Updated: *May 16, 2010*

Diophantine approximation, irrationality and transcendence

Michel Waldschmidt

Course N°2, *April 19, 2010*

These are informal notes of my course given in April – June 2010 at IMPA (*Instituto Nacional de Matematica Pura e Aplicada*), Rio de Janeiro, Brazil.

2 Irrationality Criteria

2.1 Statement of a criterion

Proposition 4. *Let ϑ be a real number. The following conditions are equivalent:*
(i) *ϑ is irrational.*
(ii) *For any $\epsilon > 0$, there exists $(p, q) \in \mathbf{Z}^2$ such that $q > 0$ and*

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

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

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

with rational integer coefficients, such that

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

(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*

$$0 < |q\vartheta - p| < \frac{1}{Q}\cdot$$

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

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

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

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

The implication (vi) $\Rightarrow$ (v) is trivial. We shall prove (i) $\Rightarrow$ (vi) later (in the section on continued fractions). We now prove the equivalence between the other conditions of Proposition 4 as follows:

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

Notice that given a positive integer q, there is at most one value of p such that $|q\vartheta - p| < 1/2$, namely the nearest integer to $q\vartheta$. Hence, when we approximate ϑ by a rational number p/q, we have only one free parameter in $\mathbf{Z}_{>0}$, namely q.

In condition (v), there is no need to assume that the left hand side is not 0: if one $p/q \in \mathbf{Q}$ produces 0, then all other ones do not, and there are again infinitely many of them.

Proof of (iv) $\Rightarrow$ (ii). Using (iv) with Q satisfying $Q > 1$ and $Q \geq 1/\epsilon$, we get (ii). $\square$

Proof of (v) $\Rightarrow$ (ii). According to (v), there is an infinite sequence of distinct rational numbers $(p_i/q_i)_{i\geq 0}$ with $q_i > 0$ such that

$$\left|\vartheta - \frac{p_i}{q_i}\right| < \frac{1}{\sqrt{5}q_i^2}\cdot$$

For each q_i, there is a single value for the numerator p_i for which this inequality is satisfied. Hence the set of q_i is unbounded. Taking $q_i \geq 1/\epsilon$ yields (ii). $\square$

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

$$0 < |q'\vartheta - p'| < |q\vartheta - p|. \tag{5}$$

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 (5). $\square$

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.

$\square$

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 $N \geq 2$.

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

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

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

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

$\square$

Remark. Theorem 1.A in Chap. II of [32] states that for any real number ϑ, 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 ϑ 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 $b \ge 2$, 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 ϑ is irrational, the number $|q\vartheta - p|$ is irrational (recall that $q > 0$), hence not equal to $1/Q$.

Proof of (iv) $\Rightarrow$ (v). Assume (iv). We already know that (iv) $\Rightarrow$ (i), hence ϑ is irrational.

Let $\{q_1, \dots, q_N\}$ be a finite set of positive integers. We are going to 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 $x \in \mathbf{R}$,

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

Since ϑ is irrational, it follows that for $1 \le j \le N$, the number $\|q_j\vartheta\|$ is non–zero. Let $Q > 1$ satisfy

$$Q > \left(\min_{1 \le j \le N} \|q_j\vartheta\|\right)^{-1}.$$

From (iv) we deduce that there exists an integer q in the range $1 \le q < Q$ such that

$$0 < \|q\vartheta_i\| \le \frac{1}{Q}\cdot$$

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

In the next section, we give another proof of (i) $\Rightarrow$ (iv) which rests on *Minkowski geometry of numbers.*

2.2 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 $\mathbf{e} = \{e_1, \ldots, e_n\}$ of G the parallelogram

$$P_{\mathbf{e}} = \{x_1 e_1 + \cdots + x_n e_n \; ; \; 0 \leq x_i < 1 \; (1 \leq i \leq n)\}$$

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

$$\mathbf{R}^n = \bigcup_{g \in G} (P_{\mathbf{e}} + g) \tag{6}$$

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 7 (Minkowski). *Let G be a lattice in $\mathbf{R}^n$ and B a measurable subset of $\mathbf{R}^n$. Assume $\mu(B) > v(G)$. Then there exist $x \neq y$ in B such that $x - y \in G$.*

Proof. From (6) 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 $x - y = g - g' \in G \setminus \{0\}$. $\square$

From Theorem 7 we deduce Minkowski's convex body Theorem (Theorem 2B, Chapter II of [32]).

