`Updated:` *May 16, 2010*

Diophantine approximation, irrationality and transcendence

Michel Waldschmidt

Course N°3, *April 26, 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.

3.3 Linear forms

3.3.1 Siegel's method: $m+1$ linear forms

For proving linear independence of real numbers, Hermite [18] considered simultaneous approximation to these numbers by algebraic numbers. The point of view introduced by Siegel in 1929 [34] 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 17. *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 [34]; see also [13] Chap. 2 § 1.4 and [6]. 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 Λ_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 17, select m of them, say $\Lambda_1,\dots,\Lambda_m$, which form with Λ_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 Δ as a linear combination with integer coefficients of $\Lambda_k(1,\vartheta_1,\dots,\vartheta_m)|$, $1\le k\le m$. The choice of ϵ yields the contradiction $|\Delta|<1$.

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

Proposition 18. *Let $\vartheta_1,\dots,\vartheta_m$ be complex numbers and $L_0,\dots,L_m$ be $m+1$ linearly independent linear forms in $m+1$ variables with coefficients in $\mathbf{Z}$. Then*

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

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

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

Define $\vartheta_0=1$. Let $\underline{\mathrm{L}}$ be the regular $(m+1)\times(m+1)$ matrix $\bigl(\ell_{ki}\bigr)_{0\le k,i\le m}$. 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 λ_k is $\le m!H(L_0)\cdots H(L_m)/H(L_k)$. We deduce

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

Proposition 18 follows.

□

An straightforward consequence of Proposition 18 is the following:

Corollary 19. *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*

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

Using either Proposition 18 or Corollary 19, we deduce the following result (compare with [27] Lemma 2.4):

Corollary 20. *Let $\vartheta_1, \ldots, \vartheta_m$ be complex numbers and $\kappa \geq 0$ be a real number. 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*

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

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

Under the assumptions of Corollary 20, since $r \leq m$, we deduce $\kappa < m$, which is a plain consequence of Corollary 19.

We recover Lemma 17 by taking $\kappa = m - 1$.

Also we recover the implication (iii) $\Rightarrow$ (i) from Proposition 12 by taking $\kappa = 0$.

Proof. We give two slightly different proofs of Corollary 20. For the first one, we use Proposition 18 as follows: consider $m - r$ linearly independent linear relations among $1, \vartheta_1, \ldots, \vartheta_m$. Denote by $\widetilde{L}_{r+1}, \ldots, \widetilde{L}_m$ these linear forms and by c their maximal height. Take $0 < \epsilon < 1/((m+1)!c^{m-r})$. Select $r+1$ linear forms $\widetilde{L}_0, \ldots, \widetilde{L}_r$ among $L_0, \ldots, L_m$ to get a maximal system of $m+1$ linearly independent linear forms $\widetilde{L}_0, \ldots, \widetilde{L}_m$. From Proposition 18 one deduces

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

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

Our second proof of Corollary 20 rests on Corollary 19. Let $1, \xi_1, \ldots, \xi_r$ be a basis of the $\mathbf{Q}$–vector space spanned by $1, \vartheta_1, \ldots, \vartheta_m$. Define $\xi_0 = \vartheta_0 = 1$ and write

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

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 ϵ 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 20. 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 19 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 ϵ, one concludes $H^\kappa < H^r$, hence $r > \kappa$.

Corollary 20 follows.

$\square$

3.3.2 Nesterenko's Criterion for linear independence

In 1985, Yu.V. Nesterenko [26], obtained a variant of Proposition 18 (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 assume an upper bound for the value of this linear form at the point $(1, \vartheta_1, \ldots, \vartheta_m)$, 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 18, 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 [15].

The main reference for this section is [6].

Theorem 21 (Nesterenko linear independence criterion). *Let c_1, c_2, τ_1, τ_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 $\underline{\vartheta} = (\vartheta_1, \ldots, \vartheta_m) \in \mathbf{R}^m$. 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

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

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 [6], which relies on the arguments in [15], is the following.

Theorem 22. *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 $A_n \le 2^{r_n+1}(B_nQ_n)^{r_n}$ for all sufficiently large integers n.

One deduces from Theorem 22 a slight refinement of Theorem 21 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 23. *Let τ_1, τ_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 22 are given in [6]. See also Corollary 33 below.

4 Criteria for transcendence

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

4.1 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 α is the unique irreducible polynomial $P \in \mathbf{Z}[X]$ which vanishes at α and has a positive leading coefficient.

The next lemma is one of many variants of Liouville's inequality (see, for instance, [21, 32, 38, 28, 27]), which is close to the original one of 1844.

Lemma 24. *Let α be an algebraic number of degree $d \geq 2$ 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 $q \geq q_0$,*

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

Proof. The result is trivial if α is not real: an admissible value for q_0 is

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

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

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

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

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

and

$$q^d P(p/q) = a_0 q^d \prod_{i=1}^{d}\left(\frac{p}{q} - \alpha_i\right). \tag{25}$$

Also

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

The left hand side of (25) is a rational integer. It is not zero because P is irreducible of degree ≥ 2. For $i \geq 2$ we use the estimate

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

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

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

□

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

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

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

The constant c can be explicitly computed (see, for instance, [13, 39]), but this is not relevant here.

