log|x + y\sqrt{d}|, \log|x - y\sqrt{d}|) \ ; \ (x, y) \in \mathbb{Z}^2, \ x^2 - dy^2 = \pm 1 \right\}.$$

It is easily checked that G is an additive subgroup of $\mathbb{R}^2$. This is due to the fact that the equation $x^2 - dy^2 = \pm 1$ can be written $(x + \sqrt{d}y)(x - \sqrt{d}y) = \pm 1$, hence the solutions (x, y) form a multiplicative group with the law given by

$$(x + y\sqrt{d})(x' + y'\sqrt{d}) = xx' + dyy' + (xy' + x'y)\sqrt{d},$$

corresponding to the identity

$$(xx' + dyy')^2 - d(xy' + x'y)^2 = (x^2 - dy^2)(x'^2 - dy'^2).$$

Now G is *discrete* in $\mathbb{R}^2$: any compact subset of $\mathbb{R}^2$ contains only finitely many elements in G, because for each $C > 0$, if $(x, y) \in \mathbb{Z}^2$ satisfies $|x + y\sqrt{d}| \leq C$ and $|x - y\sqrt{d}| \leq C$, then $|x|$ and $|y|$ are bounded.

Further G is contained in the one dimensional subspace $t_1 + t_2 = 0$ of $\mathbb{R}^2$. A discrete subgroup in a real vector space of dimension 1 has rank ≤ 1 (see § 2.2.7). It easily follows that any solution $(x, y) \in \mathbb{Z}^2$ with $x > 0$ and $y \geq 0$ of Pell's equation satisfies $x + y\sqrt{d} = (x_1 + y_1\sqrt{d})^n$ for some $n \geq 0$.

Hence the problems remains to find the fundamental solution (x_1, y_1). It turns out, as we shall see, that x_1 may be quite large without d being to large. But there is an efficient algorithm to solve the problem.

The connexion with Diophantine approximation arises from the following remark. If (x, y) is a solution, then $(x - \sqrt{d}y)(x + \sqrt{d}y) = 1$, hence x/y is a good rational approximation of $\sqrt{d}$ and this approximation is sharper when x is larger. Hence a strategy for solving Pell's equation (2.21) is based on the continued fraction expansion of $\sqrt{d}$.

Let again d be a positive integer which is not a square. It is known that the continued fraction expansion

$$\sqrt{d} = [a_0;\ \overline{a_1,\ a_2,\ \ldots,\ a_k}]$$

of the square root of $d > 0$ has $a_0 = [\sqrt{d}]$ and $a_k = 2a_0$. Moreover

$$a_1,\ a_2,\ \ldots,\ a_{k-1}$$

is a *palindrome*: $a_i = a_{k-i}$ $(1 \leq i \leq k - 1)$. The next proposition shows that the length k of the period is odd if and only if the Diophantine equation $x^2 - dy^2 = -1$ has a root in rational integers x, y.

Proposition 2.22. *Let d be a positive which is not a square. Write*

$$\sqrt{d} = [a_0;\ \overline{a_1,\ a_2,\ \ldots,\ a_k}].$$

a) When k is even, the fundamental solution of the equation $x^2 - dy^2 = 1$ is given by

$$\frac{x_1}{y_1} = [a_0;\ a_1,\ a_2,\ \ldots,\ a_{k-1}]$$

and there is no solution to the equation $x^2 - dy^2 = -1$.
b) When k is odd, the fundamental solution to $x^2 - dy^2 = -1$ is given by

$$\frac{x_1}{y_1} = [a_0;\ a_1,\ a_2,\ \ldots,\ a_{k-1}]$$

and the fundamental solution to $x^2 - dy^2 = 1$ is given by

$$\frac{x_2}{y_2} = [a_0;\ a_1,\ a_2,\ \ldots,\ a_{k-1},\ a_k,\ a_1,\ a_2,\ \ldots,\ a_{k-1}].$$

The solutions (x_n, y_n) are obtained by a similar formula: writing A for the block $a_1,\ a_2,\ \ldots,\ a_{k-1}$,

$$\frac{x_n}{y_n} = [a_0;\ A,\ a_k,\ A,\ a_k,\ \ldots,\ A,\ a_k,\ A]$$

where A occurs n times.

We consider numerical examples. The easiest Pell's equation is $x^2-2y^2=-1$ with $d=2$ and $\sqrt{2}=[1;\overline{2}]$. The fundamental solution is $(x_1,y_1)=(1,1)$. For the equation $x^2-2y^2=1$ the fundamental solution is $x=3$, $y=2$, corresponding to the expansion

$$[1;2] = 1+\frac{1}{2} = \frac{3}{2}.$$

Here is another example due to Brahmagupta in 628:

$$x^2 - 92y^2 = 1.$$

Brahmagupta did not use continued fractions but a method of his own (called "cyclic method" — Chakravala — see [39]), and he found the fundamental solution which is $x=1151$, $y=120$:

$$1151^2 - 92\cdot 120^2 = 1\,324\,801 - 1\,324\,800 = 1.$$

The continued fraction expansion of $\sqrt{92}=9,591663046625\ldots$ is [3]

$$\sqrt{92} = [9;\overline{1,\ 1,\ 2,\ 4,\ 2,\ 1,\ 1,\ 18}]$$

and the fundamental solution arises from

$$[9;\ 1,\ 1,\ 2,\ 4,\ 2,\ 1,\ 1] = \frac{1151}{120}.$$

The next example is due to Bhaskara II in his work *Bijaganita* (1150): the fundamental solution to $x^2-61y^2=1$ is

$$x = 1\,766\,319\,049, \qquad y = 226\,153\,980.$$

Here $\sqrt{61}=[7;\overline{1,\ 4,\ 3,\ 1,\ 2,\ 2,\ 1,\ 3,\ 4,\ 1,\ 14}]$ and

$$[7;1,4,3,1,2,2,1,3,4,1,14,1,4,3,1,2,2,1,3,5] = \frac{1\,766\,319\,049}{226\,153\,980}.$$

The fundamental solution to $x^2-61y^2=-1$ is obtained as follows:

$$[7;1,4,3,1,2,2,1,3,5] = \frac{29\ 718}{3\ 805},$$

$$29\ 718^2 = 883\ 159\ 524, \quad 61\cdot 3805^2 = 883\ 159\ 525.$$

[3] Easy to compute using http://wims.unice.fr/wims/

A further example due to Narayana (14th Century) is $x^2 - 103y^2 = 1$ with the fundamental solution $x = 227\,528$, $y = 22\,419$. Indeed

$$227\,528^2 - 103 \cdot 22\,419^2 = 51\,768\,990\,784 - 51\,768\,990\,783 = 1.$$

$$\sqrt{103} = [10; \overline{6,\ 1,\ 2,\ 1,\ 1,\ 9,\ 1,\ 1,\ 2,\ 1,\ 6,\ 20}]$$

and

$$[10; 6,\ 1,\ 2,\ 1,\ 1,\ 9,\ 1,\ 1,\ 2,\ 1,\ 6] = \frac{227\,528}{22\,419}.$$

Fermat also knew how to solve Pell's equation $x^2 - dy^2 = 1$: he found the fundamental solution for $d = 61$ (Bhaskara's equation) as well as for $d = 109$:

$$x = 158070671986249, \quad y = 15140424455100.$$

A Pell equation occurred already much earlier in the *Cattle problem* attributed to Archimedes. There are bulls and cows of different colors, the first part of the problem involves several unknowns and easy equations so solve:

$$B - \left(\frac{1}{2} + \frac{1}{3}\right) N = N - \left(\frac{1}{4} + \frac{1}{5}\right) X = X - \left(\frac{1}{6} + \frac{1}{7}\right) B = J.$$

Up to a factor, the solution is

$$B = 2226,\ N = 1602,\ X = 1580,\ J = 891.$$

The second part of the Cattle problem amounts to solving the Pell equation

$$x^2 - 4729494y^2 = 1.$$

A partial solution was given in 1880 by A. Amthor. The fundamental solution has been given in 1998 by Ilan Vardi in a simple explicit formula

$$\left[\frac{25194541}{184119152}\,(109931986732829734979866232821433543901088049 + \right.$$
$$\left. 50549485234315033074477819735540408986340\sqrt{4729494}\right)^{4658}\Big]$$

The size of the fundamental solution is $\simeq 10^{103275}$.

Pell-Fermat Diophantine equations occur in the construction of Riemannian varieties with negative curvature called *arithmetic varieties*. See [3].

We consider another connexion between Diophantine approximation and Diophantine equations which we shall expand in § 2.2.9. In 1909 A. Thue found a connection between Diophantine equation and refinements of Liouville's estimate. We restrict here on one specific example.

