Institute of Mathematical Sciences (IMSc)
Chennai Mathematical Institute (CMI)

updated: January 26, 2010

# Criteria for irrationality, linear independence, transcendence and algebraic independence

*Michel Waldschmidt*

These are informal notes of the beginning of my course

*Modular Algebraic Independence* [1]

December 2009 - January 2010 at Chennai Mathematical Institute (CMI)
The main reference is Nesterenko's recent book [11].

## 1 Irrationality Criteria

### 1.1 Statement of the first criterion

**Proposition 1.** *Let $\vartheta$ be a real number. The following conditions are equivalent*
(i) *$\vartheta$ is irrational.*
(ii) *For any $\epsilon > 0$, there exists $p/q \in \mathbf{Q}$ such that*

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

(iii) *For any $\epsilon > 0$, there exist two linearly independent linear forms in two variables*

$$L_0(X_0, X_1) = a_0X_0 + b_0X_1 \quad \textit{and} \quad L_1(X_0, X_1) = a_1X_0 + b_1X_1,$$

*with rational integer coefficients, such that*

$$\max\left\{|L_0(1,\vartheta)|\ ,\ |L_1(1,\vartheta)|\right\} < \epsilon.$$

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

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

[1] This text is available on the internet at the address
`http://www.math.jussieu.fr/~miw/enseignements.html`

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

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

The equivalence between (i), (ii) and (iv) is well known. See for instance [17]. See also [16].

We shall prove Proposition 1 as follows:

$$\text{(iv)} \Rightarrow \text{(ii)} \Rightarrow \text{(iii)} \Rightarrow \text{(i)} \Rightarrow \text{(iv) and (v)} \Rightarrow \text{(ii)}.$$

We do not reproduce the proof of (i) $\Rightarrow$ (v), which is a well known result due to Hurwitz. We only refer to [13]. See also [17]. Notice that an easy consequence of (iv) is the following statement, which is therefore also equivalent to the five previous assertions, even if it looks weaker than (v):

*There exist infinitely many* $p/q \in \mathbf{Q}$ *such that*

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

*Proofs of* (iv) $\Rightarrow$ (ii) *and* (v) $\Rightarrow$ (ii). Using (iv) with $Q$ satisfying $Q > 1$ and $Q \geq 1/\epsilon$, we get (ii). The proof of (v) $\Rightarrow$ (ii) is similar. □

*Proof of* (ii) $\Rightarrow$ (iii). Let $\epsilon > 0$. From (ii) we deduce the existence of $(p, q) \in \mathbf{Z} \times \mathbf{Z}$ with $q > 0$ and $\gcd(p, q) = 1$ such that

$$0 < |q\vartheta - p| < \epsilon.$$

We use (ii) once more with $\epsilon$ replaced by $|q\vartheta - p|$. There exists $(p', q') \in \mathbf{Z} \times \mathbf{Z}$ with $q' > 0$ such that

$$0 < |q'\vartheta - p'| < |q\vartheta - p|. \tag{2}$$

Define $L_0(X_0, X_1) = pX_0 - qX_1$ and $L_1(X_0, X_1) = p'X_0 - q'X_1$. It only remains to check that $L_0(X_0, X_1)$ and $L_1(X_0, X_1)$ are linearly independent. Otherwise, there exists $(s, t) \in \mathbf{Z}^2 \setminus (0, 0)$ such that $sL_0 = tL_1$. Hence $sp = tp'$, $sq = tq'$, and $p/q = p'/q'$. Since $\gcd(p, q) = 1$, we deduce $t = 1$, $p' = sp$, $q' = sq$ and $q'\vartheta - p' = s(q\vartheta - p)$. This is not compatible with (2). □

*Proof of* (iii) $\Rightarrow$ (i). Assume $\vartheta \in \mathbf{Q}$, say $\vartheta = a/b$ with $\gcd(a,b) = 1$ and $b > 0$. For any non–zero linear form $L \in \mathbf{Z}X_0 + \mathbf{Z}X_1$, the condition $L(1,\vartheta) \neq 0$ implies $|L(1,\vartheta)| \geq 1/b$, hence for $\epsilon = 1/b$ condition (iii) does not hold.

□

*Proof of* (i) $\Rightarrow$ (iv) *using Dirichlet's box principle.* Let $Q > 1$ be a given real number. 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 $x \in \mathbf{R}$ write $x = \lfloor x \rfloor + \{x\}$ with $\lfloor x \rfloor \in \mathbf{Z}$ (integral part of $x$) and $0 \leq \{x\} < 1$ (fractional part of $x$). Let $\vartheta \in \mathbf{R} \setminus \mathbf{Q}$. 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 $\vartheta$ 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 $p = \lfloor q\vartheta \rfloor + 1$. Then we have $1 \leq q \leq N-1 < Q$ and

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

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

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

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

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

□

*Remark.* Theorem 1.A in Chap. II of [13] states that for any real number $\vartheta$, 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

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

The proof given there yields strict inequality $|q\vartheta - p| < 1/Q$ in case $Q$ is not an integer. In the case where $Q$ is an integer and $\vartheta$ is rational, the result does not hold with a strict inequality in general. For instance if $\vartheta = a/b$ with $\gcd(a, b) = 1$ and $b \geq 2$, there is a solution $p/q$ to this problem with strict inequality for $Q = b + 1$, but not for $Q = b$.

However, when $Q$ is an integer and $\vartheta$ is irrational, the number $|q\vartheta - p|$ is irrational (recall that $q > 0$), hence not equal to $1/Q$.

*Proof of* (i) $\Rightarrow$ (iv) *using Minkowski geometry of numbers.* Let $\epsilon > 0$. The subset

$$\mathcal{C} = \left\{(x_0, x_1) \in \mathbf{R}^2 \ ; \ |x_0| < Q, \ |x_0\vartheta - x_1| < (1/Q) + \epsilon\right\}$$

of $\mathbf{R}^2$ is convex, symmetric and has volume $> 4$. By Minkowski's Convex Body Theorem (Corollary 7 below), it contains a non–zero element in $\mathbf{Z}^2$. Since $\mathcal{C}$ is also bounded, the intersection $\mathcal{C} \cap \mathbf{Z}^2$ is finite. Consider a non–zero element in this intersection with $|x_0\vartheta - x_1|$ minimal. Then $|x_0\vartheta - x_1| \leq 1/Q + \epsilon$ for all $\epsilon > 0$. Since this is true for all $\epsilon > 0$, we deduce $|x_0\vartheta - x_1| \leq 1/Q$. Finally, since $\vartheta$ is irrational, we also have $|x_0\vartheta - x_1| \neq 1/Q$. □

## 1.2 Irrationality of at least one number

**Proposition 3.** *Let $\vartheta_1, \ldots, \vartheta_m$ be real numbers. The following conditions are equivalent*
(i) *One at least of $\vartheta_1, \ldots, \vartheta_m$ is irrational.*
(ii) *For any $\epsilon > 0$, there exist $p_1, \ldots, p_m, q$ in $\mathbf{Z}$ with $q > 0$ such that*

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

(iii) *For any $\epsilon > 0$, there exist $m + 1$ linearly independent linear forms $L_0, \ldots, L_m$ in $m + 1$ variables with coefficients in $\mathbf{Z}$ in $m + 1$ variables $X_0, \ldots, X_m$, such that*

$$\max_{0 \leq k \leq m} |L_k(1, \vartheta_1, \ldots, \vartheta_m)| < \epsilon.$$

(iv) *For any real number* $Q > 1$, *there exists* $p_1, \dots, p_m, q$ *in* $\mathbf{Z}$ *such that* $1 \le q < Q$ *and*

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

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

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

We shall prove Proposition 3 in the following way:

$$\begin{array}{ccccc} \text{(i)} & \Rightarrow & \text{(iv)} & & \\ & & & \searrow & \\ \Uparrow & & & & \text{(v)} \\ & & & \swarrow & \\ \text{(iii)} & \Leftarrow & \text{(ii)} & & \end{array}$$

*Proof of* (iv) $\Rightarrow$ (v). We first deduce (i) from (iv). Indeed, if (i) does not hold and $\vartheta_i = a_i/b \in \mathbf{Q}$ for $1 \le i \le m$, then the condition

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

implies

$$\max_{1 \le i \le m} \left| \vartheta_i - \frac{p_i}{q} \right| \ge \frac{1}{bq},$$

hence (iv) does not hold as soon as $Q > b^m$.