The corollary below (which is [27] Prop. 3.1) is useful for proving transcendence results.

Corollary 27. *Let $\vartheta_1, \dots, \vartheta_m$ 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 $\mathbf{Z}[X_1, \dots, X_m]$, with P_n of degree $\leq \sigma(n)$ and height $H(P_n) \leq e^{\sigma(n)}$, such that, for infinitely many n,*

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

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

4.2 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 4 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 ϑ not being algebraic of degree $\leq d$ by considering algebraic approximation of ϑ 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 α 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 [9, 10].

Proposition 28. *Let ϑ be a complex number. The following conditions are equivalent:*
(i) *ϑ is transcendental.*
(ii) *For any $\kappa > 0$ there exists an algebraic number α 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 ϑ (resp. criteria for ϑ not being of degree $\leq d$) is to consider polynomial approximations $|P(\vartheta)|$ by polynomials in $\mathbf{Z}[X]$ (resp. by polynomials of degree $\leq d$).

5 Criteria for algebraic independence

5.1 Small transcendence degree: Gel'fond's criterion

Gel'fond's criterion (see, for instance, [21, 38, 28, 27]) 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 29 (Gel'fond's Transcendence Criterion). *Let $\vartheta \in \mathbf{C}$ and let γ 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 ϑ is algebraic and $P_n(\vartheta) = 0$ for all sufficiently large n.

A consequence of Theorem 29 is the following variant of Gel'fond's Criterion (Lemma 3.5 of [27]):

Corollary 30. *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 ϑ 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 ([27] § 3.3 Prop. 3.3).

Corollary 31. *Let $\vartheta_1, \ldots, \vartheta_m$ be complex numbers. 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 independent.

One should stress the following differences with Corollary 27: the conclusion of Theorem 29 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 27 (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.

5.2 Large transcendence degree

It took some time before Gel'fond's transcendence criterion could be extended into a criterion for large transcendence degree. One approach suggested by S. Lang [21] involves his so-called *transcendence type* (see [27] § 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 31 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's book on Diophantine approximation [5]) 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 [27]), is this criterion for algebraic independence due to Philippon ([27] Chap. 6). Here is Corollary 6.2 of [27]. See also [31, 28].

Theorem 32. *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 $1 \le k \le m$. Assume that the functions*

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

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

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

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 27, the special case $k = 2$ of this result is close to (but weaker than) Theorem 29 (where no lower bound was requested).

It is interesting to compare with the following criterion for algebraic independence (Corollary 3.6 of [6]), which is a corollary of Theorem 22.

Corollary 33. *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 33 is much easier than the proof of Theorem 32, since it relies on linear elimination instead of polynomial elimination. Unfortunately, Corollary 33 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 [27]).

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*

$$\vartheta_1^{i_1} \cdots \vartheta_m^{i_m} \quad (i_1 + \cdots + i_m \leq n)$$

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

$$\begin{cases} a_1x + b_1y = c_1, \\ a_2x + b_2y = c_2, \end{cases}$$

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 unity. 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 $\le d$. 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:

$$P(X) = a_0 + a_1X + \cdots + a_pX^p, \qquad Q(X) = b_0 + b_1X + \cdots + b_qX^q.$$

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: for q larger than p,

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

and for p larger than q,

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

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

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

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.

From the above expression of the resultant as a determinant, one deduces:

Proposition 34. *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 35. *There exist two polynomials U and V in $A[X]$, 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 proof is left as an exercise.

Proposition 36. *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 37. *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 $a_0, b_0, \alpha_1, \dots, \alpha_p, \beta_1, \dots, \beta_q$. 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 homogeneous 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 $c = 1$. $\square$

Corollary 38. *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 39. *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] M. Aigner and G. M. Ziegler, *Proofs from The Book*, Springer-Verlag, Berlin, fourth ed., 2010.

[2] C. Brezinski, *The long history of continued fractions and Padé approximants*, in Padé approximation and its applications (Amsterdam, 1980), vol. 888 of Lecture Notes in Math., Springer, Berlin, 1981, pp. 1–27.

[3] ——, *History of continued fractions and Padé approximants*, vol. 12 of Springer Series in Computational Mathematics, Springer-Verlag, Berlin, 1991.
`http://www.emis.de/cgi-bin/MATH-item?0714.01001`.

[4] Y. Bugeaud, *Approximation by algebraic numbers*, vol. 160 of Cambridge Tracts in Mathematics, Cambridge University Press, Cambridge, 2004.

[5] J. W. S. Cassels, *An introduction to Diophantine approximation*, Hafner Publishing Co., New York, 1972. Facsimile reprint of the 1957 edition, Cambridge Tracts in Mathematics and Mathematical Physics, No. 45.

