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

updated: December 10, 2009

Criteria for irrationality, linear independence, transcendence and algebraic independence

Michel Waldschmidt

Part I: courses of 03/12/2009 and 07/12/2009

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 [4].

1 Irrationality Criteria

1.1 Statement of the first criterion

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

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

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

$$L_0(X_0, X_1) = a_0 X_0 + b_0 X_1 \quad \textit{and} \quad L_1(X_0, X_1) = a_1 X_0 + b_1 X_1,$$

with rational integer coefficients, such that

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

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

(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*

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

(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), (iv) and (iv) is well known. See for instance [6]. See also [7].

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 [5]. See also [6]. Notice that an easy consequence of (iv) is the following statement, which is 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 $Q \ge 1/\epsilon$, 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 ϵ 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 (i) 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 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 $p = \lfloor q\vartheta \rfloor + 1$. Then we have $1 \leq q \leq N-1 < Q$ and

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

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 [5] states that for any real number x, 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

$$\left|\vartheta - \frac{p}{q}\right| \le \frac{1}{qQ}\cdot$$

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 x 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 $b \ge 3$, strict inequality holds for $Q = b$, but not for $Q = b - 1$.

However, when Q is an integer and ϑ 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

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

or $\mathbf{R}^2$ is convex, symmetric and has volume > 4. By Minkowski's Convex Body Theorem (Theorem 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 $|x_0\vartheta - x_1| \le 1/Q + \epsilon$ for all $\epsilon > 0$. Since this is true for all $\epsilon > 0$, we deduce $|x_0\vartheta - x_1| \le 1/Q$. Finally, since ϑ is irrational, we also have $|x_0\vartheta - x_1| \ne 1/Q$. □

1.2 Irrationality of at least one number

Proposition 3. *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 $\mathbf{Z}$ with $q > 0$ such that*

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

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

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

(iv) *For any real number $Q > 1$, there exists $p_1, \ldots, p_m, q$ 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 there exist $p_1, \ldots, p_m$ 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 $\{q_1, \ldots, q_N\}$ be a finite set of positive integers. Using (iv) again, we show that there exists a positive integer $q \notin \{q_1, \ldots, q_N\}$ satisfying the condition (v). Denote by $\| \cdot \|$ the distance to the nearest integer: for $x \in \mathbf{R}$,

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

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

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

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

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

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

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 $L_i(X_0, \dots, X_m) = p_i X_0 - q X_i$ 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 ϵ 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

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

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 [5] 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 [5] 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 [5] 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

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

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 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 [5]).

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 [5] Chap. II § 2 Th. 2C) is the following result.

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

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

and

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

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

Here is a consequence of Theorem 8

Corollary 9. *Let $\vartheta_1, \dots, \vartheta_m$ be real numbers. For any real number $Q > 1$, there exists $p_1, \dots, p_m, q$ 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 $-\vartheta_m X_0 + X_i$ ($1 \leq i \leq m$), and with $A_0 = Q$, $A_1 = \cdots = A_m = Q^{-1/m}$.

□

Proof of (i) $\Rightarrow$ (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' 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 [2] and [1] 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 lossed 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 [3].

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 ϵ *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

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

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 Proposition 10. Let

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

be a non–zero linear form with integer coefficients. For sufficiently small ϵ, 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

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

□

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

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

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

If $V_\epsilon \neq \mathbf{Q}^{m+1}$, then there is a hyperplane $a_0x_0 + a_1x_1 + \cdots + a_mx_m = 0$ containing E_ϵ. Any $\mathbf{u} = (q, p_1, \dots, p_m)$ in E_ϵ has

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

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

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

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

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

The right hand side tends to 0 as n tends to infinity, hence the left hand side vanishes, and $1, \vartheta_1, \dots, \vartheta_m$ 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_ϵ.

□

References

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

[2] 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`.

[3] M. Laurent, *Cours de DEA à l'université de Marseille, Institut de Mathématiques de Luminy*. 2007, unpublished manuscript notes.

[4] Y. V. Nesterenko, *Algebraic Independence*, TIFR Mumbai - Narosa, 2009.

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

[6] M. Waldschmidt, *An introduction to irrationality and transcendence methods*. Course at the 2008 Arizona Winter School and Ottawa Fields Institute in 2008.
http://people.math.jussieu.fr/∼miw/articles/pdf/Ottawa2008part1.pdf
http://people.math.jussieu.fr/∼miw/articles/pdf/Ottawa2008part2.pdf.

[7] ——, *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.

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/