Let $\{q_1, \dots, q_N\}$ be a finite set of positive integers. Using (iv) again, we show that there exists a positive integer $q \notin \{q_1, \dots, q_N\}$ satisfying the condition (v). Denote by $\| \cdot \|$ the distance to the nearest integer: for $x \in \mathbf{R}$,

$$\|x\| = \min_{a \in \mathbf{Z}} |x - a|.$$

From (i) it follows that for $1 \le j \le N$, the number $\max_{1 \le i \le m} \|q_j \vartheta_i\|$ is non–zero. Let $Q > 1$ be sufficiently large such that

$$Q^{-1/m} < \min_{1 \le j \le N} \max_{1 \le i \le m} \|q_j \vartheta_i\|.$$

We use (iv): there exists an integer $q$ in the range $1 \le q < Q$ such that

$$0 < \max_{1 \le i \le m} \|q \vartheta_i\| \le Q^{-1/m}.$$

The right hand side is $< q^{-1/m}$, and the choice of $Q$ implies $q \notin \{q_1, \dots, q_N\}$. □

*Proof of* (v) $\Rightarrow$ (ii). Given $\epsilon > 0$, there is a positive integer $q > \max\{1, 1/\epsilon^m\}$ satisfying the conclusion of (v). Then (ii) follows. $\square$

*Proof of* (ii) $\Rightarrow$ (iii). Let $\epsilon > 0$. From (ii) we deduce the existence of $(p_1, \dots, p_m, q)$ in $\mathbf{Z}^{m+1}$ with $q > 0$ such that

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

Without loss of generality we may assume $\gcd(p_1, \dots, p_m, q) = 1$. Define $L_1, \dots, L_m$ by $L_i(X_0, \dots, X_m) = p_i X_0 - qX_i$ for $1 \le i \le m$. Then $L_1, \dots, L_m$ are $m$ linearly independent linear forms in $m+1$ variables with rational integer coefficients satisfying

$$0 < \max_{1 \le i \le m} |L_i(1, \vartheta_1, \dots, \vartheta_m)| < \epsilon.$$

We use (ii) once more with $\epsilon$ replaced by

$$\max_{1 \le i \le m} |L_i(1, \vartheta_1, \dots, \vartheta_m)| = \max_{1 \le i \le m} |q\vartheta_i - p_i|.$$

Hence there exists $p'_1, \dots, p'_m, q'$ in $\mathbf{Z}$ with $q' > 0$ such that

$$0 < \max_{1 \le i \le m} |q'\vartheta_i - p'_i| < \max_{1 \le i \le m} |q\vartheta_i - p_i|. \tag{4}$$

It remains to check that one at least of the $m$ linear forms

$$L'_i(X_0, \dots, X_m) = p'_i X_0 - q' X_i$$

for $1 \le i \le m$ is linearly independent of $L_1, \dots, L_m$. Otherwise, for $1 \le i \le m$, there exist rational integers $s_i, t_{i1}, \dots, t_{im}$, with $s_i \ne 0$, such that

$$\begin{aligned} s_i(p'_i X_0 - q' X_i) &= t_{i1}L_1 + \cdots + t_{im}L_m \\ &= (t_{i1}p_1 + \cdots + t_{im}p_m)X_0 - q(t_{i1}X_1 + \cdots + t_{im}X_m). \end{aligned}$$

These relations imply, for $1 \le i \le m$,

$$s_i q' = q t_{ii}, \quad t_{ki} = 0 \quad \text{and} \quad s_i p'_i = p_i t_{ii} \quad \text{for } 1 \le k \le m, \quad k \ne i,$$

meaning that the two projective points $(p_1 : \cdots : p_m : q)$ and $(p'_1 : \cdots : p'_m : q')$ are the same. Since $\gcd(p_1, \dots, p_m, q) = 1$, it follows that $(p'_1, \dots, p'_m, q')$ is an integer multiple of $(p_1, \dots, p_m, q)$. This is not compatible with (4).

$\square$

*Proof of* (iii) $\Rightarrow$ (i). We proceed by contradiction. Assume (i) is not true: there exists $(a_1, \dots, a_m, b) \in \mathbf{Z}^{m+1}$ with $b > 0$ such that $\vartheta_k = a_k/b$ for $1 \le k \le m$. Use (iii) with $\epsilon = 1/b$: we get $m+1$ linearly independent linear forms $L_0, \dots, L_m$ in $\mathbf{Z}X_0 + \cdots + \mathbf{Z}X_m$. One at least of them, say $L_k$, does not vanish at $(1, \vartheta_1, \dots, \vartheta_m)$. Then we have

$$0 < |L_k(b, a_1, \dots, a_m)| = b|L_k(1, \vartheta_1, \dots, \vartheta_m)| < b\epsilon = 1.$$

Since $L_k(b, a_1, \dots, a_m)$ is a rational integer, we obtain a contradiction.

□

It remains to prove (i) $\Rightarrow$ (iv) of Proposition 3. We give a proof (compare with [13] Chap. II § 2 p. 35) which relies Minkowski's linear form Theorem. Another proof of (i) $\Rightarrow$ (iv) in the special case where $Q^{1/m}$ is an integer, by means of Dirichlet's box principle, can be found in [13] Chap. II Th. 1E p. 28. A third proof (using again the geometry of numbers, but based on a result by Blichfeldt) is given in [13] Chap. II § 2 p. 32.

We need some geometry of numbers. Recall that a discrete subgroup of $\mathbf{R}^n$ of maximal rank $n$ is called a *lattice* of $\mathbf{R}^n$.

Let $G$ be a lattice in $\mathbf{R}^n$. For each basis $\mathbf{e} = \{e_1, \dots, e_n\}$ 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 $\mathbf{R}^n$ as

$$\mathbf{R}^n = \bigcup_{g \in G} (P_{\mathbf{e}} + g) \tag{5}$$

A change of bases of $G$ is obtained with a matrix with integer coefficients having determinant $\pm 1$, 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 6** (Minkowski)**.** *Let $G$ be a lattice in $\mathbf{R}^n$ and $B$ a measurable subset of $\mathbf{R}^n$. Set $\mu(B) > v(G)$. Then there exist $x \neq y$ in $B$ such that $x - y \in G$.*

*Proof.* From (5) 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 $x - y = g - g' \in G \setminus \{0\}$. □

From Theorem 6 we deduce Minkowski's convex body Theorem (Theorem 2B, Chapter II of [13]).

**Corollary 7.** *Let $G$ be a lattice in $\mathbf{R}^n$ and let $B$ be a measurable subset of $\mathbf{R}^n$, 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 6 with the set

$$B' = \frac{1}{2}B = \{x \in \mathbf{R}^n \ ; \ 2x \in B\}.$$

We have $\mu(B') = 2^{-n}\mu(B) > v(G)$, hence by Theorem 6 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 7, if $B$ is also compact in $\mathbf{R}^n$, then the weaker inequality $\mu(B) \geq 2^n v(G)$ suffices to reach the conclusion. This is obtained by applying Corollary 7 with $(1 + \epsilon)B$ for $\epsilon \to 0$.*

Minkowski's Linear Forms Theorem (see for instance [13] Chap. II § 2 Th. 2C) is the following result.

**Theorem 8** (Minkowski's Linear Forms Theorem)**.** *Suppose that* $\vartheta_{ij}$ *(*$1 \leq i, j \leq n$*) are real numbers with determinant* $\pm 1$ *. Suppose that* $A_1, \ldots, A_n$ *are positive numbers with* $A_1 \cdots A_n = 1$*. Then there exists an integer point* $\underline{x} = (x_1, \ldots, x_n) \neq 0$ *such that*

$$|\vartheta_{i1}x_1 + \cdots + \vartheta_{in}x_n| < A_i \qquad (1 \leq i \leq n-1)$$

*and*

$$|\vartheta_{n1}x_1 + \cdots + \vartheta_{nn}x_n| \leq A_n.$$

*Proof.* We apply Corollary 7 with $A_n$ replaced with $A_n + \epsilon$ for a sequence of $\epsilon$ which tends to 0. □

Here is a consequence of Theorem 8

**Corollary 9.** *Let* $\vartheta_1, \ldots, \vartheta_m$ *be real numbers. For any real number* $Q > 1$*, there exists* $p_1, \ldots, p_m, q$ *in* $\mathbf{Z}$ *such that* $1 \leq q < Q$ *and*

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

*Proof of Corollary 9.* We apply Theorem 8 to the $n \times n$ matrix (with $n = m + 1$)

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ -\vartheta_1 & 1 & 0 & \cdots & 0 \\ -\vartheta_2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\vartheta_m & 0 & 0 & \cdots & 1 \end{pmatrix}$$

corresponding to the linear forms $X_0$ and $-\vartheta_i X_0 + X_i$ $(1 \leq i \leq m)$, and with $A_0 = Q$, $A_1 = \cdots = A_m = Q^{-1/m}$.