Liouville's estimate for the rational Diophantine approximation of $\sqrt[3]{2}$ is

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{1}{9q^3}$$

for sufficiently large q (use Lemma 1.19 with $P(X) = X^3 - 2$, $c = 3\sqrt[3]{2} < 9$). Thue was the first to achieve an improvement of the exponent 3. A explicit estimate was then obtained by A. Baker

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{1}{10^6 q^{2.955}}$$

and refined by Chudnovskii, Easton, Rickert, Voutier and others, until 1997 when M. Bennett proved that *for any* $p/q \in \mathbb{Q}$,

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| \geq \frac{1}{4\ q^{2,5}}.$$

From his result, Thue deduced that *for any fixed* $k \in \mathbb{Z} \setminus \{0\}$, *there are only finitely many* $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ *satisfying the Diophantine equation* $x^3 - 2y^3 = k$. The result of Baker shows more precisely that if $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ is a solution to $x^3 - 2y^3 = k$, then

$$|x| \leq 10^{137}|k|^{23}.$$

M. Bennett gave the sharper estimate: *for any* $(x, y) \in \mathbb{Z}^2$ *with* $x > 0$,

$$|x^3 - 2y^3| \geq \sqrt{x}.$$

The connexion between Diophantine approximation to $\sqrt[3]{2}$ and the Diophantine equation $x^3 - 2y^3 = k$ is explained in the next lemma.

Lemma 2.23. *Let* η *be a positive real number. The two following properties are equivalent.*
(i) There exists a constant $c_1 > 0$ *such that, for any* $p/q \in \mathbb{Q}$ *with* $q > 0$,

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{c_1}{q^\eta}.$$

(ii) There exists a constant $c_2 > 0$ *such that, for any* $(x, y) \in \mathbb{Z}^2$ *with* $x > 0$,

$$|x^3 - 2y^3| \geq c_2 x^{3-\eta}.$$

Properties (i) and (ii) are true but uninteresting with $\eta \geq 3$. They are not true with $\eta < 2$. It is not expected that they are true with $\eta = 2$, but it is expected that they are true for any $\eta > 2$.

Proof. We assume $\eta < 3$, otherwise the result is trivial. Set $\alpha = \sqrt[3]{2}$.

Assume (i) and let $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ have $x > 0$. Set $k = x^3 - 2y^3$. Since 2 is not the cube of a rational number we have $k \neq 0$. If $y = 0$ assertion (ii) plainly holds. So assume $y \neq 0$.

Write

$$x^3 - 2y^3 = (x - \alpha y)(x^2 + \alpha xy + \alpha^2 y^2).$$

The polynomial $X^2 + \alpha X + \alpha^2$ has negative discriminant $-3\alpha^2$, hence has a positive minimum $c_0 = 3\alpha^2/4$. Hence the value at (x, y) of the quadratic form $X^2 + \alpha XY + \alpha^2 Y^2$ is bounded form below by $c_0 y^2$. From (i) we deduce

$$|k| = |y|^3 \left| \sqrt[3]{2} - \frac{x}{y} \right| (x^2 + \alpha xy + \alpha^2 y^2) \geq \frac{c_1 c_0 |y|^3}{|y|^\eta} = c_3 |y|^{3-\eta}.$$

This gives an upper bound for $|y|$:

$$|y| \leq c_4 |k|^{1/(3-\eta)}, \quad \text{hence} \quad |y^3| \leq c_4 |k|^{3/(3-\eta)}.$$

We want an upper bound for x: we use $x^3 = k + 2y^3$ and we bound $|k|$ by $|k|^{3/(3-\eta)}$ since $3/(3-\eta) > 1$. Hence

$$x^3 \leq c_5 |k|^{3/(3-\eta)} \quad \text{and} \quad x^{3-\eta} \leq c_6 |k|.$$

Conversely, assume (ii). Let p/q be a rational number. If p is not the nearest integer to $q\alpha$, then $|q\alpha - p| > 1/2$ and the estimate (i) is trivial. So we assume $|q\alpha - p| \leq 1/2$. We need only the weaker estimate $c_7 q < p < c_8 q$ with some positive constants c_7 and c_8, showing that we may replace p by q or q by p in our estimates, provided that we adjust the constants. From

$$p^3 - 2q^3 = (p - \alpha q)(p^2 + \alpha pq + \alpha^2 q^2),$$

using (ii), we deduce

$$c_2 p^{3-\eta} \leq c_{10} q^3 \left| \alpha - \frac{p}{q} \right|,$$

and (i) easily follows.

□

2.2.4 Algebraic preliminaries: algebraic and transcendental elements, algebraic independence

Content

Rings: domains (no zero divisor), Euclidean rings, examples ($\mathbb{Z}$, $k[X]$, $\mathbb{Z}[i]$), PID (domain where any ideal is principal), UFD (unique factorization domain), further example ($\mathbb{Z}[X]$, $k[X_1, \ldots, X_n]$).
Fields. Vector spaces, modules. Example: $\mathbb{Z}$–module = abelian group.
Extensions of fields. Subrings, subfields. Intersection of subrings, subfields, submodules, vector subspaces. Subrings or subfield generated by a subset: $A[E]$, $k(E)$ (and modules or vector spaces spanned by a subset). Special cases where $E = \{\alpha_1, \ldots, \alpha_n\}$: finitely generated ring or field extension: $A[\alpha_1, \ldots, \alpha_n]$, $k(\alpha_1, \ldots, \alpha_n)$. Simple extension ($n = 1$).
Finite extension, example: $\mathbb{Q}(i)/\mathbb{Q}$. Degree $[K : k]$ of a finite extension K/k. Multiplicativity of the degree for $K_1 \subset K_2 \subset K_3$.
Algebraic element over a field k: equivalent properties. Transcendental element,

examples: e is transcendental over $\mathbb{Q}$; also X in the field of rational fractions over the complex field is transcendental over $\mathbb{C}$. Irreducible (monic) polynomial of an algebraic element. For α in $\mathbb{C}$, we have $k(\alpha) = k[\alpha]$ iff α is algebraic; computing the inverse of an algebraic element using Euclidean division and Bézout's Theorem.
Sum and product of algebraic elements: prove that they are algebraic either by linear algebra or by means of the theorem of the elementary symmetric functions (see § 2.2.5). Field $\overline{\mathbb{Q}}$ of algebraic numbers, algebraic closure.
Example of an algebraic extension which is not finite: $\overline{\mathbb{Q}}/\mathbb{Q}$. Algebraic extension, any finite extension is algebraic.
Algebraically independent or dependent elements (algebraically free subset). Examples: numbers, functions. Transcendence degree, transcendence basis of a finitely generated extension. Properties: additivity of the transcendence degree for $K_1 \subset K_2 \subset K_3$. Transcendence degree 0 means algebraic extension.
Corollary: algebraic independence over $\mathbb{Q}$ is equivalent to algebraic independence over $\overline{\mathbb{Q}}$.
The transcendence degree of $k(E)/k$ is $\geq n$ if and only if there exists in E a set of at least n algebraically independent elements over k.

Exercise 2.24. Let α be a complex number. Show that the following properties are equivalent.
(i) The number α is algebraic.
(ii) The numbers $1, \alpha, \alpha^2, \ldots$ are linearly dependent over $\mathbb{Q}$.
(iii) The $\mathbb{Q}$-vector subspace of $\mathbb{C}$ spanned by the numbers $1, \alpha, \alpha^2, \ldots$ has finite dimension.
(iv) There exists an integer $N \geq 1$ such that the $\mathbb{Q}$-vector subspace of $\mathbb{C}$ spanned by the N numbers $1, \alpha, \alpha^2, \ldots, \alpha^{N-1}$ has dimension $< N$.
(v) There exists positive integers $n_1 < n_2 < \ldots < n_k$ such that $\alpha^{n_1}, \ldots, \alpha^{n_k}$ are linearly dependent over $\mathbb{Q}$.

Exercise 2.25. Show that the field $\overline{\mathbb{Q}}$ is an algebraic extension of $\mathbb{Q}$ which is not finite.
`Hint.` *One of many solutions is to check that for any $n \geq 1$ the polynomial $X^n - 2$ is irreducible.*
A more challenging solution is to check that the numbers $\sqrt{m}$, where m ranges over the squarefree integers, are linearly independent over $\mathbb{Q}$. One may show by induction that if $a_1, \ldots, a_n$ are positive squarefree integers > 1 which are pairwise relatively prime, then the 2^n numbers

$$\sqrt{\prod_{i \in I} a_i}, \quad I \subset \{1, \ldots, n\},$$

are linearly independent over $\mathbb{Q}$. Hence the field $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})$ has degree 2^n over $\mathbb{Q}$.

