

Chapter 1

Irrationality and diophantine approximation

In this introductory chapter, we prove that the numbers \sqrt{d} , e and π are irrational, as well as the values of the Tschakaloff function (section 1.4). These four proofs allow us to identify the notion of diophantine approximation and to link it with irrationality problems (section 1.5). We conclude with some methodological remarks (section 1.6).

1.1 Irrationality of \sqrt{d}

Theorem 1.1 *Let $d \in \mathbb{N}$. Assume that d is not a perfect square. Then \sqrt{d} is irrational.*

Proof Assume on the contrary that \sqrt{d} is a rational number. Then $\sqrt{d} = a/b$, where a and b are coprime integers. Squaring this equality yields $b^2d = a^2$. As d is not a perfect square, there exists a prime p and an integer k such that $d = p^{2k+1}\delta$, with $p \nmid \delta$. Then $p^{2k+1} \mid a^2$ and therefore $p^{k+1} \mid a$, so that $a = p^{k+1}\alpha$. Hence $b^2\delta = p\alpha^2$. The prime number p divides $b^2\delta$ but does not divide δ . Therefore $p \mid b^2$, whence $p \mid b$. So $p \mid a$ and $p \mid b$, contradiction because a and b are coprime. Theorem 1.1 is proved.

Corollary 1.1 If $d \in \mathbb{N}$ is not a perfect square, the numbers 1 and \sqrt{d} are linearly independent over \mathbb{Q} . In other words, if $p, q \in \mathbb{Q}$ and $p + q\sqrt{d} = 0$, then $p = q = 0$.

Proof If q was different from zero, the equality $p + q\sqrt{d} = 0$ would imply $\sqrt{d} = -p/q \in \mathbb{Q}$, contradiction with theorem 1.1. Therefore $q = 0$ and $p = 0$.

We will use corollary 1.1 repeatedly in chapters 4 and 5.

1.2 Irrationality of e

Theorem 1.2 e is irrational.

Proof For every natural integer n , we can write

$$e = \sum_{k=0}^n \frac{1}{k!} + R_n, \quad \text{with } R_n = \sum_{k=n+1}^{+\infty} \frac{1}{k!}. \quad (1.1)$$

It is clear that $R_n > 0$. Moreover,

$$\begin{aligned} R_n &= \frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \frac{1}{(n+3)!} + \dots \\ R_n &= \frac{1}{(n+1)!} \left(1 + \frac{1}{n+2} + \frac{1}{(n+2)(n+3)} + \frac{1}{(n+2)(n+3)(n+4)} + \dots \right) \\ R_n &< \frac{1}{(n+1)!} \left(1 + \frac{1}{2} + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^3 + \dots \right) = \frac{2}{(n+1)!}. \end{aligned}$$

Therefore (1.1) yields

$$0 < n!e - n! \sum_{k=0}^n \frac{1}{k!} < \frac{2}{n+1}. \quad (1.2)$$

We argue again by *reductio ad absurdum*. Assume that $e = a/b$, where a and b are natural integers. Denote $\alpha_n = n! \sum_{k=0}^n \frac{1}{k!}$. Then $\alpha_n \in \mathbb{N}$, and (1.2)

$$\text{yields } 0 < n!a - b\alpha_n < \frac{2b}{n+1}.$$

This implies that the integer $\beta_n = n!a - b\alpha_n$ is not zero and vanishes when n tends to infinity. This is impossible, because *the absolute value of a non zero integer is always greater than 1*. This proves theorem 1.2.

1.3 Irrationality of π

Theorem 1.3 π is irrational.

Proof Let $P(x)$ be any polynomial of degree $2n$. Put

$$F(x) = P(x) - P''(x) + P^{(4)}(x) - \dots + (-1)^n P^{(2n)}(x).$$

We observe that $P(x) \sin x = (F'(x) \sin x - F(x) \cos x)'$, which yields at once *Hermite's formula*:

$$\int_0^\pi P(x) \sin x dx = F(0) + F(\pi). \tag{1.3}$$

Assume that $\pi = a/b$, $a, b \in \mathbb{N}$, and apply Hermite formula with

$$P(x) = \frac{1}{n!} x^n (a - bx)^n.$$

Denote $I_n = \int_0^\pi P(x) \sin x dx$.