□

*Proof of* (i) ⇒ (iv) *in Proposition 3.* Use Corollary 9. From the assumption (i) we deduce

$$\max_{1 \leq i \leq m} \left| \vartheta_i - \frac{p_i}{q} \right| \neq 0.$$

□

# 2 Criteria for linear independence

## 2.1 Hermite's method

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. The goal is to prove that the number

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

is not 0.

Hermite's idea (see [6] and [4] Chap. 2 § 1.3) is to approximate simultaneously $\vartheta_1, \ldots, \vartheta_m$ by rational numbers $p_1/q, \ldots, p_m/q$ with the same denominator $q > 0$.

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

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

Then $qL = M + R$ with

$$M = a_0q + a_1p_1 + \cdots + a_mp_m \in \mathbf{Z}$$

and

$$R = a_1\epsilon_1 + \cdots + a_m\epsilon_m \in \mathbf{R}.$$

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 $(q, p_1, \ldots, p_m)$ such that $(p_1/q, \ldots, p_m/q)$ is a simultaneous rational approximation to $(\vartheta_1, \ldots, \vartheta_m)$, but we also require that it lies outside the hyperplane $a_0X_0 + a_1X_1 + \cdots + a_mX_m = 0$ of $\mathbf{Q}^{m+1}$. Our goal is to prove the linear independence over $\mathbf{Q}$ of $1, \vartheta_1, \ldots, \vartheta_m$; hence this needs to be checked for all hyperplanes. The solution to this problem is to construct not only one tuple $(q, p_1, \ldots, p_m)$ in $\mathbf{Z}^{m+1} \setminus \{0\}$, but $m+1$ such tuples which are linearly independent. This yields $m+1$ pairs $(M_k, R_k)$ $(k = 0, \ldots, m)$ in place of a single pair $(M, R)$. From $(a_0, \ldots, a_m) \neq (0, \ldots, 0)$, one deduces that one at least of $M_0, \ldots, M_m$ is not 0.

It turns out (Proposition 10 below) that nothing is losed by using such arguments: existence of linearly independent simultaneous rational approximations for $\vartheta_1, \ldots, \vartheta_m$ are characteristic of linearly independent real numbers $1, \vartheta_1, \ldots, \vartheta_m$.

## 2.2 Rational approximations

The following criterion is due to M. Laurent [8].

**Proposition 10.** *Let $\underline{\vartheta} = (\vartheta_1, \ldots, \vartheta_m) \in \mathbf{R}^m$. Then the following conditions are equivalent.*
(i) *The numbers $1, \vartheta_1, \ldots, \vartheta_m$ are linearly independent over $\mathbf{Q}$.*
(ii) *For any $\epsilon > 0$, there exist $m+1$ linearly independent elements $\mathbf{u}_0, \mathbf{u}_1, \ldots, \mathbf{u}_m$ in $\mathbf{Z}^{m+1}$, say*

$$\mathbf{u}_i = (q_i, p_{1i}, \ldots, p_{mi}) \quad (0 \le i \le m)$$

*with $q_i > 0$, such that*

$$\max_{1 \le k \le m} \left| \vartheta_k - \frac{p_{ki}}{q_i} \right| \le \frac{\epsilon}{q_i} \quad (0 \le i \le m). \tag{11}$$

The condition on linear independence of the elements $\mathbf{u}_0, \mathbf{u}_1, \ldots, \mathbf{u}_m$ 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

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

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

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

Also for $\underline{x} = (x_1, \ldots, x_m) \in \mathbf{R}^m$ and $\underline{y} = (y_1, \ldots, y_m) \in \mathbf{R}^m$ set

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

so that

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

Then the relation (11) in Proposition 10 can be written

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

The easy implication (which is also the useful one for Diophantine applications: linear independence, transcendence and algebraic independence) is (ii)⇒(i). We shall prove a more explicit version of it by checking that *any tuple* $(q, p_1, \dots, p_m) \in \mathbf{Z}^{m+1}$, *with* $q > 0$, *producing a tuple* $(p_1/q, \dots, p_m/q) \in \mathbf{Q}^m$ *of sufficiently good rational approximations to* $\underline{\vartheta}$ *satisfies the same linear dependence relations as* $1, \vartheta_1, \dots, \vartheta_m$.

**Lemma 12.** *Let* $\vartheta_1, \dots, \vartheta_m$ *be real numbers. Assume that the numbers* $1, \vartheta_1, \dots, \vartheta_m$ *are linearly dependent over* $\mathbf{Q}$*: 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* $\epsilon$ *be a real number satisfying*

$$0 < \epsilon < \left( \sum_{k=1}^{m} |b_k| \right)^{-1}.$$

*Assume further that* $(q, p_1, \dots, p_m) \in \mathbf{Z}^{m+1}$ *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

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

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 Proposition 10.* Let

$$aX_0 + b_1X_1 + \cdots + b_mX_m$$

be a non–zero linear form with integer coefficients. For sufficiently small $\epsilon$, assumption (ii) show that there exist $m + 1$ linearly independent elements $\mathbf{u}_i \in \mathbf{Z}^{m+1}$ such that the corresponding rational approximation satisfy the assumptions of Lemma 12. Since $\mathbf{u}_0, \dots, \mathbf{u}_m$ is a basis of $\mathbf{Q}^{m+1}$, one at least of the $L(\mathbf{u}_i)$ is not 0. Hence Lemma 12 implies

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

□

*Proof of (i)⇒(ii) in Proposition 10.* Let $\epsilon > 0$. By Corollary 9, there exists $\mathbf{u} = (q, p_1, \ldots, p_m) \in \mathbf{Z}^{m+1}$ with $q > 0$ such that

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

Consider the subset $E_\epsilon \subset \mathbf{Z}^{m+1}$ of these tuples. Let $V_\epsilon$ be the $\mathbf{Q}$-vector subspace of $\mathbf{Q}^{m+1}$ spanned by $E_\epsilon$.

If $V_\epsilon \neq \mathbf{Q}^{m+1}$, then there is a hyperplane $a_0 x_0 + a_1 x_1 + \cdots + a_m x_m = 0$ containing $E_\epsilon$. Any $\mathbf{u} = (q, p_1, \ldots, p_m)$ in $E_\epsilon$ has

$$a_0 q + a_1 p_1 + \cdots + a_m p_m = 0.$$

For each $n \ge 1/\epsilon$, let $\mathbf{u} = (q_n, p_{1n}, \ldots, p_{mn}) \in E_\epsilon$ satisfy

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

Then

$$a_0 + a_1 \vartheta_1 + \cdots + a_m \vartheta_m = \sum_{k=1}^{m} a_k \left( \vartheta_k - \frac{p_{kn}}{q_n} \right).$$

Hence

$$|a_0 + a_1 \vartheta_1 + \cdots + a_m \vartheta_m| \le \frac{1}{n q_n} \sum_{k=1}^{m} |a_k|.$$

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 $\mathbf{Q}$–linearly dependent, which means that $(i)$ does not hold.

Therefore, if $(i)$ holds, then $V_\epsilon = \mathbf{Q}^{m+1}$, hence there are $m+1$ linearly independent elements in $E_\epsilon$.

□

## 2.3 Linear forms

### 2.3.1 Siegel's method: $m+1$ linear forms

For proving linear independence of real numbers, Hermite [6] considered simultaneous approximation to these numbers by algebraic numbers. The point of view introduced by Siegel in 1929 [14] is dual (duality in the sense of convex bodies): he considers simultaneous approximation by means of independent linear forms.