Exercise 2.26. Let R and S be two rational fractions in $k(T)$. Show that there exists a non–zero polynomial $F \in k[X, Y]$ such that $F(R, S) = 0$. Deduce

that any set of at least two elements in $k(T)$ consists of algebraically dependent elements, hence $k(T)$ has transcendence degree 1 over k.
Generalize to $k(T_1, \ldots, T_n)$

Exercise 2.27. Let $t_1, \ldots, t_n$ be algebraically independent complex numbers. Check that any subset of $\{t_1, \ldots, t_n\}$ consists of algebraically independent element. Check that for any P and Q in $\overline{\mathbb{Q}}[X_1, \ldots, X_n]$ for which $Q(t_1, \ldots, t_n) \neq 0$ and such that the rational fraction $R = P/Q$ is not constant, the number $R(t_1, \ldots, t_n)$ is transcendental.

Exercise 2.28. Check that an entire function (which means a complex function which is analytic in all of $\mathbb{C}$) is transcendental if and only if it is not a polynomial. Check that a meromorphic function in $\mathbb{C}$ is transcendental if and only if it is not a rational function.

2.2.5 Elementary symmetric functions

References for this section are [9, 21].

Let L be the field $\mathbb{Q}(x_1, \ldots, x_n)$ of rational fractions in n variables over $\mathbb{Q}$. The *elementary symmetric functions* $s_1, \ldots, s_n \in \mathbb{Q}[x_1, \ldots, x_n]$ are defined by

$$(X - x_1)(X - x_2) \cdots (X - x_n) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \cdots + (-1)^n s_n.$$

For instance

$$s_1 = x_1 + \cdots + x_n, \quad s_n = x_1 \cdots x_n$$

and

$$s_2 = x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_2x_n + \cdots + x_{n-1}x_n.$$

More generally, for $1 \leq k \leq n$, *the k-th elementary symmetric function in n variables* is

$$s_k = \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

The *general polynomial of degree n* is $f(X) = (X - x_1)(X - x_2) \cdots (X - x_n)$. Further, let K denote the subfield $\mathbb{Q}(s_1, \ldots, s_n)$ of L. The polynomial f has its coefficients in K and its splitting field over K is L. Since f has degree n, the Galois group of L over K is (isomorphic to) a subgroup of $\mathfrak{S}_n$. As a consequence $[L : K] \leq n!$.

Any permutation of $\{1, \ldots, n\}$ induces an automorphism of L which fixes each of s_k $(1 \leq k \leq n)$. Hence K is contained in the subfield $L^{\mathfrak{S}_n}$ of L fixed by $\mathfrak{S}_n$. According to Galois theory, the extension $L/L^{\mathfrak{S}_n}$ has degree $n!$ Hence $K = L^{\mathfrak{S}_n}$ and L is an extension of K of degree $n!$ and Galois group $\mathfrak{S}_n$.

A rational function $F(x_1, \ldots, x_n) \in L$ is called *symmetric* if it is invariant under $\mathfrak{S}_n$. Hence we have proved:

Proposition 2.29. *A rational function $F(x_1, \ldots, x_n) \in \mathbb{Q}(x_1, \ldots, x_n)$ is symmetric if and only if there exists a rational function G in n variables such that*

$$F(x_1, \ldots, x_n) = G(s_1, \ldots, s_n).$$

The rational function G is unique. If F is a polynomial, then G is also a polynomial. An algorithm for computing it is given in exercise 37, § 14.6 of [9].

Exercise 2.30. Prove that the elements $s_1, \ldots, s_n$ are algebraically independent over $\mathbb{Q}$.

2.2.6 Modules over principal rings

References for this section are [9, 15, 21].

Let A be a ring (commutative with unit, as usual), M a A–module, N_1 and N_2 submodules of M. By definition M is the direct sum of N_1 and N_2 if the map $(x_1, x_2) \mapsto x_1 + x_2$ is an isomorphism of A-modules of $N_1 \times N_2$ onto M. In this case we write $M = N_1 \oplus N_2$. This means $M = N_1 + N_2$ and $N_1 \cap N_2 = \{0\}$.

A *free A–module* is a A-module having a basis. Example like $\mathbb{Z}/2\mathbb{Z}$ (and more generally any finite abelian group viewed as a $\mathbb{Z}$–module) or $\mathbb{Q}$ show that modules over $\mathbb{Z}$ may not have a basis.

When A is a domain and M a A-module, the *rank* of M is the maximal number of elements in M which are linearly independent over A. If we denote by K the field of fractions of A and if M is a free A–module, then one can embed M into a K-vector space V and the rank of a submodule N of M is the dimension of the K–vector space spanned by N in V. For instance the rank of M itself is the number of elements in any basis of M over A.

Proposition 2.31 (Free modules over a PID)**.** *Let A be a PID, M a free A-module of rank m and N a sub–A-module of M. Then N is free of rank $n \leq m$. Moreover there exists a basis $\{e_1, \ldots, e_m\}$ of M as a A-module and there exists elements $a_1, \ldots, a_n$ in A such that $\{a_1 e_1, \ldots, a_n e_n\}$ is a basis of N over A and a_i divides a_{i+1} in A for $1 \leq i < n$.*

The ideals $a_1 A \supset a_2 A \supset \cdots \supset a_n A$ of A are called the *invariant factors* of the sub–A-module N of M: they do not depend on the basis $(a_1, \ldots, e_n)$ of M satisfying the conditions of Proposition 2.31.

2.2.7 Geometry of numbers: subgroups of $\mathbb{R}^n$.

References for this section are [4, 16, 29].

Lemma 2.32. *A subgroup G of $\mathbb{R}^n$ is discrete in $\mathbb{R}^n$ if and only if there exists an open subset U of $\mathbb{R}^n$ containing 0 such that $G \cap U$ is discrete.*

Exercise 2.33. 1. Check that a non discrete subgroup of $\mathbb{R}$ is dense in $\mathbb{R}$
2. Give the list of closed subgroups of $\mathbb{R}$.
3. Let G be a finitely generated subgroup of $\mathbb{R}$. Give a necessary and sufficient condition on the rank of G for G to be dense in $\mathbb{R}$.

4. Let $\vartheta \in \mathbb{R}$. Give a necessary and sufficient condition on ϑ for the subgroup $\mathbb{Z} + \mathbb{Z}\vartheta$ to be dense in $\mathbb{R}$.

Proposition 2.34. *Let G be a discrete subgroup of $\mathbb{R}^n$. There exists an integer t in the interval $0 \leq t \leq n$ and there exist elements $e_1, \ldots, e_t$ in G, which are linearly independent over $\mathbb{R}$, such that $G = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_t$.*

In particular $e_1, \ldots, e_t$ are linearly independent over $\mathbb{Z}$, hence G is free of rank t. The integer t is the dimension of the $\mathbb{R}$–subspace of $\mathbb{R}^n$ spanned by G.

Exercise 2.35. From Proposition 2.34, deduce that in a discrete subgroup of $\mathbb{R}^n$, linearly independent elements over $\mathbb{Z}$ are linearly independent over $\mathbb{R}$.

Definition. *A discrete subgroup of $\mathbb{R}^n$ of maximal rank n is called a lattice) of $\mathbb{R}^n$.*

Proof of Proposition 2.34. Denote by V the vector subspace of $\mathbb{R}^n$ over $\mathbb{R}$ spanned by G, by t its dimension and let $\{f_1, \ldots, f_t\}$ be a maximal subset of G which is free over $\mathbb{R}$: it is a basis of V over $\mathbb{R}^n$ and $G' = \mathbb{Z}f_1 + \cdots + \mathbb{Z}f_t$ is a subgroup of G. We show that G' has finite index in G, which means that there are only finitely many classes of G modulo G'.

Let K be the compact subset of $\mathbb{R}^n$ defined by

$$\{u_1 f_1 + \cdots + u_t f_t \ ; \ 0 \leq u_i \leq 1 \ (1 \leq i \leq t)\}.$$

Since G is discrete, $G \cap K$ is finite.

Let $x \in G$. Then $x \in V$, hence we can write $x = x_1 f_1 + \cdots + x_t f_t$ with $x_i \in \mathbb{R}$. Let $m_i = [x_i]$ be the integral part of x_i:

$$m_i \in \mathbb{Z}, \quad 0 \leq x_i - m_i < 1 \qquad (1 \leq i \leq n).$$

Set $x' = m_1 f_1 + \cdots + m_t f_t$. Then $x' \in G'$ and $x - x' \in G \cap K$. Therefore there are only finitely many classes of G modulo G', which means that G' has finite index in G.