Then $I_n > 0$ because $P(x) \sin x$ is a continuous, non negative and non identically zero function on $[0, \pi]$. Moreover, $x(a - bx) \leq a^2/4b$ on

$[0, \pi]$, whence $I_n \leq \frac{1}{n!} \pi \left(\frac{a^2}{4b}\right)^n$. Therefore $\lim_{n \rightarrow +\infty} I_n = 0$. But it can be

proved (exercise 1.1) that $F(0) \in \mathbb{Z}$ and $F(\pi) \in \mathbb{Z}$ for every $n \in \mathbb{N}$.

Thus $I_n \in \mathbb{Z}$ for every $n \in \mathbb{N}$. Hence the *positive* sequence I_n vanishes at infinity, which is impossible. Therefore π is irrational.

1.4. Irrationality of the values of the Tschakaloff function

Let $q \in \mathbb{C}$, $q > 1$. The *Tschakaloff function* is defined by

$$T_q(x) = \sum_{n=0}^{+\infty} \frac{x^n}{q^{\frac{n(n+1)}{2}}}, \quad \forall x \in \mathbb{C}. \tag{1.4}$$

It satisfies the functional equation

$$T_q(qx) = 1 + xT_q(x). \tag{1.5}$$

We will prove the following result.

Theorem 1.4 Let $q \in \mathbb{Z}$, $|q| \geq 2$. Then $T_q(x)$ is irrational for every $x \in \mathbb{Q}^*$.

We need the following lemma, which will be also useful in the study of Padé approximants (chapter 8).

Lemma 1.1 Let \mathbb{K} be any subfield of \mathbb{C} , and let $f(x) = \sum_{n=0}^{+\infty} a_n x^n$, with $a_n \in \mathbb{K}$ for every $n \in \mathbb{N}$ and radius of convergence $R > 0$. Assume p, q, r are 3 natural integers satisfying $p < r \leq p + q + 1$. Then there exist $P, Q \in \mathbb{K}[x]$, $Q \neq 0$, and a series $g(x) = \sum_{n=0}^{+\infty} b_n x^n$, $|x| < R$, such that $\deg P \leq p$, $\deg Q \leq q$ and

$$Q(x)f(x) + P(x) = x^r g(x). \quad (1.6)$$

The proof of lemma 1.1 is left as an exercise (exercise 1.2).

We now prove theorem 1.4. Let $x = \alpha\beta$, $(\alpha, \beta) \in \mathbb{Z}^2$. Assume that $T_q(x) = \mu/\nu$, $(\mu, \nu) \in \mathbb{Z}^2$. An easy induction using the functional equation

$$(1.5) \text{ shows that } T_q\left(\frac{x}{q^n}\right) = \frac{A_n}{\nu \alpha^n} \text{ for every } n \in \mathbb{N}, \text{ where } A_n \in \mathbb{Z}.$$

Let ρ be a fixed integer, such that $|\alpha q^\rho| < 1$.

We use lemma 1.1, with $\mathbb{K} = \mathbb{Q}$, $f(x) = T_q(x)$, $p = q = 2\rho$, $r = 3\rho$. Then the polynomials P and Q have rational coefficients. However, if we multiply (1.6) by the LCM of these coefficients, we see that we may assume that P and Q have integer coefficients. Hence we can write

$$Q(x)T_q(x) + P(x) = x^{3\rho} g(x), \quad (1.7)$$

where $P, Q \in \mathbb{Z}[x]$, $\deg Q \leq 2\rho$, $\deg P \leq 2\rho$, $Q \neq 0$.