We define the *height* of a linear form $L = a_0X_0 + \cdots + a_mX_m$ with complex coefficients by

$$H(L) = \max\{|a_0|, \ldots, |a_m|\}.$$

**Lemma 13.** *Let $\vartheta_1, \ldots, \vartheta_m$ be complex numbers. Assume that, for any $\epsilon > 0$, there exists $m+1$ linearly independent linear forms $L_0, \ldots, L_m$ in $m+1$ variables, with coefficients in $\mathbf{Z}$, such that*

$$\max_{0\le k\le m} |L_k(1, \vartheta_1, \ldots, \vartheta_m)| < \frac{\epsilon}{H^{m-1}} \quad \textit{where} \quad H = \max_{0\le k\le m} H(L_k).$$

*Then $1, \vartheta_1, \ldots, \vartheta_m$ are linearly independent over $\mathbf{Q}$.*

The proof is given by C.L. Siegel in [14]; see also [4] Chap. 2 § 1.4 and [1]. We sketch the argument here, and we expand it below.

Assume $1, \vartheta_1, \ldots, \vartheta_m$ are linearly dependent over $\mathbf{Q}$: let $\Lambda_0 \in \mathbf{Z}X_0 + \mathbf{Z}X_1 + \cdots + \mathbf{Z}X_m$ be a non–zero linear form in $m+1$ variables which vanishes at the point $(1, \vartheta_1, \ldots, \vartheta_m)$. Denote by $A$ the maximum of the absolute values of the coefficients of $\Lambda_0$ and use the assumption with $\epsilon = 1/m!mA$. Among the $m+1$ linearly independent linear forms which are given by the assumption of Lemma 13, select $m$ of them, say $\Lambda_1, \ldots, \Lambda_m$, which form with $\Lambda_0$ a set of $m+1$ linearly independent linear forms. The $(m+1)\times(m+1)$ matrix of coefficients of these forms is regular; using the inverse matrix, one expresses its determinant $\Delta$ as a linear combination with integer coefficients of $\Lambda_k(1, \vartheta_1, \ldots, \vartheta_m)|$, $1 \le k \le m$. The choice of $\epsilon$ yields the contradiction $|\Delta| < 1$.

We develop this idea and deduce the following more precise statement.

**Proposition 14.** *Let $\vartheta_1, \ldots, \vartheta_m$ be complex numbers and $L_0, \ldots, L_m$ be $m+1$ linearly independent linear forms in $m+1$ variables with coefficients in $\mathbf{Z}$. Then*

$$\max_{0\le k\le m} \frac{|L_k(1, \vartheta_1, \ldots, \vartheta_m)|}{H(L_k)} \ge \frac{1}{(m+1)!H(L_0)\cdots H(L_m)}.$$

*Proof.* For $0 \le k \le m$, write

$$L_k(X_0, \ldots, X_m) = \sum_{i=0}^{m} \ell_{ki}X_i \quad \text{and set} \quad \lambda_k = L_k(1, \vartheta_1, \ldots, \vartheta_m).$$

Define $\vartheta_0 = 1$. Let $\underline{\mathrm{L}}$ be the regular $(m+1)\times(m+1)$ matrix $\big(\ell_{ki}\big)_{0\le k,i\le m}$. Using the relation

$$\begin{pmatrix} \vartheta_0 \\ \vdots \\ \vartheta_m \end{pmatrix} = \underline{\mathrm{L}}^{-1} \begin{pmatrix} \lambda_0 \\ \vdots \\ \lambda_m \end{pmatrix},$$

one can write the product of $\vartheta_0 = 1$ by $\det(\underline{\mathrm{L}})$ as a linear combination of $\lambda_0, \dots, \lambda_m$ with rational integer coefficients. In this linear combination, the absolute value of the coefficient of $\lambda_k$ is $\le m! H(L_0) \cdots H(L_m)/H(L_k)$. We deduce

$$1 \le |\det(\underline{\mathrm{L}})| \le m! \sum_{k=0}^{m} H(L_0) \cdots H(L_m) \frac{|\lambda_k|}{H(L_k)}.$$

Proposition 14 follows.

□

An straightforward consequence of Proposition 14 is the following:

**Corollary 15.** *Let $\vartheta_1, \dots, \vartheta_m$ be complex numbers, $H$ be a positive real number and $L_0, \dots, L_m$ be $m+1$ linearly independent linear forms in $m+1$ variables with coefficients in $\mathbf{Z}$ of height $\le H$. Then*

$$\max_{0 \le k \le m} |L_k(1, \vartheta_1, \dots, \vartheta_m)| \ge \frac{1}{(m+1)! H^m}.$$

Using either Proposition 14 or Corollary 15, we deduce the following result (compare with [11] Lemma 2.4):

**Corollary 16.** *Let $\vartheta_1, \dots, \vartheta_m$ be complex numbers and $\kappa \ge 0$ be a real number. Assume that, for any $\epsilon > 0$, there exists $m+1$ linearly independent linear forms $L_0, \dots, L_m$ in $m+1$ variables, with coefficients in $\mathbf{Z}$, such that*

$$\max_{0 \le k \le m} |L_k(1, \vartheta_1, \dots, \vartheta_m)| < \frac{\epsilon}{H^\kappa} \quad \text{where} \quad H = \max_{0 \le k \le m} H(L_k).$$

*Denote by $r+1$ the dimension of the $\mathbf{Q}$–vector space spanned by $1, \vartheta_1, \dots, \vartheta_m$. Then $r > \kappa$.*

Under the assumptions of Corollary 16, since $r \le m$, we deduce $\kappa < m$, which is a plain consequence of Corollary 15.

We recover Lemma 13 by taking $\kappa = m - 1$.

Also we recover the implication (iii) ⇒ (i) from Proposition 3 by taking $\kappa = 0$.

*Proof.* One can deduce Corollary 16 from Proposition 14 as follows: consider $m - r$ linearly independent linear relations among $1, \vartheta_1, \dots, \vartheta_m$. Denote by $\widetilde{L}_{r+1}, \dots, \widetilde{L}_m$ these linear forms and by $c$ their maximal height. Take $0 < \epsilon < 1/((m+1)! c^{m-r})$. Select $r+1$ linear forms $\widetilde{L}_0, \dots, \widetilde{L}_r$ among

$L_0, \dots, L_m$ to get a maximal system of $m+1$ linearly independent linear forms $\widetilde{L}_0, \dots, \widetilde{L}_m$. From Proposition 14 one deduces

$$\begin{aligned}\frac{1}{(m+1)!c^{m-r}H(\widetilde{L}_0)\cdots H(\widetilde{L}_r)} &\le \frac{1}{(m+1)!H(\widetilde{L}_0)\cdots H(\widetilde{L}_m)}\\ &\le \max_{0\le k\le m}\frac{|\widetilde{L}_k(1,\vartheta_1,\dots,\vartheta_m)|}{H(\widetilde{L}_k)}\\ &\le \max_{0\le k\le r}\frac{|\widetilde{L}_k(1,\vartheta_1,\dots,\vartheta_m)|}{H(\widetilde{L}_k)}\\ &\le \max_{0\le k\le m}\frac{|L_k(1,\vartheta_1,\dots,\vartheta_m)|}{H(L_k)}.\end{aligned}$$

From the choice of $\epsilon$, one concludes $H^\kappa < H^r$, hence $r > \kappa$.

Here is another proof of Corollary 16, which rests on Corollary 15. Let $1, \xi_1, \dots, \xi_r$ be a basis of the $\mathbf{Q}$–vector space spanned by $1, \vartheta_1, \dots, \vartheta_m$. Define $\xi_0 = \vartheta_0 = 1$ and write

$$\vartheta_h = \sum_{j=0}^{r} a_{hj}\xi_j \quad (0 \le h \le m).$$

In particular $a_{00} = 1$ and $a_{0j} = 0$ for $1 \le j \le m$. Define

$$c = \max_{0\le j\le r}\sum_{h=0}^{m}|a_{hj}|$$

and let $\epsilon$ satisfy $0 < \epsilon < 1/(r+1)!c^r$. Let $L_0, \dots, L_m$ be the $m+1$ linearly independent linear forms in $m+1$ variables with integer coefficients given by the assumption of Corollary 16. Write

$$L_k(X_0, \dots, X_m) = \sum_{h=0}^{m}\ell_{kh}X_h \quad (0 \le k \le m).$$

By assumption $\max_{0\le k,h\le m}|\ell_{kh}| \le H$. Consider the $m+1$ linear forms $\Lambda_0, \dots, \Lambda_m$ in $r+1$ variables $Y_0, \dots, Y_r$ defined by

$$\Lambda_k(Y_0, \dots, Y_r) = \lambda_{k0}Y_0 + \cdots + \lambda_{kr}Y_r \quad (0 \le k \le m)$$

with

$$\lambda_{kj} = \sum_{h=0}^{m}\ell_{kh}a_{hj}.$$

The connexion between the linear forms $L_0, \dots, L_m$ in $\mathbf{Z}X_0 + \cdots + \mathbf{Z}X_m$ on the one side and and $\Lambda_0, \dots, \Lambda_m$ in $\mathbf{Z}Y_0 + \cdots + \mathbf{Z}Y_r$ on the other side is

$$\Lambda_k(Y_0, \dots, Y_r) = L_k\left(\sum_{j=0}^{r} a_{0j}Y_j, \dots, \sum_{j=0}^{r} a_{mj}Y_j\right) \qquad (0 \le k \le m).$$