Denote by s the order of the finite group G/G' and set $f_i' = f_i/s$ $(1 \leq i \leq t)$. We have

$$G' = \mathbb{Z}f_1 + \cdots + \mathbb{Z}f_t \subset G \subset \mathbb{Z}f_1' + \cdots + \mathbb{Z}f_t',$$

and the conclusion follows from Proposition 2.31.

□

Theorem 2.36 (Structure of subgroups of $\mathbb{R}^n$)**.** *Let G be an additive subgroup of $\mathbb{R}^n$. There exists a maximal vector subspace V of $\mathbb{R}^n$ over $\mathbb{R}$ which is contained in the topological closure of G. Let d be the dimension of V and $d + t$ the dimension of the vector space spanned by G over $\mathbb{R}$. Set $G' = G \cap V$. Then G' is dense in V and there exists a discrete subgroup G'' of G, of rank t, such that G is the direct sum of G' and G''.*

Exercise 2.37. Let $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$. Consider the subgroup

$$G = \mathbb{Z}^n + \mathbb{Z}\mathbf{x} = \{(a_1 + a_0x_1, \ldots, a_n + a_0x_n)\ ;\ (a_0, \ldots, a_n) \in \mathbb{Z}^{n+1}\}$$

of $\mathbb{R}^n$.
1. Show that G is discrete in $\mathbb{R}^n$ if and only if $\mathbf{x} \in \mathbb{Q}^n$.
2. Deduce that the following properties are equivalent.
(i) 0 is an accumulation point of G.
(ii) For any $\epsilon > 0$, there exist integers $p_1, \ldots, p_n$, q, with $q > 0$, such that

$$0 < \max_{1 \le i \le n} |qx_i - p_i| < \epsilon.$$

(iii) A least one of the n numbers $x_1, \ldots, x_n$ is irrational.
3. Check that G is dense in $\mathbb{R}^n$ if and only if the numbers $1, x_1, \ldots, x_n$ are linearly independent over $\mathbb{Q}$.
Deduce that for any $(\xi_1, \xi_2) \in \mathbb{R}^2$ and for any $\epsilon > 0$, there exist rational integers p_1, p_2 and q with

$$|\xi_1 - p_1 - q\sqrt{2}| \le \epsilon \quad \text{and} \quad |\xi_2 - p_1 - q\sqrt{3}| \le \epsilon.$$

Let G be a lattice in $\mathbb{R}^n$. For each basis $\mathbf{e} = \{e_1, \ldots, e_n\}$ of G the parallelogram

$$P_{\mathbf{e}} = \{x_1e_1 + \cdots + x_ne_n\ ;\ 0 \le x_i < 1\ (1 \le i \le n)\}$$

is a *fundamental domain* for G, which means a complete system of representative of classes modulo G. We get a partition of $\mathbb{R}^n$ as

$$\mathbb{R}^n = \bigcup_{g \in G} (P_{\mathbf{e}} + g) \tag{2.38}$$

A change of bases of G is obtained with a matrix with integer coefficients having determinant ± 1, hence the Lebesgue measure $\mu(P_{\mathbf{e}})$ of $P_{\mathbf{e}}$ does not depend on $\mathbf{e}$: this number is called the *volume* of the lattice G and denoted by $v(G)$.

Here is an example of results obtained by H. Minkowski in the XIX–th century as an application of his *geometry of numbers.*

Theorem 2.39 (Minkowski)**.** *Let G be a lattice in $\mathbb{R}^n$ and B a measurable subset of $\mathbb{R}^n$. Set $\mu(B) > v(G)$. Then there exist $x \neq y$ in B such that $x - y \in G$.*

Proof. From (2.38) we deduce that B is the disjoint union of the $B \cap (P_{\mathbf{e}} + g)$ with g running over G. Hence

$$\mu(B) = \sum_{g \in G} \mu\left(B \cap (P_{\mathbf{e}} + g)\right).$$

Since Lebesgue measure is invariant under translation

$$\mu\left(B \cap (P_{\mathbf{e}} + g)\right) = \mu\left((-g + B) \cap P_{\mathbf{e}}\right).$$

The sets $(-g+B) \cap P_{\mathbf{e}}$ are all contained in $P_{\mathbf{e}}$ and the sum of their measures is $\mu(B) > \mu(P_{\mathbf{e}})$. Therefore they are not all pairwise disjoint – this is one of the versions of the *Dirichlet box principle*). There exists $g \neq g'$ in G such that

$$(-g + B) \cap (-g' + B) \neq \emptyset.$$

Let x and y in B satisfy $-g + x = -g' + y$. Then $x - y = g - g' \in G \setminus \{0\}$.

□

Corollary 2.40. *Let G be a lattice in $\mathbb{R}^n$ and let B be a measurable subset of $\mathbb{R}^n$, convex and symmetric with respect to the origin, such that $\mu(B) > 2^n v(G)$. Then $B \cap G \neq \{0\}$.*

Proof. We use Theorem 2.39 with the set

$$B' = \frac{1}{2}B = \{x \in \mathbb{R}^n \ ; \ 2x \in B\}.$$

We have $\mu(B') = 2^{-n}\mu(B) > v(G)$, hence by Theorem 2.39 there exists $x \neq y$ in B' such that $x - y \in G$. Now $2x$ and $2y$ are in B, and since B is symmetric $-2y \in B$. Finally B is convex, hence $(2x - 2y)/2 = x - y \in G \cap B \setminus \{0\}$.

□

Remark. *With the notations of Corollary 2.40, if B is also compact in $\mathbb{R}^n$, then the weaker inequality $\mu(B) \geq 2^n v(G)$ suffices to reach the conclusion. This is obtained by applying Corollary 2.40 with $(1+\epsilon)B$ for $\epsilon \to 0$.*

Exercise 2.41. Let m and n be positive integers.
a) Let t_{ij} for $1 \leq i, j \leq n$ be n^2 real numbers with determinant ± 1. Let $A_1, \ldots, A_n$ be positive real numbers with $A_1 \cdots A_n = 1$. Show that there exists an non–zero element $(x_1, \ldots, x_n)$ in $\mathbb{Z}^n$ such that

$$|x_1 t_{i1} + \cdots + x_n t_{in}| < A_i \quad \text{for} \quad 1 \leq i \leq n-1$$

and

$$|x_1 t_{1n} + \cdots + x_n t_{nn}| \leq A_n.$$

`Hint`. First solve the system with the weaker inequality $<$ in place of $<$

$$|x_1 t_{i1} + \cdots + x_n t_{in}| \leq A_i \quad \text{for} \quad 1 \leq i \leq n$$

by using Corollary 2.40. Next use the same method but with A_n replaced with $A_n + \epsilon$ for a sequence of ϵ which tends to 0.
b) Deduce the following result. Let ϑ_{ij} $(1 \leq i \leq n,\ 1 \leq j \leq m)$ be mn real numbers. Let $Q > 1$ be a real number. Show that there exists rational integers $q_1, \ldots, q_m$, $p_1, \ldots, p_n$ with

$$1 \leq \max\{|q_1|, \ \ldots, \ |q_m|\} < Q^{n/m}$$

and

$$\max_{1\le i\le n} |\vartheta_{i1}q_1 + \cdots + \vartheta_{im}q_m - p_i| \le \frac{1}{Q}.$$

`Hint`. Use a) with n replaced by $n+m$ and for a triangular matrix $(t_{ij})_{1\le i,j\le m+n}$ with 1 on the diagonal.
c) Deduce that if $\vartheta_1, \ldots, \vartheta_m$ are real numbers and H a real number > 1, then there exists a tuple $(a_0, a_1, \ldots, a_m)$ of rational integers such that

$$0 < \max_{1\le i\le m} |a_i| < H \quad \text{and} \quad |a_0 + a_1\vartheta_1 + \cdots + a_m\vartheta_m| \le H^{-m}.$$

d) Let ϑ be a real number with $|\vartheta| \le 1/2$, d a positive integer and H a positive integer. Show that there exists a non–zero polynomial $P \in \mathbb{Z}[X]$ of degree $\le d$ and coefficients in the interval $[-H, H]$ such that

$$|P(\vartheta)| \le H^{-d}.$$

We conclude this section with the definition of a *rational subspace*. Let $k \subset K$ be a field extension and n a positive integer. For a K-vector subspace V of K^n, the two following properties are equivalent:
(i) There exists a basis of V which consists of elements in k^n.
(ii) There exist linear forms $L_1, \ldots, L_m$ with coefficients in k such that V is the intersection of the hyperplans $L_i = 0$, $(1 \le i \le m)$.
When there properties are satisfied the subspace V is called *rational over* k.