But g is not identically zero : if it was the case, T_q would be a rational fraction because of (1.7), and therefore a polynomial because it is defined on \mathbb{C} , which is impossible considering its Taylor expansion (1.4). Therefore at least one of the Taylor coefficients of g is not zero. Hence there exist an integer $\sigma \geq 0$ and a function h such that

$$Q(x)T_q(x) + P(x) = x^{3\rho+\sigma} h(x), \quad h(0) \neq 0. \quad (1.8)$$

Replace $x = \alpha\beta$ by x/q^n in (1.8), multiply by $v\alpha^n\beta^{2\rho}q^{2\rho n}$, and denote by B_n the common value of both sides of the equation

$$\begin{aligned} B_n &= \frac{v\alpha^{3\rho+\sigma}}{\beta^{\rho+\sigma}} \left(\frac{\alpha}{q^{\rho+\sigma}} \right)^n h \left(\frac{\alpha}{\beta q^n} \right) \\ &= \left(\beta^{2\rho} q^{2\rho n} Q \left(\frac{\alpha}{\beta q^n} \right) \right) \left(v\alpha^n T_q \left(\frac{\alpha}{\beta q^n} \right) \right) + v\alpha^n \left(\beta^{2\rho} q^{2\rho n} P \left(\frac{\alpha}{\beta q^n} \right) \right). \end{aligned} \quad (1.9)$$

As $\left(\beta^{2\rho} q^{2\rho n} P \left(\frac{\alpha}{\beta q^n} \right) \right)$, $v\alpha^n T_q \left(\frac{\alpha}{\beta q^n} \right)$, and $\left(\beta^{2\rho} q^{2\rho n} Q \left(\frac{\alpha}{\beta q^n} \right) \right) \in \mathbb{Z}$, we see

that $B_n \in \mathbb{Z}$. Moreover, $B_n \sim \frac{v\alpha^{3\rho+\sigma}}{\beta^{\rho+\sigma}} \left(\frac{\alpha}{q^{\rho+\sigma}} \right)^n h(0)$, which implies that $\lim_{n \rightarrow +\infty} B_n = 0$ because $|\alpha/q^\rho| < 1$, and also that $B_n \neq 0$ as $\alpha \neq 0$ and $h(0) \neq 0$. Again, we have constructed a sequence of non zero integers which vanishes at infinity. This proves theorem 1.4.

1.5 Diophantine approximation

Constructing a *diophantine approximation* of a given real number α means finding a sequence of rational numbers P_n/Q_n and a function f vanishing at infinity, such that

$$\left| \alpha - \frac{P_n}{Q_n} \right| \leq f(Q_n), \quad \forall n \in \mathbb{N}. \quad (1.10)$$

Observe that we have proved the irrationality of the numbers e and $T_q(\alpha/\beta)$ by using diophantine approximations.

Indeed, in the case of e , we can write (1.2) as

$$0 < e - \frac{P_n}{Q_n} < \frac{2}{(n+1)Q_n} \leq \frac{2}{Q_n}, \quad (1.11)$$

where $P_n = n! \sum_{k=0}^n \frac{1}{k!}$ and $Q_n = n!$.

In the case of $T_q(\alpha/\beta)$, it is not so clear. One has to observe that

$$T_q \left(\frac{\alpha}{\beta q^n} \right) = \frac{k_n}{\alpha^n} T_q \left(\frac{\alpha}{\beta} \right) + \frac{\ell_n}{\alpha^n},$$

where $(k_n, \ell_n) \in \mathbb{Z}^2$ (induction by using (1.5)). Hence (1.9) yields

$$T_q \left(\frac{\alpha}{\beta} \right) + \frac{P_n}{Q_n} \leq \frac{c}{Q_n} \left(\frac{\alpha}{q^{\rho+\sigma}} \right)^n \leq \frac{c}{Q_n} \quad (1.12)$$

with $Q_n = k_n \beta^{2\rho} q^{2\rho n} Q(\alpha/\beta q^n)$, $P_n = \alpha^n \beta^{2\rho} q^{2\rho n} P(\alpha/\beta q^n) + \ell_n Q_n/k_n$, and $c = \max_{n \in \mathbb{N}} \alpha^{3\rho+\sigma} \beta^{-\rho-\sigma} h(\alpha \beta^{-1} q^{-n})$.