Since $1, \xi_1, \dots, \xi_r$ are $\mathbf{Q}$–linearly independent, the $r+1$ columns of the $(m+1) \times (r+1)$ matrix $\big(a_{hj}\big)_{\substack{0 \le h \le m \\ 0 \le j \le r}}$ are linearly independent in $\mathbf{Q}^{m+1}$, hence this matrix has rank $r+1$, and therefore the rank of the set of $m+1$ linear forms $\Lambda_0, \dots, \Lambda_m$ is $r+1$. By construction

$$\Lambda_k(1, \xi_1, \dots, \xi_r) = L_k(1, \vartheta_1, \dots, \vartheta_m) \quad (0 \le k \le m).$$

Applying Corollary 15 to the point $(1, \xi_1, \dots, \xi_r)$ with $r+1$ independent linear forms among $\Lambda_0, \dots, \Lambda_m$, we deduce

$$\max_{0 \le k \le m} |\Lambda_k(1, \xi_1, \dots, \xi_r)| \ge \frac{1}{(r+1)!\widetilde{H}^r}$$

with

$$\widetilde{H} = \max_{0 \le k \le m} H(\Lambda_k) = \max_{\substack{0 \le k \le m \\ 0 \le j \le r}} |\lambda_{kj}| \le cH.$$

Again, from the choice of $\epsilon$, one concludes $H^\kappa < H^r$, hence $r > \kappa$.

Corollary 16 follows.

□

### 2.3.2 Nesterenko's Criterion for linear independence

In 1985, Yu.V. Nesterenko [10], obtained a variant of Proposition 14 (Siegel's linear independence criterion). There are two main differences: on the one hand, Nesterenko does not need $m+1$ linearly independent forms, but he needs only one; at the same time he does not only assumes an upper bound for the value of this linear form at the point $(1, \vartheta_1, \dots, \vartheta_m)$, but also a lower bound. On the other hand, for Nesterenko it is not sufficient to have infinitely many linear forms as in Siegel's Proposition 14, but he needs a sequence of such forms (for all sufficiently large $n$, and not only for infinitely many $n$). A simplification of the original proof by Nesterenko was proposed by F. Amoroso and worked out by P. Colmez. A new approach, which at the same time simplifies further the argument and yields refinements, is due to S. Fischler and W. Zudilin [5].

The main reference for this section is [1].

**Theorem 17** (Nesterenko linear independence criterion)**.** *Let $c_1, c_2, \tau_1, \tau_2$ be positive real numbers and $\sigma(n)$ a non–decreasing positive function such that*

$$\lim_{n\to\infty} \sigma(n) = \infty \quad \text{and} \quad \limsup_{n\to\infty} \frac{\sigma(n+1)}{\sigma(n)} = 1.$$

*Let $\underline{\vartheta} = (\vartheta_1, \dots, \vartheta_m) \in \mathbf{R}^m$. Assume that, for all sufficiently large integers $n$, there exists a linear form with integer coefficients in $m+1$ variables*

$$L_n(\underline{X}) = \ell_{0n}X_0 + \ell_{1n}X_1 + \cdots + \ell_{mn}X_m,$$

*which satisfies the conditions*

$$H(L_n) \le e^{\sigma(n)} \quad \text{and} \quad c_1 e^{-\tau_1\sigma(n)} \le |L_n(1, \underline{\vartheta})| \le c_2 e^{-\tau_2\sigma(n)}.$$

*Then* $\dim_{\mathbf{Q}}(\mathbf{Q} + \mathbf{Q}\vartheta_1 + \cdots + \mathbf{Q}\vartheta_m) \ge (1+\tau_1)/(1+\tau_1-\tau_2)$.

The main result of [1], which relies on the arguments in [5], is the following.

**Theorem 18.** *Let $\underline{\xi} = (\xi_i)_{i\ge 0}$ be a sequence of real numbers with $\xi_0 = 1$, $(r_n)_{n\ge 0}$ a non–decreasing sequence of positive integers, $(Q_n)_{n\ge 0}$, $(A_n)_{n\ge 0}$ and $(B_n)_{n\ge 0}$ sequences of positive real numbers such that $\lim_{n\to\infty} A_n^{1/r_n} = \infty$ and, for all sufficiently large integers $n$,*

$$Q_n B_n \le Q_{n+1} B_{n+1}.$$

*Assume that, for any sufficiently large integer $n$, there exists a linear form with integer coefficients in $r_n + 1$ variables*

$$L_n(\underline{X}) = \ell_{0n}X_0 + \ell_{1n}X_1 + \cdots + \ell_{r_n n}X_{r_n}$$

*such that*

$$\sum_{i=0}^{r_n} |\ell_{in}| \le Q_n, \quad 0 < |L_n(\underline{\xi})| \le \frac{1}{A_n} \quad \text{and} \quad \frac{|L_{n-1}(\underline{\xi})|}{|L_n(\underline{\xi})|} \le B_n.$$

*Then $A_n \le 2^{r_n+1}(B_n Q_n)^{r_n}$ for all sufficiently large integers $n$.*

One deduces from Theorem 18 a slight refinement of Theorem 17 where the condition $\limsup_{n\to\infty} \frac{\sigma(n+1)}{\sigma(n)} = 1$ is relaxed, the cost being to replace $\sigma(n)$ by $\sigma(n+1)$ in the upper bound for $|L_n(1, \underline{\vartheta})|$.

**Corollary 19.** *Let $\tau_1, \tau_2$ be positive real numbers and $\sigma(n)$ a non–decreasing positive function such that $\lim_{n\to\infty} \sigma(n) = \infty$. Let $\underline{\vartheta} = (\vartheta_1, \ldots, \vartheta_m) \in \mathbf{R}^m$. Assume that, for all sufficiently large integers $n$, there exists a linear form with integer coefficients in $m+1$ variables*

$$L_n(\underline{X}) = \ell_{0n}X_0 + \ell_{1n}X_1 + \cdots + \ell_{mn}X_m$$

*which satisfies the conditions*

$$H(L_n) \le e^{\sigma(n)} \quad \text{and} \quad e^{-(\tau_1+o(1))\sigma(n)} \le |L_n(1, \underline{\vartheta})| \le e^{-(\tau_2+o(1))\sigma(n+1)}.$$

*Then* $\dim_{\mathbf{Q}}(\mathbf{Q} + \mathbf{Q}\vartheta_1 + \cdots + \mathbf{Q}\vartheta_m) \ge (1+\tau_1)/(1+\tau_1-\tau_2)$.

Further consequences of Theorem 18 are given in [1]. See also Corollary 29 below;

# 3 Criteria for transcendence

The main Diophantine tool for proving transcendence results is Liouville's inequality.

## 3.1 Liouville's inequality

Recall that the ring $\mathbf{Z}[X]$ is factorial, its irreducible elements of positive degree are the non-constant polynomials with integer coefficients which are irreducible in $\mathbf{Q}[X]$ (i.e. not a product of two non-constant polynomials in $\mathbf{Q}[X]$) and have content 1. The *content* of a polynomial in $\mathbf{Z}[X]$ is the greatest common divisor of its coefficients.

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

The next lemma is one of many variants of Liouville's inequality (see, for instance, [7, 13, 15, 9, 11]), which is close to the original one of 1844.

**Lemma 20.** *Let $\alpha$ be an algebraic number of degree $d \ge 2$ and minimal polynomial $P \in \mathbf{Z}[X]$. Define $c = |P'(\alpha)|$. Let $\epsilon > 0$. Then there exists an integer $q_0$ such that, for any $p/q \in \mathbf{Q}$ with $q \ge q_0$,*

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

*Proof.* The result is trivial if $\alpha$ is not real: an admissible value for $q_0$ is

$$q_0 = (c|\Im m(\alpha)|)^{-1/d}.$$

Assume now $\alpha$ is real. Let $q$ be a sufficiently large positive integer and let $p$ be the nearest integer to $q\alpha$. In particular

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

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

$$q^d P(p/q) = a_0 q^d \prod_{i=1}^{d} \left(\frac{p}{q} - \alpha_i\right). \tag{21}$$

Also

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

The left hand side of (21) is a rational integer. It is not zero because $P$ is irreducible of degree $\geq 2$. 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

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

□

The same proof yields the next result.