Exercise 2.42. Let $\vartheta_1, \ldots, \vartheta_m$ be real numbers. Assume that $1, \vartheta_1, \ldots, \vartheta_m$ are linearly independent over $\mathbb{Q}$. Let V be a vector subspace of $\mathbb{R}^{m+1}$ which is rational over $\mathbb{Q}$ and has dimension $\le m$.
a) Check that the intersection of V with the real line $\mathbb{R}(1, \vartheta_1, \ldots, \vartheta_m)$ is $\{0\}$.
b) Deduce that

$$\|(x_0, x_1, \ldots, x_m)\| = \max_{1\le i\le m} |x_0\vartheta_j - x_j|$$

defines a norm on V.

2.2.8 Elimination Theory, Resultant.

References for this section are [9, 21, 35].

Let k be a field and P, Q two polynomials in $\mathbb{Q}[X]$ of degrees n and m respectively. Since $k[X]$ is a UFD, we can decompose P and Q as products of irreducible polynomials. The ideal $\mathcal{I}$ generated by P and Q is principal, generated by the greatest common divisor of P and Q (this gcd is unique up to a constant, it is unique if we require that it is monic. Bézout's Theorem states that this gcd can be written as $UP + VQ$ with U and V in $k[X]$, and Euclide's algorithms gives a solution (U, V) with $\deg U < \deg Q$ and $\deg V < \deg P$. This ideal is $k[X]$ if and only if the monic gcd is 1, which means also that P and Q have no common zero in an algebraic closure of k.

Assume $\gcd(P,Q) = 1$. The problem with Euclide's algorithm is that it is efficient for numerical purposes, when the polynomials P and Q are given, but it is not so efficient for giving estimates for the coefficients of U and V. Fortunately there is another efficient algorithm to compute U and V such that $PU + QV$ is a non–zero constant in k. Write

$$P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0, \quad Q = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_0$$

and

$$U = u_{m-1} X^{m-1} + u_{m-2} X^{m-2} + \cdots + u_0, \quad V = v_{n-1} X^{n-1} + v_{n-2} X^{n-2} + \cdots + v_0.$$

Consider the coefficients $u_0, u_1, \ldots, u_{m-1}$, $v_0, v_1, \ldots, v_{n-1}$ of U and V as $m+n$ unknowns which should satisfy the system of $m+n$ equations given by the fact that the coefficients of $X, X^2, \ldots, X^{m+n-1}$ in $PU + QV$ is zero, while the constant coefficient is not zero. The determinant of the matrix of this system is not zero, since there is a solution by Bézout's Theorem. Here is the matrix

$$\begin{pmatrix}
a_n & a_{n-1} & \cdots & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\
0 & a_n & \cdots & \cdots & a_2 & a_1 & a_0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & a_n & a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_0 \\
b_m & b_{m-1} & \cdots & b_1 & b_0 & 0 & 0 & \cdots & 0 \\
0 & b_m & \cdots & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & & \vdots & \vdots & \ddots & & \vdots \\
\vdots & \vdots & & \ddots & & & & \ddots & \vdots \\
0 & 0 & \cdots & 0 & b_m & b_{m-1} & b_{m-2} & \cdots & b_0
\end{pmatrix}$$

There are m rows with the coefficients of P and n rows [4] with the coefficients of Q, the diagonal is $(a_n, \ldots, a_n, b_0, \ldots, b_0)$. This matrix can be considered for any pair (P,Q) of polynomials with coefficients in any domain A. The determinant R of this matrix is then an element in A which is called the *resultant* of P and Q. The determinant is invariant by linear combinations of the columns: multiplying the k–th column by X^{m+n-k}, adding to the last column and expanding the determinant shows that there are polynomials U and V such that $R = PU + QV$. The resultant is not zero if and only if U and V are relatively prime in $k[X]$, where k is the quotient field of A.

Exercise 2.43. a) Using the Cauchy–Schwarz inequality

$$\left| \sum_i x_i y_i \right|^2 \leq \left| \sum_i x_i \right|^2 \cdot \left| \sum_i y_i \right|^2,$$

show that the absolute value of a determinant with complex coefficients is bounded by the product of the Euclidean norms of its columns.

[4] The matrix has been written in the case $m = n - 1$

b) For a polynomial $P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$ in $\mathbb{C}[X]$, define

$$\|P\| = (|a_n|^2 + \cdots + |a_0|^2)^{1/2}.$$

Let P and Q be two non–constant polynomials in $\mathbb{Z}[X]$ of degrees n and m respectively. Show that the two following properties are equivalent:
(i) P and Q are relatively prime in $\mathbb{Q}[X]$.
(ii) For any $\vartheta \in \mathbb{C}$,

$$(m+n)\|P\|^m \|Q\|^n \max\{|P(\vartheta)|, |Q(\vartheta)|\} > 1.$$

2.2.9 Diophantine Approximation: historical survey

References for this section are [12, 29, 11, 5].

Definition. *Given a real irrational number ϑ, a function $\varphi = \mathbb{N} \to \mathbb{R}_{>0}$ is an irrationality measure for ϑ if there exists an integer $q_0 > 0$ such that, for any $p/q \in \mathbb{Q}$ with $q \geq q_0$,*

$$\left|\vartheta - \frac{p}{q}\right| \geq \varphi(q).$$

Further, a real number κ is an irrationality exponent for ϑ if there exists a positive constant c such that the function c/q^κ is an irrationality measure for ϑ.

From Dirichlet's box principle (see (i)⇒(iv) in Lemma 1.11) it follows that any irrationality exponent κ satisfies $\kappa \geq 2$. Irrational quadratic numbers have irrationality exponent 2. It is known (see for instance [29] Th. 5F p. 22) that 2 is an irrationality exponent for an irrational real number ϑ if and only if the sequence of *partial quotients* $(a_0, a_1, \ldots)$ in the continued fraction expansion of ϑ is bounded: these are called the *badly approximable numbers*.

From Liouville's inequality in Lemma 2.16 it follows that any irrational algebraic real number α has a finite irrationality exponent $\leq d$. Liouville numbers are by definition exactly the irrational real numbers which have no finite irrationality exponent.

For any $\kappa \geq 2$, there are irrational real numbers ϑ for which κ is an irrationality exponent and is the best: no positive number less than κ is an irrationality exponent for ϑ. Examples due to Y. Bugeaud in connexion with the triadic Cantor set (see [38]) are

$$\sum_{n=0}^{\infty} 3^{-\lceil \lambda \kappa \rceil^n}$$

where λ is any positive real number.

The first significant improvement to Liouville's inequality is due to the Norwegian mathematician Axel Thue who proved in 1909:

Theorem 2.44 (A. Thue, 1909)**.** *Let α be a real algebraic number of degree $d \geq 3$. Then any $\kappa > (d/2) + 1$ is an irrationality exponent for α.*

The fact that the irrationality exponent is $< d$ has very important consequences in the theory of Diophantine equations. We gave an example in § 2.2.3, here is the more general result of Thue on Diophantine equations.

Theorem 2.45 (Thue)**.** *Let $f \in \mathbb{Z}[X]$ be an irreducible polynomial of degree $d \geq 3$ and m a non-zero rational integer. Define $F(X,Y) = Y^d f(X/Y)$. Then the Diophantine equation $F(x,y) = m$ has only finitely many solutions $(x,y) \in \mathbb{Z} \times \mathbb{Z}$.*

The equation $F(x,y) = m$ in Proposition 2.45 is called *Thue equation*. The connexion between Thue equation and Liouville's inequality has been explained in Lemma 2.23 in the special case $\sqrt[3]{2}$; the general case is similar.

Lemma 2.46. *Let α be an algebraic number of degree $d \geq 3$ and minimal polynomial $f \in \mathbb{Z}[X]$, let $F(X,Y) = Y^d f(X/Y) \in \mathbb{Z}[X,Y]$ be the associated homogeneous polynomial. Let $0 < \kappa \leq d$. The following conditions are equivalent:*
(i) There exists $c_1 > 0$ such that, for any $p/q \in \mathbb{Q}$,

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c_1}{q^\kappa}.$$

(ii) There exists $c_2 > 0$ such that, for any $(x,y) \in \mathbb{Z}^2$ with $x > 0$,

$$|F(x,y)| \geq c_2 \; x^{d-\kappa}.$$

In 1921 C.L. Siegel sharpened Thue's result 2.44 by showing that any real number

$$\kappa > \min_{1 \leq j \leq d} \left(\frac{d}{j+1} + j \right)$$

is an irrationality exponent for α. With $j = [\sqrt{d}]$ it follows that $2\sqrt{d}$ is an irrationality exponent for α. Dyson and Gel'fond in 1947 independently refined Siegel's estimate and replaced the hypothesis in Thue's Theorem 2.44 by $\kappa > \sqrt{2d}$. The essentially best possible estimate has been achieved by K.F. Roth in 1955: any $\kappa > 2$ is an irrationality exponent for a real irrational algebraic number α.