The difference between e and $T_q(\alpha/\beta)$ consists in the fact that the diophantine approximation given by par (1.11) is an *explicit* one (one can compute explicitly P_n and Q_n as functions of n), whereas the one given by (1.12) is not. In this last case, P_n and Q_n are expressed by using polynomials P and Q , and lemma 1.1 asserts the *existence* of these polynomials, but gives no way how to compute them.

However, in both cases, we get an irrationality result, because after multiplying by Q_n , the product $Q_n f(Q_n)$ vanishes at infinity. We say we have obtained a *good diophantine approximation*, and can state the following result.

Theorem 1.5 *Let $\alpha \in \mathbb{R}$. Assume there exists a sequence P_n/Q_n of rational numbers satisfying*

$$\forall n \in \mathbb{N}, \quad 0 < \left| \alpha - \frac{P_n}{Q_n} \right| \leq \frac{\varepsilon(n)}{Q_n}, \quad \text{with } \lim_{n \rightarrow +\infty} \varepsilon(n) = 0.$$

Then α is irrational.

Proof See exercise 1.3.

The following theorem has been proved by Dirichlet (1805-1859). It shows that, for a given irrational α , there exist good diophantine approximations.

Theorem 1.6 *Let $\alpha \in \mathbb{R}$. Assume α to be irrational. Then there exists an infinite sequence of rational numbers P_n/Q_n satisfying*

$$0 < \left| \alpha - \frac{P_n}{Q_n} \right| \leq \frac{1}{Q_n^2}, \quad \forall n \in \mathbb{N}.$$

For the proof of theorem 1.6, we will need the following lemma.

Lemma 1.2 Assume α is irrational. Then, for every integer $Q > 1$, one can find $p/q \in \mathbb{Q}$ such that $1 \leq q < Q$ and $0 < |q\alpha - p| \leq \frac{1}{Q}$.

Proof of lemma 1.2 Denote by $[\alpha]$ the integral part of α , and consider the $Q+1$ numbers $0, 1, \alpha - [\alpha], 2\alpha - [2\alpha], \dots, (Q-1)\alpha - [(Q-1)\alpha]$. All these numbers belong to the interval $[0,1]$, and all are of the form $a\alpha + b$, a and b integers, $0 \leq a \leq Q-1$. We now use the *pigeon-hole principle*. We divide the interval $[0,1]$ into Q sub-intervals, namely $[0,1/Q], [1/Q,2/Q], \dots, [(Q-1)/Q,1]$. Then at least two of the above $Q+1$ numbers belong to the *same* sub-interval (try to put the $Q+1$ numbers into the Q intervals). Denote these two numbers by $\xi_1 = a_1\alpha + b_1$ and $\xi_2 = a_2\alpha + b_2$, with $0 \leq a_1 \leq Q-1$, $0 \leq a_2 \leq Q-1$, and $a_1 \neq a_2$ (because $a_1 = a_2$ implies $a_1 = a_2 = 0$, that is $\xi_1 = 0$ and $\xi_2 = 1$, which is impossible). We can assume that $a_1 > a_2$. By the choice of ξ_1 and ξ_2 , $|\xi_1 - \xi_2| = |(a_1 - a_2)\alpha + b_1 - b_2| \leq 1/Q$, with $0 < a_1 - a_2 \leq Q-1$, which proves lemma 1.2.

We now prove theorem 1.6 by induction. Choose an arbitrary integer $Q > 1$. By lemma 1.2, we can find a rational number P_1/Q_1 such that $0 < |\alpha - P_1/Q_1| \leq 1/QQ_1$ and $1 \leq Q_1 < Q$. Hence $0 < |\alpha - P_1/Q_1| < 1/Q^2$.