Define the height $H(P)$ of a polynomial $P$ with complex coefficients (any number of variables) as the maximum modulus of its coefficients.

**Proposition 22** (Liouville's inequality)**.** *Let $\alpha_1, \ldots, \alpha_m$ be algebraic numbers. There exists a constant $c = c(\alpha_1, \ldots, \alpha_m) > 0$ such that, for any polynomial $P \in \mathbf{Z}[X_1, \ldots, X_m]$ satisfying $P(\alpha_1, \ldots, \alpha_m) \neq 0$, the inequality*

$$|P(\alpha_1, \ldots, \alpha_m)| \geq H^{-c} e^{-cd}$$

*holds with $H = \max\{2, H(P)\}$ and $d$ the total degree of $P$.*

The constant $c$ can be explicitly computed (see, for instance, [4, 16]), but this is not relevant here.

The corollary below (which is [11] Prop. 3.1) is useful for proving transcendence results.

**Corollary 23.** *Let $\vartheta_1, \ldots, \vartheta_m$ be complex numbers $\mathbf{C}$. Let $\sigma(n)$ and $\lambda(n)$ be two non–decreasing positive real functions with $\lim_{n\to\infty} \sigma(n) = \infty$ and $\lim_{n\to\infty} \lambda(n)/\sigma(n) = \infty$. Assume that there exists a sequence $(P_n)_{n\geq 0}$ of polynomials in $\mathbf{Z}[X_1, \ldots, X_m]$, with $P_n$ of degree $\leq \sigma(n)$ and height $H(P_n) \leq e^{\sigma(n)}$, such that, for infinitely many $n$,*

$$0 < |P_n(\vartheta_1, \ldots, \vartheta_m)| \leq e^{-\lambda(n)}.$$

*Then at least one of the numbers $\vartheta_1, \ldots, \vartheta_m$ is transcendental.*

### 3.2 Transcendence criterion of A. Durand

Liouville's result is not a necessary and sufficient condition for transcendence. One way of extending the irrationality criterion of Proposition 1 into a transcendence criterion is to replace rational approximation by approximation by algebraic numbers. For instance, given an integer $d$, one gets a criterion for $\vartheta$ not being algebraic of degree $\leq d$ by considering algebraic approximation of $\vartheta$ by algebraic numbers of degree $\leq d$. One may also let $d$ vary and get a transcendence criterion as follows.

Define the height of a $H(\alpha)$ of an algebraic number $\alpha$ as the height of its irreducible polynomial in $\mathbf{Z}[X]$, and the size $s(\alpha)$ as

$$s(\alpha) := [\mathbf{Q}(\alpha) : \mathbf{Q}] + \log H(\alpha).$$

The following result (we shall not use it and we do not include a proof) is due to A. Durand [2, 3].

**Proposition 24.** *Let $\vartheta$ be a complex number. The following conditions are equivalent*

(i) *$\vartheta$ is transcendental.*
(ii) *For any $\kappa > 0$ there exists and algebraic number $\alpha$ such that*

$$0 < |\vartheta - \alpha| < e^{-\kappa s(\alpha)}.$$

(iii) *There exists a sequence $(\alpha_n)_{n\geq 0}$ of pairwise distinct algebraic numbers such that*

$$\lim_{n\to\infty} \frac{\log|\vartheta - \alpha_n|}{s(\alpha_n)} = -\infty.$$

Another way of getting transcendence criteria for a number $\vartheta$ (resp. criteria for $\vartheta$ not being of degree $\leq d$) is to consider polynomial approximations $|P(\vartheta)|$ by polynomials in $\mathbf{Z}[X]$ (resp. by polynomials of degree $\leq d$).

# 4 Criteria for algebraic independence

## 4.1 Small transcendence degree: Gel'fond's criterion

Gel'fond's criterion (see, for instance, [7, 15, 9, 11]) is a powerful tool to prove the algebraic independence of at least two numbers.

A slightly refined version (due to A. Chantanasiri) is the following one.

Define the size $t(P)$ of a polynomial $P \in \mathbf{C}[X]$ as

$$t(P) := \log H(P) + (\log 2)\deg P.$$

**Theorem 25** (Gel'fond's transcendence Criterion)**.** *Let $\vartheta \in \mathbf{C}$ and let $\gamma$ be a real number with $\gamma > 1$. Let $(d_n)_{n=1}^{\infty}$ and $(t_n)_{n=1}^{\infty}$ be two non–decreasing sequences of real numbers with $\lim_{n\to\infty} t_n = \infty$. Assume that there exists a sequence $(P_n)_{n\geq 0}$ of polynomials in $\mathbf{Z}[X]$ with $P_n$ of degree $\leq d_n$ and size $t(P_n) \leq t_n$ such that, for all sufficiently large integer $n$,*

$$|P_n(\vartheta)| \leq e^{-\gamma(d_n t_n + d_{n+1}t_n + d_n t_{n+1})}.$$

*Then $\vartheta$ is algebraic and $P_n(\vartheta) = 0$ for all sufficiently large $n$.*

A consequence is Lemma 3.5 of [11].

**Corollary 26.** *Let $\vartheta \in \mathbf{C}$ and let $\sigma(n)$ be a non–decreasing unbounded positive real function. Assume that there exists a sequence $(P_n)_{n\geq 0}$ of polynomials in $\mathbf{Z}[X]$ with $P_n$ of size $t(P_n) \leq \sigma(n)$ such that, for all sufficiently large integer $n$,*

$$|P_n(\vartheta)| \leq e^{-5\sigma(n+1)^2}.$$

*Then $\vartheta$ is algebraic and $P_n(\vartheta) = 0$ for all sufficiently large $n$.*

This result is useful to prove that in some given set of specific numbers, at least two numbers are algebraically independent ([11] § 3.3 Prop. 3.3).

**Corollary 27.** *Let $\vartheta_1, \ldots, \vartheta_m$ be complex numbers* $\mathbf{C}$. *Let $\sigma(n)$ and $\lambda(n)$ be two non–decreasing positive real function with $\lim_{n\to\infty} \sigma(n) = \infty$ and $\lim_{n\to\infty} \lambda(n)/\sigma(n+1)^2 = \infty$. Assume that there exists a sequence $(P_n)_{n\geq 0}$ of polynomials in $\mathbf{Z}[X_1, \ldots, X_m]$, with $P_n$ of degree $\leq \sigma(n)$ and height $H(P_n) \leq e^{\sigma(n)}$, such that, for all sufficiently large $n$,*

$$0 < |P_n(\vartheta_1, \ldots, \vartheta_m)| \leq e^{-\lambda(n)}.$$

*Then at least two of the numbers $\vartheta_1, \ldots, \vartheta_m$ are algebraically independentl.*

One should stress the following differences with Corollary 23: the conclusion of Theorem 25 is that the transcendence degree of the field $\mathbf{Q}(\vartheta_1, \ldots, \vartheta_m)$ is at least 2, while Liouville's argument shows only that it is at least 1. There is a price for that. On the one hand, the assumption $\lim_{n\to\infty} \lambda(n)/\sigma(n+1)^2 = \infty$ is stronger than the assumption $\lim_{n\to\infty} \lambda(n)/\sigma(n) = \infty$ in Corollary 23 (what is important is the square, not the $n+1$ in place of $n$). On the other hand, Liouville's assumption is assumed to be satisfied for infinitely many $n$, while Gel'fond requires it for all sufficiently large $n$.

## 4.2 Large transcendence degree

It took some time before an extension of Gel'fond's transcendence criterion could be extended into a criterion for large transcendence degree. One approach suggested by S. Lang [7] involves his so-called *transcendence type* (see [11] § 7.3): this is an assumption which amounts to avoid Liouville type numbers. The idea is to prove algebraic independence by induction, but the results which are obtained in this way are comparatively weak.

One might hope that assuming $\lim_{n\to\infty} \lambda(n)/\sigma(n+1)^k = \infty$ in Corollary 27 would suffice to prove that the transcendence degree of the field $\mathbf{Q}(\vartheta_1, \ldots, \vartheta_m)$ is at least $k$. However this is not the case, as an example from Khinchine (reproduced in Cassels book on Diophantine approximation) shows. The first one to obtain a criterion for large transcendence degree was G.V. Chudnovskii in 1976. The original criterion was not sharp, the estimate for the transcendence degree was the logarithm of the expected one. A few years later Philippon reached the optimal exponent.