Theorem 2.47 (A. Thue, C.L. Siegel, F. Dyson, K.F. Roth 1955)**.** *For any real algebraic number α, for any $\epsilon > 0$, the set of $p/q \in \mathbb{Q}$ with $|\alpha - p/q| < q^{-2-\epsilon}$ is finite.*

It is expected that the result is not true with $\epsilon = 0$ as soon as the degree of α is ≥ 3, which means that it is expected no real algebraic number of degree at least 3 is badly approximable, but essentially nothing is known on the continued fraction of such numbers: we do not know whether there exists an irrational algebraic number which is not quadratic and has bounded partial quotient in its continued fraction expansion, but we do not know either whether there exists a real algebraic number of degree at least 3 whose sequence of partial quotients is not bounded!

A guide to state conjectures is to consider which properties are valid for *almost all numbers*, which means outside a set of Lebesgue measure 0, and to expect that algebraic numbers will share these properties. This guideline should not be followed carelessly: an intersection of subsets of full measure (that means that the complementary has measure 0) may be empty. For instance

$$\bigcap_{x\in\mathbb{R}} \mathbb{R}\setminus\{x\} = \emptyset.$$

Nevertheless, this point of view may yields valid guesses.

The so–called *metrical theory of Diophantine approximation* goes back to Cantor's proof of the existence of transcendental numbers. If you list the algebraic numbers in the interval $[0,1]$, if, for each of them, you write its binary expansion (writing the two expansions if this algebraic number is a rational number with denominator a power of two), then taking the digits on the diagonal yields a number θ such that $1-\theta$ is not in the list, hence θ is transcendental.

It is known from a result by Khinchin (1924) that for almost all real numbers, any $\kappa > 2$ is an irrationality exponent. Hence from this point of view algebraic numbers behave like almost all numbers.

Khinchin's Theorem is much more precise: Denote by $\mathcal{K}$ (like Khinchin) the set of *non-increasing* functions ψ from $\mathbb{R}_{\geq 1}$ to $\mathbb{R}_{>0}$. Set

$$\mathcal{K}_c = \left\{ \Psi\in\mathcal{K}\,;\, \sum_{n\geq 1}\Psi(n) \text{ converges} \right\}, \quad \mathcal{K}_d = \left\{ \Psi\in\mathcal{K}\,;\, \sum_{n\geq 1}\Psi(n) \text{ diverges} \right\}$$

Hence $\mathcal{K} = \mathcal{K}_c \cup \mathcal{K}_d$.

Theorem 2.48 (Khinchin)**.** *Let $\Psi\in\mathcal{K}$. Then for almost all real numbers ξ, the inequality*

$$|q\xi - p| < \Psi(q) \tag{2.49}$$

has

- *only finitely many solutions in integers p and q if $\Psi\in\mathcal{K}_c$*
- *infinitely many solutions in integers p and q if $\Psi\in\mathcal{K}_d$.*

For instance, for any $\epsilon > 0$, the set of irrational real numbers for which the function

$$q \mapsto \frac{1}{q^2(\log q)^{1+\epsilon}} \tag{2.50}$$

is not an irrationality measure has Lebesgue measure 0. One expects that for any irrational algebraic number α, the function 2.50 is an irrationality measure.

However B. Adamczewski and Y. Bugeaud noticed recently (see [38]) that for any $\xi\in\mathbb{R}\setminus\mathbb{Q}$, there exists $\psi\in\mathcal{K}_d$ for which the inequality (2.49) has no solution. Hence no real number behaves generically with respect to Khinchin's Theorem in the divergent case. Also S. Schanuel proved that the set of real numbers which behave like almost all numbers from the point of view of Khinchin's Theorem in

the convergent case is the set of real numbers with bounded partial quotients, and this set has measure 0.

Here is an example of application of Diophantine approximation to transcendental number theory. Let $(u_n)_{n\geq 0}$ be an increasing sequence of integers and let b be a rational integer, $b \geq 2$. We wish to prove that the number

$$\vartheta = \sum_{n\geq 0} b^{-u_n} \tag{2.51}$$

is transcendental. A conjecture of Borel (1950 – see [37]) states that *the digits in the binary expansion of a real algebraic irrational number should be uniformly equidistributed*; in particular the sequence of 1's should not be lacunary.

For sufficiently large n, define

$$q_n = b^{u_n}, \quad p_n = \sum_{k=0}^{n} b^{u_n - u_k} \quad \text{and} \quad r_n = \vartheta - \frac{p_n}{q_n}.$$

Since the sequence $(u_n)_{n\geq 0}$ is increasing, we have $u_{n+h} - u_{n+1} \geq h - 1$ for any $h \geq 1$, hence

$$0 < r_n \leq \frac{1}{b^{u_{n+1}}} \sum_{h\geq 1} \frac{1}{b^{h-1}} = \frac{b}{2^{u_{n+1}}(b-1)} \leq \frac{2}{q_n^{u_{n+1}/u_n}}.$$

Therefore if the sequence $(u_n)_{n\geq 0}$ satisfies

$$\limsup_{n\to\infty} \frac{u_{n+1}}{u_n} = +\infty$$

then ϑ is a Liouville number, and therefore is transcendental. For instance $u_n = n!$ satisfies this condition: hence the number $\sum_{n\geq 0} b^{-n!}$ is transcendental.

Exercise 2.52. Let $(a_n)_{n\geq 0}$ be a bounded sequence of rational integers and $(u_n)_{n\geq 0}$ be an increasing sequence of integers satisfying

$$\limsup_{n\to\infty} \frac{u_{n+1}}{u_n} = +\infty.$$

Assume that the set $\{n \geq 0\ ;\ a_n \neq 0\}$ is infinite.

Define

$$\vartheta = \sum_{n\geq 0} a_n 2^{-u_n}.$$

Show that ϑ is a Liouville number.

Roth's Theorem 2.47 yields the transcendence of the number ϑ in (2.51) under the weaker hypothesis

$$\limsup_{n\to\infty} \frac{u_{n+1}}{u_n} > 2.$$

The sequence $u_n = [2^{\theta n}]$ satisfies this condition as soon as $\theta > 1$. For example the transcendence of the number

$$\sum_{n\geq 0} b^{-3^n}$$

follows from Theorem 2.47.

A stronger result follows from Ridout's Theorem 2.53 below, using the fact that the denominators b^{u_n} are powers of b.

Let S be a set of prime. A rational number is called *a S–integer* if it can be written u/v where all prime factors of the denominator v belong to S. For instance when a, b and m are rational integers with $b \neq 0$, the number a/b^m is a S–integer for S the set of prime divisors of b.

Theorem 2.53 (D. Ridout, 1957)**.** *Let S be a finite set of prime numbers. For any real algebraic number α, for any $\epsilon > 0$, the set of $p/q \in \mathbb{Q}$ with q a S–integer and $|\alpha - p/q| < q^{-1-\epsilon}$ is finite.*

Therefore the condition

$$\limsup_{n\to\infty} \frac{u_{n+1}}{u_n} > 1$$

suffices to imply the transcendence of the sum of the series (2.51). An example is the transcendence of the number

$$\sum_{n\geq 0} b^{-2^n}.$$

This result goes back to A. J. Kempner in 1916.

The theorems of Thue–Siegel–Roth and Ridout are very special cases of Schmidt's subspace Theorem (1972) together with its p-adic extension by H.P. Schlickewei (1976). We state do not state it in full generality but we give only two special cases.

For $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{Z}^m$, define $|\mathbf{x}| = \max\{|x_1|, \ldots, |x_m|\}$.

Theorem 2.54 (W.M. Schmidt (1970): simplified form)**.** *For $m \geq 2$ let $L_1, \ldots, L_m$ be independent linear forms in m variables with algebraic coefficients. Let $\epsilon > 0$. Then the set*

$$\{\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{Z}^m \ ; \ |L_1(\mathbf{x}) \cdots L_m(\mathbf{x})| \leq |\mathbf{x}|^{-\epsilon}\}$$

is contained in the union of finitely many proper subspaces of $\mathbb{Q}^m$.

Thue–Siegel–Roth's Theorem 2.47 follows from Theorem 2.54 by taking

$$m = 2, \quad L_1(x_1, x_2) = x_1, \quad L_2(x_1, x_2) = \alpha x_1 - x_2.$$

A $\mathbb{Q}$-vector subspace of $\mathbb{Q}^2$ which is not $\{0\}$ not $\mathbb{Q}^2$ (that is *a proper subspace* is of the generated by an element $(p_0, q_0) \in \mathbb{Q}^2$. There is one such subspace

with $q_0 = 0$, namely $\mathbb{Q} \times \{0\}$ generated by $(1, 0)$, the other ones have $q_0 \neq 0$. Mapping such a rational subspace to the rational number p_0/q_0 yields a 1 to 1 correspondence. Hence Theorem 2.54 says that there is only a finite set of exceptions p/q in Roth's Theorem.