Now we use again lemma 1.2, by choosing Q such that $Q^{-1} < |\alpha - P_1/Q_1|$. We can find a rational number P_2/Q_2 satisfying $1 \leq Q_2 < Q$ and $0 < |\alpha - P_2/Q_2| \leq 1/QQ_2 < 1/Q^2$. Moreover,

$$\left| \frac{P_1}{Q_1} - \frac{P_2}{Q_2} \right| \geq \left| \alpha - \frac{P_2}{Q_2} \right| - \left| \alpha - \frac{P_1}{Q_1} \right| \neq 0$$

since $|\alpha - P_1/Q_1| > 1/Q$ and $|\alpha - P_2/Q_2| \leq 1/QQ_2 \leq 1/Q$.

By induction we obtain an infinite sequence of rational numbers P_n/Q_n satisfying $|\alpha - P_n/Q_n| < 1/Q^n$, which proves theorem 1.6.

Remark 1.1 Theorem 1.6 asserts the existence of the sequence P_n/Q_n , but gives no way how to compute it. The theory of regular continued fractions (formula (4.8)) will enable us to get an explicit result.

1.6 Methodological remarks

We have used, in this chapter, three methods worth describing.

For proving the irrationality of \sqrt{d} , we have argued by *reductio ad absurdum*. Assuming that $\sqrt{d} = a/b$, we have proved that $\sqrt{d} = a'/b'$, with $a' < a$, $b' < b$. From here, there are two possibilities:

- a. Use the fact that the starting point was minimal. In our proof, we have assumed a/b to be irreducible.
- b. Alternatively, consider that, starting from a given value a , we construct a decreasing sequence $a > a' > a'' > \dots$ of *positive integers*, which is clearly impossible. This last process is called the *descent method*.

For proving the irrationality of e , π and $T_q(\alpha/\beta)$, we have constructed a *sequence of positive integers vanishing at infinity*, which is impossible. Generally, the most difficult part in this sort of proof, which forms the basis of transcendence proofs (chapter 12), consists in proving that no term of this sequence can be zero.

Finally, we have used the *pigeon-hole principle*: if $n+1$ pigeons nest in n pigeon-holes, then at least 2 pigeons have to nest in the same hole. A consequence of this principle is the following result.

If $(u_n)_{n \in \mathbb{N}}$ is a bounded sequence of integers, there exist two integers n and p , $n \neq p$, such that $u_n = u_p$.

Exercises

1.1 With the notations of theorem 1.3, prove that $P(0) = P'(0) = \dots = P^{(n-1)}(0) = 0$. Deduce that $F(0) \in \mathbb{Z}$ and $F(\pi) \in \mathbb{Z}$.

1.2 Prove lemma 1.1.

1.3 Prove theorem 1.5.

1.4 Prove that $\alpha = \sqrt[3]{2} + \sqrt{5}$ is irrational.

1.5 Prove that $\beta = \log_{10} 2$ is irrational.

1.6 Let $P(x) = a_0 + a_1x + \dots + a_nx^n$, with $a_n \neq 0$, be a polynomial with integer coefficients. Let $r = p/q$, p and q coprimes and not zero, a rational root with multiplicity d of $P(x)$. Prove that q^d divides a_n .

Application: Prove that $\cos \frac{\pi}{n}$ is irrational for every $n \geq 4$.

1.7 Let $m \in \mathbb{Z}$, $m \geq 2$. Prove that $\sum_{n=0}^{+\infty} \frac{1}{m^{n^2}}$ is irrational.

Give two different proofs.

1.8 An irrational number α is said to be *quadratic* if there exist integers a, b, c with $ac \neq 0$, such that $a\alpha^2 + b\alpha + c = 0$.

1) Prove that the *golden number* $\Phi = (1 + \sqrt{5})/2$ is quadratic.