One of the main tools, in Nesterenko's proof of his main result (Theorem 4.2 in [11]), is this criterion for algebraic independence due to Philippon ([11] Chap. 6). Here is Corollary 6.2 of [11]. See also [12, 9].

**Theorem 28.** *Let $\vartheta_1, \ldots, \vartheta_m$ be complex numbers, $\sigma(n)$ and $S(n)$ be two non–decreasing positive real functions and $k$ be a real number in the range $1 \leq k \leq m$. Assume that the functions*

$$\sigma(n) \quad \text{and} \quad \frac{S(n-1)}{\sigma(n)^k}$$

*are non–decreasing and unbounded. Assume, further, that there exists a constant $c_0$ and a sequence $(P_n)_{n\geq 0}$ of polynomials in $\mathbf{Z}[X]$ with $P_n$ of size $t(P_n) \leq \sigma(n)$ such that, for all sufficiently large $n$,*

$$e^{-c_0 S(n-1)} < |P_n(\vartheta_1, \ldots, \vartheta_m)| \leq e^{-S(n)}.$$

*Then the transcendence degree over $\mathbf{Q}$ of the field $\mathbf{Q}(\vartheta_1, \ldots, \vartheta_m)$ is $> k-1$.*

The special case $k = 1$ of this result is close to (but weaker than) Corollary 23, the special case $k = 2$ of this result is close to (but weaker than) Theorem 25 (where no lower bound was requested).

It is interesting to compare with the following criterion for algebraic independence (Corollary 3.6 of [1]), which is a corollary of Theorem 18.

**Corollary 29.** *Let $\vartheta_1, \ldots, \vartheta_t$ be real numbers and $(\tau_d)_{d\geq 1}$, $(\eta_d)_{d\geq 1}$ two sequences of positive real numbers satisfying*

$$\frac{\tau_d}{d^{t-1}(1+\eta_d)} \longrightarrow +\infty.$$

*Further, let $\sigma(n)$ be a non–decreasing unbounded positive real function. Assume that for all sufficiently large $d$, there is a sequence $(P_n)_{n\geq n_0(d)}$ of polynomials in $\mathbf{Z}[X_1, \ldots, X_t]$, where $P_n$ has degree $\leq d$ and length $\leq e^{\sigma(n)}$, such that, for $n \geq n_0(d)$,*

$$e^{-(\tau_d+\eta_d)\sigma(n)} \leq |P_n(\vartheta_1, \ldots, \vartheta_t)| \leq e^{-\tau_d \sigma(n+1)}.$$

*Then $\vartheta_1, \ldots, \vartheta_t$ are algebraically independent.*

The proof of Corollary 29 is much easier than the proof of Theorem 28, since it relies on linear elimination instead of polynomial elimination. Unfortunately, Corollary 29 does not seem to suffice for the proof of Nesterenko's algebraic independence Theorem on $q$, $P(q)$, $Q(q)$ and $R(q)$ (Theorem 4.2 of [11]).

**Exercise**. *Let $\vartheta_1, \ldots, \vartheta_m$ be complex numbers and $d$ a positive integer. Check that the following conditions are equivalent.*

*(i) There exists a non–zero polynomial* $A \in \mathbf{Q}[X_1, \ldots, X_m]$ *of degree* $\leq d$ *such that* $A(\vartheta_1, \ldots, \vartheta_m) = 0$.
*(ii) The dimension of the* $\mathbf{Q}$*–vector space spanned by the numbers*

$$\theta_1^{i_1} \cdots \theta_m^{i_m}, \quad (i_1 + \cdots + i_m \leq n)$$

*is bounded from above by*

$$d\frac{n^{m-1}}{(m-1)!} + \mathrm{O}(n^{m-1})$$

*as* $n \to \infty$.

## Appendix: the resultant of two polynomials in one variable

The main tool for the proof of Gel'fond's criterion is the resultant of two polynomials in one variable.

Given two linear equations in two unknowns

$$\begin{cases} a_1 x + b_1 y = c_1, \\ a_2 x + b_2 y = c_2, \end{cases}$$

in order to compute $y$, one eliminates $x$. This amounts to find the projection on the $y$ axis of the intersection point $(x, y)$ of two lines in the plane. More generally, linear algebra enables one to find the intersection point (unique in general) of $n$ hyperplanes in dimension $n$ by means of a determinant.

Given two plane curves

$$f(x, y) = 0 \quad \text{and} \quad g(x, y) = 0$$

without common components, there are only finitely many intersection points; the values $y$ of the coordinates $(x, y)$ of these points are roots of a polynomial $R$ in $K_0[Y]$, where $K_0$ is the base field. This polynomial is computed by eliminating $x$ between the two equations $f(x, y) = 0$ and $g(x, y) = 0$. The ideal of $K_0[Y]$ which is the intersection of $K_0[Y]$ with the ideal of $K_0[X, Y]$ generated by $f$ and $g$ is principal, and $R$ is a generator: there is a pair $(U, V)$ of polynomials in $K_0[X, Y]$ such that $R = Uf + Vg$. If $(U, V)$ satisfies this *Bézout condition*, then so does $(U - Wg, V + Wf)$ for any $W$ in $K_0[X, Y]$. By Euclidean division in the ring $K_0[Y][X]$ of $U$ by $g$, one gets a solution $(U, V)$ with $\deg U < \deg g$, and then $\deg V < \deg f$. When $f$ and $g$ have no common factor, such a pair $(U, V)$ is unique up to a multiplicative constant. When $f$ and $g$ have their coefficients in a domain $A_0$ in place of a field $K_0$,

one takes for $K_0$ the quotient field of $A_0$ and one multiplies by a denominator, so that $U$ and $V$ can be taken as polynomials in $A_0[X,Y]$, and then $R \in A_0$.

The multiplicities of intersection of the two curves are reflected by the multiplicities of zeros of the roots of $R$ as a polynomial in $Y$.

It is useful to work with a ring $A$ more general than $A_0[Y]$. Let $A$ be a commutative ring with unit. Denote by $S$ the ring $A[X]$ of polynomials in one variable with coefficients in $A$. For $d$ a non-negative integer, let $S_d$ be the $A$–module of elements in $S$ of degree $\leq d$. Then $S_d$ is a free $A$–module of rank $d+1$ with a basis $1, X, \ldots, X^d$.

Let $P$ and $Q$ be polynomials of degrees $p$ and $q$ respectively

$$P(X) = a_0 + a_1 X + \cdots + a_p X^p, \qquad Q(X) = b_0 + b_1 X + \cdots + b_q X^q.$$

The homomorphism of $A$–modules

$$\begin{array}{ccc} S_{q-1} \times S_{p-1} & \longrightarrow & S_{p+q-1} \\ (U,V) & \longmapsto & UP + VQ \end{array}$$

has the following matrix in the given bases:

$$\begin{pmatrix} a_0 & 0 & \cdot & \cdot & \cdot & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \cdot & \cdot & \cdot & 0 & b_1 & b_0 & \cdots & 0 \\ \vdots & \vdots & \cdot & \cdot & \cdot & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{p-1} & a_{p-2} & \cdot & \cdot & \cdot & 0 & b_{p-1} & b_{p-2} & \cdots & b_0 \\ a_p & a_{p-1} & \cdot & \cdot & \cdot & 0 & b_p & b_{p-1} & \cdots & b_1 \\ 0 & a_p & \cdot & \cdot & \cdot & 0 & b_{p+1} & b_p & \cdots & b_2 \\ \vdots & \vdots & \cdot & \cdot & \cdot & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdot & \cdot & \cdot & a_0 & b_{q-1} & b_{q-2} & \cdots & b_{q-p} \\ 0 & 0 & \cdot & \cdot & \cdot & a_1 & b_q & b_{q-1} & \cdots & b_{q-p+1} \\ 0 & 0 & \cdot & \cdot & \cdot & a_2 & 0 & b_q & \cdots & b_{q-p+2} \\ \vdots & \vdots & \cdot & \cdot & \cdot & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdot & \cdot & \cdot & a_p & 0 & 0 & \cdots & b_q \end{pmatrix}$$

The $q$ first columns are the components, in the basis $(1, X, \ldots, X^{p+q-1})$, of $P, XP, \ldots, X^{q-1}P$, while the $p$ last columns are the components, in the same basis, of $Q, XQ, \ldots, X^{p-1}Q$. The main diagonal is $(a_0, \ldots, a_0, b_q, \ldots, b_q)$.