Corollary 8. *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 7 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 7 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 $(2x - 2y)/2 = x - y \in G \cap B \setminus \{0\}$.

□

Corollary 9. *With the notations of Corollary 8, 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.*

Proof. Assume $\mu(B) = 2^n v(G)$. For $\epsilon > 0$, set $B_\epsilon = (1+\epsilon)B = \{(1+\epsilon)t \; ; \; t \in B\}$. Since $\mu(B_\epsilon) > 2^n v(G)$, we deduce from Corollary 8 $B_\epsilon \cap G \neq \{0\}$. Since B_ϵ is compact and G discrete, $B_\epsilon \cap G \setminus \{0\}$ is a finite non–empty set. Also

$$B_{\epsilon'} \cap G \subset B_\epsilon \cap G$$

for $\epsilon' < \epsilon$. Hence there exists $t \in G \setminus \{0\}$ such that $t \in B_\epsilon$ for all $\epsilon > 0$. Define $t_\epsilon \in B$ by $t = (1+\epsilon)t_\epsilon$. Since B is compact, there is a sequence $\epsilon_n \to 0$ such that t_{ϵ_n} has a limit in B. But $\lim_{\epsilon \to 0} t_\epsilon = t$. Hence $t \in B$.

□

Remark. The example of $G = \mathbf{Z}^n$ and $B = \big\{(x_1, \ldots, x_n) \in \mathbf{R}^n \; ; \; |x_i| < 1\big\}$ shows how sharp are Corollaries 8 and 9.

Minkowski's Linear Forms Theorem (see, for instance, [32] Chap. II § 2 Th. 2C) is the following result.

Theorem 10 (Minkowski's Linear Forms Theorem)**.** *Suppose that ϑ_{ij} ($1 \leq i, j \leq n$) are real numbers with determinant ± 1 . Suppose that $A_1, \ldots, A_n$ 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 8 with A_n replaced with $A_n + \epsilon$ for a sequence of ϵ which tends to 0. $\square$

Here is a consequence of Theorem 10

Corollary 11. *Let $\vartheta_1, \dots, \vartheta_m$ be real numbers. For any real number $Q > 1$, there exist $p_1, \dots, p_m, q$ in $\mathbf{Z}$ such that $1 \le q < Q$ and*

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

Proof of Corollary 11. We apply Theorem 10 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 $-\vartheta_i X_0 + X_i$ $(1 \le i \le m)$, and with $A_0 = Q$, $A_1 = \cdots = A_m = Q^{-1/m}$.

$\square$

Proof of (i) $\Rightarrow$ (iv) *in Proposition 4 using Minkowski's geometry of numbers.* Let $\epsilon > 0$. The subset

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

of $\mathbf{R}^2$ is convex, symmetric and has volume > 4. By Minkowski's Convex Body Theorem (Corollary 8 below), it contains a non–zero element in $\mathbf{Z}^2$. Since $\mathcal{C}_\epsilon$ is also bounded, the intersection $\mathcal{C}_\epsilon \cap \mathbf{Z}^2$ is finite. Consider a non–zero element (x_0, x_1) in this intersection with $|x_0 \vartheta - x_1|$ minimal. Then $(x_0, x_1) \in \mathcal{C}_\epsilon$ for all $\epsilon > 0$, hence $|x_0 \vartheta - x_1| \le 1/Q + \epsilon$ 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 $|x_0 \vartheta - x_1| \ne 1/Q$. $\square$