For x a non–zero rational number, write the decomposition of x into prime factors

$$x = \prod_p p^{v_p(x)},$$

where p runs over the set of prime numbers and $v_p(x) \in \mathbb{Z}$ (with only finitely many $v_p(x)$ distinct from 0), and set

$$|x|_p = p^{-v_p(x)}.$$

For $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{Z}^m$ and p a prime number, define $|\mathbf{x}| = \max\{|x_1|_p, \ldots, |x_m|_p\}$.

Theorem 2.55 (Schmidt's Subspace Theorem)**.** *Let $m \geq 2$ be a positive integer, S a finite set of prime numbers. Let $L_1, \ldots, L_m$ be independent linear forms in m variables with algebraic coefficients. Further, for each $p \in S$ let $L_{1,p}, \ldots, L_{m,p}$ be m independent linear forms in m variables with rational coefficients. Let $\epsilon > 0$. Then the set of $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{Z}^m$ such that*

$$|L_1(\mathbf{x}) \cdots L_m(\mathbf{x}) \prod_{p \in S} |L_{1,p}(\mathbf{x}) \cdots L_{m,p}(\mathbf{x})|_p \leq |\mathbf{x}|^{-\epsilon}$$

is contained in the union of finitely many proper subspaces of $\mathbb{Q}^m$.

Ridout's Theorem 2.53 is a consequence of Schmidt's subspace Theorem: in Theorem 2.55 take $m = 2$,

$$\begin{aligned} L_1(x_1, x_2) &= L_{1,p}(x_1, x_2) = x_1, \\ L_2(x_1, x_2) &= \alpha x_1 - x_2, \quad L_{2,p}(x_1, x_2) = x_2. \end{aligned}$$

For $(x_1, x_2) = (b, a)$ with b a S–integer and $p \in S$, we have

$$\begin{aligned} &|L_1(x_1, x_2)| = b, \quad |L_2(x_1, x_2)| = |b\alpha - a|, \\ &|L_{1p}(x_1, x_2)|_p = |b|_p, \quad |L_{2,p}(x_1, x_2)|_p = |a|_p \leq 1. \end{aligned}$$

and

$$\prod_{p \in S} |b|_p = b^{-1}$$

since b is a S–integer.

Problem of effectivity.
`Content of the lecture:` Sketch of proof of Thue's inequality, of Roth's refinement. Upper bound for the number of exceptions in Roth's Theorem, for the number of exceptional subspaces in Schmidt's Theorem. Effective refinement of Liouville's inequality, consequences to Diophantine equations: Baker's method.

2.2.10 Hilbert's seventh problem and its development.

Euler question, Hilbert's 7th problem: transcendence of α^β, of quotients of logartithms. Examples: $2^{\sqrt{2}}$, e^π.
Weierstraß: example of transcendental entire functions with many algebraic values. Interpolation series (see Exercise 2.56).
Polya (1914): integer valued entire functions — 2^z is the "smallest" entire transcendental function mapping the positive integers to rational integers. More precisely, *if* $f(n) \in \mathbb{Z}$ *for all* $n \in \mathbb{Z}_{\geq 0}$, *then*

$$\limsup_{R\to\infty} 2^{-R}|f|_R \geq 1.$$

Interpolation series: write

$$f(z) = f(\alpha_1) + (z-\alpha_1)f_1(z), \quad f_1(z) = f(\alpha_2) + (z-\alpha_2)f_2(z), \dots$$

We deduce an expansion

$$f(z) = a_0 + a_1(z-\alpha_1) + a_2(z-\alpha_1)(z-\alpha_2) + \cdots$$

with

$$a_0 = f(\alpha_1), \quad a_1 = f_1(\alpha_2), \dots, \quad a_n = f_n(\alpha_{n+1}).$$

Exercise 2.56. Let $x, z, \alpha_1, \dots, \alpha_n$ be complex numbers with $x \notin \{z,\ \alpha_1, \dots, \alpha_n\}$.
a) Check

$$\frac{1}{x-z} = \frac{1}{x-\alpha_1} + \frac{z-\alpha_1}{x-\alpha_1}\cdot\frac{1}{x-z}.$$

b) Deduce the next formula due to Hermite:

$$\frac{1}{x-z} = \sum_{j=0}^{n-1} \frac{(z-\alpha_1)(z-\alpha_2)\cdots(z-\alpha_j)}{(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{j+1})} + \frac{(z-\alpha_1)(z-\alpha_2)\cdots(z-\alpha_n)}{(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)}\cdot\frac{1}{x-z}.$$

c) Let $\mathcal{D}$ be an open disc containing $\alpha_1, \dots, \alpha_n$, let $\mathcal{C}$ denote the circumference of $\mathcal{D}$, let $\mathcal{D}'$ be an open disc containing the closure of $\mathcal{D}$ and let f be an analytic function in $\mathcal{D}'$. Define

$$A_j(z) = \frac{1}{2i\pi}\int_{\mathcal{C}} \frac{F(x)dx}{(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{j+1})} \qquad (0 \leq j \leq n-1)$$

and

$$R_n(z) = (z-\alpha_1)(z-\alpha_2)\cdots(z-\alpha_n)\cdot\frac{1}{2i\pi}\int_{\mathcal{C}} \frac{F(x)dx}{(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)(x-z)}.$$

Check the following formula, known as Newton interpolation expansion: for any $z \in \mathcal{D}'$,

$$f(z) = \sum_{j=0}^{n-1} A_j(z-\alpha_1)\cdots(z-\alpha_j) + R_n(z).$$

G.H. Hardy, G. Pólya, D. Sato, E.G. Straus, A. Selberg, Ch. Pisot, F. Carlson, F. Gross,. . . .
Gel'fond (1929): same problem for $\mathbb{Z}[i]$: A transcendental entire function f such that $f(a+ib) \in \mathbb{Z}[i]$ for all $a+ib \in \mathbb{Z}[i]$ satisfies

$$\limsup_{R\to\infty} \frac{1}{R^2} \log |f|_R \geq \gamma.$$

Weierstraß sigma function (Hadamard canonical product for $\mathbb{Z}[i]$): $\gamma \leq \pi/2$.
A.O. Gel'fond: $\gamma = 10^{-45}$.
Fukasawa, D.W. Masser, F. Gramain (1981): $\gamma = \pi/(2e)$.
Connection with $e^\pi = 23,140\,692\,632\,779\,269\,005\,729\,086\,367\ldots$
Siegel (1929): Dirichlet's box principle, lemma of Thue–Siegel, application to transcendence (elliptic curves).
Gel'fond–Schneider's Theorem in 1934.
"Criteria" for analytic functions satisfying differential equations: Schneider, Lang. Statement of the Schneider–Lang Theorem. Corollaries: Hermite–Lindemann, Gel'fond–Schneider.
Mahler's method:

$$f(z) = \sum_{n\geq 0} 2^{-n(n-1)} z^n, \quad f(z) = 1 + zf(z/4), \quad f(1/2) = \sum_{n\geq 0} 2^{-n^2}.$$

Also $f(z) = \sum_{n\geq 0} z^{d^n}$, for $d \geq 2$, satisfies the functional equation $f(z^d)+z = f(z)$ for $|z| < 1$.
Baker's Theorem.
Algebraic independence: Gel'fond's criterion, algebraic independence of $2^{\sqrt[3]{2}}$ and $2^{\sqrt[3]{4}}$. Gel'fond–Schneider problem on the transcendence degree of $\mathbb{Q}(\alpha^{\beta_1}, \ldots, \alpha^{\beta_m})$ (see Exercise 2.57).
Algebraic independence of π and $\Gamma(1/4)$: Chudnovskii (1978). Algebraic independence of π, e^π and $\Gamma(1/4)$: Nesterenko (1996).
Schanuel's conjecture. Consequences.
Auxiliary functions, zero estimates, Laurent's interpolation determinants. Arakelov Theory (J-B. Bost): slope inequalities.

Exercise 2.57. Let α be a non-zero algebraic number and let ℓ be any non–zero number such that $e^\ell = \alpha$. For $z \in \mathbb{C}$ define α^z as $\exp\{z\ell\}$ (which is the same as $e^{z\ell}$). Show that the following statements are equivalent.
(i) For any irrational algebraic complex number β, the transcendence degree over $\mathbb{Q}$ of the field

$$\mathbb{Q}\big\{\alpha^{\beta^i}\ ;\ i \geq 1\big\}$$

is $d-1$ where d is the degree of β.
(ii) For any algebraic numbers $\beta_1, \ldots, \beta_m$ such that the numbers $1, \beta_1, \ldots, \beta_m$ are $\mathbb{Q}$-linearly independent, the numbers $\alpha^{\beta_1}, \ldots, \alpha^{\beta_m}$ are algebraically independent.