*Definition.* The *resultant* of $P$ and $Q$ is the determinant of this matrix. We denote it by $\mathrm{Res}(P,Q)$. The *universal resultant* is the resultant of the two polynomials

$$U_0 + U_1 X + \cdots + U_p X^p, \quad \text{et} \quad V_0 + V_1 X + \cdots + V_q X^q,$$

in the ring $A_{pq} = \mathbf{Z}[U_0, U_1, \ldots, U_p, V_0, V_1, \ldots, V_q]$ of polynomials with coefficients in $\mathbf{Z}$ in $p+q+2$ variables. One deduces the resultant of $P$ and $Q$ by *specialisation*, i.e. as the image under the canonical homomorphism from $A_{pq}$ to $A$ which maps $U_i$ to $a_i$ and $V_j$ to $b_j$. When the characteristic is 0, this canonical homomorphism is injective.

The above determinant suffices to deduce:

**Proposition 30.** *The universal resultant is a polynomial in*

$$U_0, U_1, \ldots, U_p, V_0, V_1, \ldots, V_q$$

*which is homogeneous of degree $q$ in $U_0, \ldots, U_p$, and homogeneous of degree $p$ in $V_0, \ldots, V_q$.*

**Proposition 31.** *There exist two polynomials $U$ and $V$ in $S$, of degrees $< q$ and $< p$ respectively, such that the resultant $R = \mathrm{Res}(P, Q)$ of $P$ and $Q$ can be written $R = UP + VQ$.*

It follows that if $P$ and $Q$ have a common zero in some field containing $A$, then $\mathrm{Res}(P, Q) = 0$. The converse is true. It uses the following easy property, whose is left as an exercise.

**Proposition 32.** *Let $A_0$ be a ring, $A = A_0[Y_1, \ldots, Y_n]$ the ring of polynomials in $n$ variables with coefficients in $A_0$, and $P$, $Q$ elements in $A_0[Y_0, \ldots, Y_n]$, homogeneous of degrees $p$ and $q$ respectively. Consider $P$ and $Q$ as elements in $A[Y_0]$ and denote by $R = \mathrm{Res}_{Y_0}(P, Q) \in A$ their resultant with respect to $Y_0$. Then $R$ is homogeneous of degree $pq$ in $Y_1, \ldots, Y_n$.*

From these properties we deduce:

**Proposition 33.** . – *If*

$$P(X) = a_0 \prod_{i=1}^{p} (X - \alpha_i) \quad \textit{and} \quad Q(X) = b_0 \prod_{j=1}^{q} (X - \beta_j),$$

*then*

$$\begin{aligned} \mathrm{Res}(P, Q) &= a_0^q b_0^p \textstyle\prod_{i=1}^{p} \prod_{j=1}^{q} (\alpha_i - \beta_j) \\ &= (-1)^{pq} b_0^p \textstyle\prod_{j=1}^{q} P(\beta_j) \\ &= a_0^q \textstyle\prod_{i=1}^{p} Q(\alpha_i). \end{aligned}$$

*Proof.* Without loss of generality one, may assume that $A$ is the ring of polynomials with coefficients in $\mathbf{Z}$ in the variables $a_0, b_0, \alpha_1, \ldots, \alpha_p, \beta_1, \ldots, \beta_q$. In this factorial ring, $\alpha_i - \beta_j$ is an irreducible element which divides $R = \mathrm{Res}(P, Q)$ (indeed, if one specializes $\alpha_i = \beta_j$, then the resultant vanishes). Now

$$a_0^q b_0^p \prod_{i=1}^{p} \prod_{j=1}^{q} (\alpha_i - \beta_j)$$

is homogenous of degree $q$ in the coefficients of $P$ and of degree $p$ in the coefficients of $Q$. Therefore it can be written $cR$ with some $c \in \mathbf{Z}$. Finally the coefficient of the monomial $a_0^p b_0^q$ is 1, hence $c = 1$. □

**Corollary 34.** *Let $K$ be a field containing $A$ in which $P$ and $Q$ completely split in factors of degree* 1. *Then the resultant* $\mathrm{Res}(P, Q)$ *is zero if and only if $P$ and $Q$ have a common zero in $K$.*

**Corollary 35.** *If the ring $A$ is factorial, then* $\mathrm{Res}(P, Q) = 0$ *if and only if $P$ and $Q$ have a common irreducible factor.*

## References


[1] A. Chantanasiri, *On the criteria for linear independence of Nesterenko, Fischler and Zudilin.* 13 p. `arXiv:0912.4904v1 (math.NT)`.

[2] A. Durand, *Un critère de transcendance*, in Séminaire Delange-Pisot-Poitou (15e année: 1973/74), Théorie des nombres, Fasc. 2, Exp. No. G11, Secrétariat Mathématique, Paris, 1975, p. 9.

[3] ——, *Indépendance algébrique de nombres complexes et critère de transcendance*, Compositio Math., 35 (1977), pp. 259–267.

[4] N. I. Fel′dman and Y. V. Nesterenko, *Transcendental numbers*, in Number Theory, IV, vol. 44 of Encyclopaedia Math. Sci., Springer, Berlin, 1998.

[5] S. Fischler and W. Zudilin, *A refinement of Nesterenko's linear independence criterion with applications to zeta values.* `http://www.mpim-bonn.mpg.de/preprints/send?bid=4020`.

[6] C. Hermite, *Sur la fonction exponentielle*, C. R. Acad. Sci. Paris, 77 (1873), pp. 18–24, 74–79, 226–233, 285–293. Œuvres de Charles

Hermite, Paris: Gauthier-Villars, 1905-1917. University of Michigan Historical Math Collection
http://name.umdl.umich.edu/AAS7821.0001.001.

[7] S. Lang, *Introduction to transcendental numbers*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1966. Collected papers. Vol. I (1952–1970), Springer–Verlag 2000, p. 396–506.

[8] M. Laurent, *Cours de DEA à l'Université de Marseille, IML (Institut de Mathématiques de Luminy)*. Unpublished manuscript notes, 2007.

[9] Y. Nesterenko and P. Philippon, eds., *Introduction to algebraic independence theory*, vol. 1752 of Lecture Notes in Mathematics, Springer-Verlag, Berlin, 2001.

[10] Y. V. Nesterenko, *Linear independence of numbers*, Vestnik Moskov. Univ. Ser. I Mat. Mekh., (1985), pp. 46–49, 108.

[11] ——, *Algebraic Independence*, TIFR Mumbai - Narosa, 2009.

[12] D. Roy, *Philippon's criterion for algebraic independence (lectures 3 and 4)*. Summer School in Analytic Number Theory and Diophantine Approximation University of Ottawa, Ontario Canada, June 30-July 11, 2008
http://aix1.uottawa.ca/∼droy/summer-school-2008/droy_lecture3-4.pdf.

[13] W. M. Schmidt, *Diophantine approximation*, vol. **785**, Lecture Notes in Mathematics. Berlin-Heidelberg-New York: Springer-Verlag, 1980, new ed. 2001.

[14] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abhandlungen Akad. Berlin, Nr. 1 (1929), p. 70 S.

[15] M. Waldschmidt, *Nombres transcendants*, Springer-Verlag, Berlin, 1974. Lecture Notes in Mathematics, Vol. 402.

[16] ——, *Diophantine approximation on linear algebraic groups*, vol. 326 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Springer-Verlag, Berlin, 2000. Transcendence properties of the exponential function in several variables.

[17] ——, *An introduction to irrationality and transcendence methods*. Course at the 2008 Arizona Winter School and Ottawa Fields Institute.
http://people.math.jussieu.fr/∼miw/articles/pdf/Ottawa2008part1.pdf

http://people.math.jussieu.fr/∼miw/articles/pdf/Ottawa2008part2.pdf,
2008.

Michel WALDSCHMIDT
Université P. et M. Curie (Paris VI)
Institut Mathématique de Jussieu
Problèmes Diophantiens, Case 247
4, Place Jussieu
75252 Paris CEDEX 05, France
miw@math.jussieu.fr

http://www.math.jussieu.fr/∼miw/

This text is available on the internet at the address
http://www.math.jussieu.fr/∼miw/enseignements.html