2.3 Irrationality of at least one number

Proposition 12. *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*

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

(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*

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

(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*

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

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

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

We shall prove Proposition 12 in the following way:

$$\begin{tikzcd}
\text{(i)} \arrow[r, Rightarrow] & \text{(iv)} \arrow[dr] & \\
& & \text{(v)} \arrow[dl] \\
\text{(iii)} \arrow[uu, Rightarrow] & \text{(ii)} \arrow[l, Rightarrow] &
\end{tikzcd}$$

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

$$\max_{1 \le i \le m} |q\vartheta_i - p_i| < \frac{1}{b}$$

implies $q\vartheta_i - p_i = 0$ for $1 \le i \le m$, 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 are going to show that there exists a positive integer $q \notin \{q_1, \ldots, q_N\}$ satisfying the condition (v). Recall that $\|\cdot\|$ denotes the distance to the nearest integer. 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 $q \notin \{q_1, \dots, q_N\}$.
$\square$

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 $L_i(X_0, \dots, X_m) = p_i X_0 - qX_i$ 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 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

$$0 < \max_{1 \le i \le m} |q'\vartheta_i - p'_i| < \max_{1 \le i \le m} |q\vartheta_i - p_i|. \tag{13}$$

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 (13).
$\square$

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

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

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

$\square$

Proof of (i) $\Rightarrow$ (iv). Use Corollary 11. From the assumption (i) we deduce

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

$\square$

Remark. This proof of the implication (i) $\Rightarrow$ (iv) in Proposition 12 (compare with [32] Chap. II § 2 p. 35) relies on 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 [32] 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 [32] Chap. II § 2 p. 32.

3 Criteria for linear independence

3.1 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, under certain conditions, the number

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

is not 0.

Hermite's idea (see [18] and [13] 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 14 below) that nothing is lost by using such arguments: existence of linearly independent simultaneous rational approximations for $\vartheta_1, \ldots, \vartheta_m$ are characteristic of linearly independent real numbers $1, \vartheta_1, \ldots, \vartheta_m$.

3.2 Rational approximations

The following criterion is due to M. Laurent [22].

Proposition 14. *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*

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

with $q_i > 0$, *such that*

$$\max_{1 \leq k \leq m} \left| \vartheta_k - \frac{p_{ki}}{q_i} \right| \leq \frac{\epsilon}{q_i} \quad (0 \leq i \leq m). \tag{15}$$

The condition of linear independence on 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 (15) in Proposition 14 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) $\Rightarrow$ (i) . We shall prove a more explicit version of it by checking that *any tuple* $(q, p_1, \ldots, p_m) \in \mathbf{Z}^{m+1}$*, with* $q > 0$*, producing a tuple* $(p_1/q, \ldots, p_m/q) \in \mathbf{Q}^m$ *of sufficiently good rational approximations to* $\underline{\vartheta}$ *satisfies the same linear dependence relations as* $1, \vartheta_1, \ldots, \vartheta_m$.

Lemma 16. *Let* $\vartheta_1, \ldots, \vartheta_m$ *be real numbers. Assume that the numbers* $1, \vartheta_1, \ldots, \vartheta_m$ *are linearly dependent over* $\mathbf{Q}$*: let* $a, b_1, \ldots, b_m$ *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 $(q, p_1, \ldots, p_m) \in \mathbf{Z}^{m+1}$ *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

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

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

$\square$

Proof of (ii) $\Rightarrow$ (i) *in Proposition 14.* 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 16. Since $\mathbf{u}_0, \ldots, \mathbf{u}_m$ is a basis of $\mathbf{Q}^{m+1}$, one at least of the $L(\mathbf{u}_i)$ is not 0. Hence Lemma 16 implies

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

$\square$

Proof of (i) $\Rightarrow$ (ii) *in Proposition 14.* Let $\epsilon > 0$. By Corollary 11, there exists $\mathbf{u} = (q, p_1, \ldots, p_m) \in \mathbf{Z}^{m+1}$ with $q > 0$ such that

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

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 $\mathbf{u} = (q, p_1, \ldots, p_m)$ in E_ϵ has

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

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

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

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.

$\square$

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/enseignement.html