`Remark:` that both statements are true is a conjecture of Gel'fond and Schneider. It is not yet proved.

Exercise 2.58. Deduce from Schanuel's Conjecture the following statement: the numbers

$$\begin{aligned} &e,\ \pi,\ e^{\pi},\ \pi^{e},\ e^{e},\ \pi^{\pi},\ (\log 2)^{\log 3},\ (\log 3)^{\log 2},\ \pi^{\log 2},\ \pi^{\log 3}, \\ &\log \pi,\ \log\log \pi,\ \log\log 2,\ \log\log 3 \end{aligned} \tag{2.59}$$

are algebraically independent.

References

[1] M. Aigner & G.M. Ziegler – *Proofs from THE BOOK*, Springer (2001).

[2] J.-P. Allouche & J. Shallit – *Automatic sequences, Theory, applications, generalizations*, Cambridge University Press, Cambridge, 2003,

[3] N. Bergeron – *Sur la topologie de certains espaces provenant de constructions arithmétiques.*

[4] N. Bourbaki – *Eléments de Mathématique*, Topologie Générale, Herman 1974, Chap. VII, § 1, N°1, Prop. 2;

[5] Y. Bugeaud – *Approximation by algebraic numbers*, Cambridge Tracts in Mathematics, vol. 160, Cambridge University Press, Cambridge, 2004.

[6] J.W.S. Cassels– *An introduction to Diophantine approximation.* Cambridge Tracts in Mathematics and Mathematical Physics, **45**. Cambridge University Press, New York, 1957.

[7] H. Cohn – *A short proof of the simple continued fraction expansion of* e, Math Monthly **113** January 2006, 57–62 = MathArxiv NT/061660 v2 January 30 2006.

[8] J. Cosgrave – *New Proofs of the Irrationality of* e^2 *and* e^4, unpublished – see http://services.spd.dcu.ie/johnbcos/esquared.htm

[9] D.S. Dummit & R.M. Foote – *Abstract Algebra*, Prentice Hall 1991, 1999.

[10] L. Euler – *De fractionibus continuis dissertatio*, Commentarii Acad. Sci. Petropolitanae, 9 (1737), 1744, p. 98–137; Opera Omnia Ser. I vol. 14, Commentationes Analyticae, p. 187–215.

[11] N. I. Fel′dman & Y. V. Nesterenko – *Transcendental numbers*, in *Number Theory, IV*, Encyclopaedia Math. Sci., vol. **44**, Springer, Berlin, 1998, p. 1–345.

[12] N.I. Fel'dman & A.B. Šidlovskiĭ – *The development and present state of the theory of transcendental numbers*, (Russian) Uspehi Mat. Nauk **22** (1967) no. 3 (135) 3–81; Engl. transl. in Russian Math. Surveys, **22** (1967), no. 3, 1–79.

[13] S. Fischler – *Irrationalité de valeurs de zêta, (d'après Apéry, Rivoal, ...)*, Sém. Bourbaki 2002-2003, N° 910 (Novembre 2002). Astérisque **294** (2004), 27-62.
http://www.math.u-psud.fr/∼fischler/publi.html

[14] Bùi Xuân Hải – *Lý Thuyết Trường & Galois*, Nha xuat ban Dai hoc Quoc gia NXB ĐHQG Tp HCM 2007.

[15] Bùi Xuân Hải – *Nhóm Tuyến Tính* (chuyên đề cao học), NXB ĐHQG Tp HCM 2007.

[16] G.H. Hardy & A.M. Wright, – *An Introduction to the Theory of Numbers*, Oxford Sci. Publ., 1938.

[17] C. Hermite – *Sur la fonction exponentielle*, C. R. Acad. Sci. Paris, **77** (1873), 18–24; 74–79; 226–233; 285–293; *Oeuvres*, Gauthier Villars (1905), III, 150–181. See also *Oeuvres* III, 127–130, 146–149, and *Correspondance Hermite-Stieltjes*, II, lettre 363, 291–295.

[18] Hua Loo Keng & Wang Yuan – *Application of number theory to numerical analysis*, Springer Verlag (1981).

[19] A. Ya. Khinchin – *Continued fractions*, Dover Publications Inc., third edition (1997).

[20] H. Lambert - *Mémoire sur quelques propriétés remarquables des quantités transcendantes circulaires et logarithmiques*, Mémoires de l'Académie des Sciences de Berlin, 17 (1761), 1768, p. 265–322; lu en 1767; Math. Werke, t. II.

[21] S. Lang – *Algebra*, Third edition. Addison-Wesley Publishing Co., Reading, Mass., 1993. Trad. franç. *Algèbre*, Dunod, 2004.

[22] H.W. Lenstra Jr– *Solving the Pell Equation*, Notices of the A.M.S. **49** (2) (2002) 182–192.

[23] J. Liouville – *Sur l'irrationalité du nombre* $e = 2,718\ldots$, J. Math. Pures Appl. (1) **5** (1840), p. 192.

[24] J. Liouville – *Addition à la note sur l'irrationalité du nombre e*, J. Math. Pures Appl. (1) **5** (1840), p. 193–194.

[25] Yu. V.Ñesterenko & M. Waldschmidt – *On the approximation of the values of exponential function and logarithm by algebraic numbers.* (In russian) Mat. Zapiski, **2** *Diophantine approximations, Proceedings of papers dedicated to the memory of Prof. N. I. Feldman*, ed. Yu. V. Nesterenko, Centre for applied research under Mech.-Math. Faculty of MSU, Moscow (1996), 23–42.
http://fr.arXiv.org/abs/math/0002047

[26] I. Niven – *Irrational numbers*, Carus Math. Monographs **11** (1956).

[27] Benoît Rittaud – *Le fabuleux destin de* $\sqrt{2}$, Éditions Le Pommier (2006).

[28] T. Rivoal – *Applications arithmétiques de l'interpolation lagrangienne*, IJNT, to appear.

[29] W. M. Schmidt – *Diophantine approximation*, Lecture Notes in Mathematics, vol. 785, Springer-Verlag, Berlin, 1980.

[30] M.R. Schroeder – *Number theory in science and communication, with applications in cryptography, physics, digital information, computing and self similarity*, Springer series in information sciences **7** 1986. 4th ed. (2006) 367 p.

[31] J. Shallit – *Real numbers with bounded partial quotients: a survey*, L'Enseignement Mathématique, **38** (1992), 151-187.

[32] S.A. Shirali – *Continued fraction for e*, Resonance, vol. **5** N°1, Jan. 2000, 14–28.
http://www.ias.ac.in/resonance/

[33] C.L. Siegel – *Transcendental Numbers*, Annals of Mathematics Studies, **16**. Princeton University Press, Princeton, N. J., 1949.

[34] Jonathan Sondow – *Criterion for irrationality of Euler's constant*, (2002)
http://xxx.lanl.gov/pdf/math.NT/0209070
http://home.earthlink.net/∼jsondow/

[35] M. Waldschmidt – *Nombres transcendants*, Lecture Notes in Mathematics, Vol. **402**, Springer-Verlag (1974). See Chap. 5.

[36] M. Waldschmidt, *Open Diophantine Problems*, Moscow Mathematical Journal **4** N°1, 2004, 245–305.

[37] M. Waldschmidt – *Words and Transcendence*. To appear
http://www.math.jussieu.fr/∼miw/articles/pdf/WordsTranscendence.pdf

[38] M. Waldschmidt – *Report on some recent progress in Diophantine approximation*. To appear
http://www.math.jussieu.fr/∼miw/articles/pdf/miwLangMemorialVolume.pdf

[39] A. Weil – *Number theory. An approach through history. From Hammurapi to Legendre,* Birkhäuser Boston, Inc., Boston, Mass., (1984) 375 pp.

[40] J.C. Yoccoz– *Conjugaison différentiable des difféomorphismes du cercle dont le nombre de rotation vérifie une condition diophantienne*. Ann. scient. Éc. Norm. Sup. 4è série, t. **17** (1984), 333-359.

There is a also good collection of Lecture Notes which are available on the internet. A list can be found at the URL
http://www.numbertheory.org/ntw/lecture_notes.html.
See for instance
Algebraic Number Theory and commutative algebra, Lecture Notes by Robert Ash
and
Course Notes by Jim Milne: *Algebraic number theory.*

http://www.math.jussieu.fr/∼miw/coursHCMUNS2007.html