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

[7] H. Cohn, *A short proof of the simple continued fraction expansion of* e, Amer. Math. Monthly, 113 (2006), pp. 57–62.
`arXiv:math/0601660`.

[8] J. Cosgrave, *New proofs of the irrationality of* e^2 *and* e^4.
`http://staff.spd.dcu.ie/johnbcos/transcendental_numbers.htm`
`http://staff.spd.dcu.ie/johnbcos/esquared.htm`.

[9] 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.
`http://www.numdam.org/numdam-bin/fitem?id=SDPP_1973-1974__15_2_A7_0`.

[10] ——, *Indépendance algébrique de nombres complexes et critère de transcendance*, Compositio Math., 35 (1977), pp. 259–267.
`http://www.numdam.org/numdam-bin/fitem?id=CM_1977__35_3_259_0`.

[11] L. Euler, *De fractionibus continuis dissertatio*, Commentarii Acad. Sci. Petropolitanae, 9 (1737), pp. 98–137. Opera Omnia Ser. I vol. 14, Commentationes Analyticae, p. 187–215.
Classification Ensetröm E71 – Archive Euler
`www.math.dartmouth.edu/∼euler/pages/E071.html`.

[12] P. Eymard and J.-P. Lafon, *The number* π, American Mathematical Society, Providence, RI, 2004. Translated from the 1999 French original by Stephen S. Wilson.

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

[14] S. Fischler, *Irrationalité de valeurs de zêta (d'après Apéry, Rivoal,...)*, Astérisque, 294 (2004), pp. 27–62. Séminaire Bourbaki, Vol. 2002/2003.

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

[16] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, Oxford, sixth ed., 2008. Revised by D. R. Heath-Brown and J. H. Silverman.

[17] 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), III, 150–181. See also *Oeuvres* III, 127–130, 146–149, and *Correspondance Hermite-Stieltjes*, II, lettre 363, 291–295. University of Michigan Historical Math Collection `http://name.umdl.umich.edu/AAS7821.0001.001`.

[18] ——, *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`.

[19] A. Y. Khinchin, *Continued fractions*, Dover Publications Inc., Mineola, NY, russian ed., 1997. With a preface by B. V. Gnedenko, Reprint of the 1964 translation.

[20] H. Lambert, *Mémoire sur quelques propriétés remarquables des quantités transcendantes circulaires et logarithmiques*. Mémoires de l'Académie des Sciences de Berlin, 17 (1761), 1768, p. 265–322; lu en 1767; Math. Werke, t. II., 1767.

[21] 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.

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

[23] H. W. Lenstra, Jr., *Solving the Pell equation*, Notices Amer. Math. Soc., 49 (2002), pp. 182–192.
`http://www.ams.org/notices/200202/fea-lenstra.pdf`.

[24] J. Liouville, *Addition à la note sur l'irrationalité du nombre e*, J. Math. Pures Appl., 1 (1840), pp. 193–194.
`http://portail.mathdoc.fr/JMPA/`.

[25] ——, *Sur l'irrationalité du nombre* $e = 2,718\ldots$, J. Math. Pures Appl., 1 (1840), p. 192.
`http://gallica.bnf.fr/Catalogue/noticesInd/FRBNF34348784.htm`.

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

[27] ——, *Algebraic independence*, Published for the Tata Institute of Fundamental Research, Bombay, 2009.

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

[29] O. Perron, *Die Lehre von den Kettenbrüchen. Dritte, verbesserte und erweiterte Aufl. Bd. II. Analytisch-funktionentheoretische Kettenbrüche*, B. G. Teubner Verlagsgesellschaft, Stuttgart, 1957.

[30] B. Rittaud, *Le fabuleux destin de* $\sqrt{2}$. Éditions Le Pommier, 2006.

[31] 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`.

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

[33] S. Shirali, *Continued fraction for e*. Resonance, vol. **5** N°1, Jan. 2000, 14–28.
`http://www.ias.ac.in/resonance/`.

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

[35] ——, *Transcendental numbers*, Princeton, N. J.: Princeton University Press, 1949.

[36] J. Sondow, *Criteria for irrationality of Euler's constant*, Proc. Amer. Math. Soc., 131 (2003), pp. 3335–3344 (electronic). Proc. Amer. Math. Soc. **131** (2003), 3335–3344
`http://xxx.lanl.gov/pdf/math.NT/0209070`
`http://home.earthlink.net/~jsondow/`.

[37] B. Sury, *Bessels contain continued fractions of progressions.* Resonance, vol. **10** N°3, March 2005, 80–87.
`http://www.ias.ac.in/resonance/`.

[38] M. Waldschmidt, *Nombres transcendants*, Springer-Verlag, Berlin, 1974. Lecture Notes in Mathematics, Vol. 402
`http://www.springerlink.com/content/110312/` .

[39] ——, *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/`

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