2) Prove that e is not quadratic.

1.9 The *Fermat numbers* F_n are defined by $F_n = 2^{2^n} + 1$. Our aim is

to prove that $\chi = \sum_{n=0}^{+\infty} \frac{1}{F_n}$ is irrational. We define, for $|x| < 1$,

$$f(x) = \sum_{n=0}^{+\infty} \frac{x^{2^n}}{1 - x^{2^n}}, \quad g(x) = \sum_{n=0}^{+\infty} \frac{x^{2^n}}{1 + x^{2^n}}.$$

1) Prove that $f(x) - g(x) = 2 \left(f(x) - \frac{x}{1-x} \right)$.

2) Prove that $f(1/2)$ is irrational.

3) Deduce that χ is irrational.

1.10 For $a \in \mathbb{N}$, let $f_a(x) = \sum_{n=0}^{+\infty} (1+a)(1+aq)\dots(1+aq^{n-1})x^n q^{-\frac{n(n+1)}{2}}$,

with $q \in \mathbb{Z}$, $|q| \geq 2$. Prove that, if $x \in \mathbb{Q}^*$ and $|x| < \frac{|q|}{a}$, then $f_a(x) \notin \mathbb{Q}$.

1.11 Pell's equation

Let $d \in \mathbb{N}$. Assume d is not a square. Our aim is to prove that the diophantine equation $x^2 - dy^2 = 1$ has at least one solution $(x, y) \neq (1, 0)$.

1) Prove there exist infinitely many pairs of non-zero positive integers (x, y) such that $0 < |x^2 - dy^2| < 1 + 2\sqrt{d}$.

2) Prove there exist an integer k ($|k| < 1 + 2\sqrt{d}$), and integers m and n such that the system $x^2 - dy^2 = k$, $x \equiv m \pmod{k}$, $y \equiv n \pmod{k}$ admits infinitely many solutions.

3) Let (x', y') and (x'', y'') be two pairs solutions of this system. Prove there exists $(\xi, \eta) \in \mathbb{Z}^2$ such that

$$\begin{cases} (x' - y'\sqrt{d})(x'' + y''\sqrt{d}) = k(\xi + \eta\sqrt{d}) \\ (x' + y'\sqrt{d})(x'' - y''\sqrt{d}) = k(\xi - \eta\sqrt{d}) \end{cases}$$

4) Conclude.

1.12 An example of transcendental number

Let $\alpha \in \mathbb{R}$. We say that α is algebraic of degree d if there exist an integer $d \geq 1$ and rational integers a_0, a_1, \dots, a_d , with $a_d \neq 0$, such that $a_0 + a_1\alpha + \dots + a_d\alpha^d = 0$. For example, rational numbers are algebraic of degree 1, quadratic numbers are algebraic of degree 2. We say that α is transcendental if it is not algebraic. The purpose of this exercise is to prove that, for every $q \in \mathbb{Z}$ satisfying $|q| \geq 2$, the number $\alpha = \sum_{n=0}^{+\infty} q^{-2^n}$ is transcendental.

1) Prove that, for every $h \in \mathbb{N} - \{0\}$, $\alpha^h = \sum_{n=0}^{+\infty} b_h(n)q^{-n}$, where $b_h(n) = 0$ if the expression of n in base 2 counts at least $h+1$ digits 1, and $b_h(n) = h!$ if it counts exactly h digits 1.

2) For every integer $k \geq 2$, let $n_k = (1 + 2 + \dots + 2^{d-1})2^k$. For every $h \in \{1, 2, \dots, d\}$, compute a) $b_h(n_k)$, b) $b_h(n_k + 1)$, $b_h(n_k + 2)$, ..., $b_h(n_k + 2^{k-1})$, c) $b_h(n_k - 1)$, $b_h(n_k - 2)$, ..., $b_h(n_k - 2^{k-2})$.

3) Prove that α is transcendental.