

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

*Michel Waldschmidt*

Part II: courses of 10/12/2009 and 14/12/2009

### 2.3 Linear forms

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

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

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

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

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

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

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

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

Assume  $1, \vartheta_1, \dots, \vartheta_m$  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  $(1, \vartheta_1, \dots, \vartheta_m)$ . Denote by  $A$  the sum of the absolute values of the coefficients of  $\Lambda_0$  and use the assumption with  $\epsilon = 1/m!A$ . Among the  $m + 1$  linearly independent linear forms which are given by the assumption of Lemma 13, select  $m$  of them, say  $\Lambda_1, \dots, \Lambda_m$ , which form with  $\Lambda_0$  a

set of  $m + 1$  linearly independent linear forms. The  $(m + 1) \times (m + 1)$  matrix of coefficients of these forms is regular; using the inverse matrix, one expresses its determinant  $\Delta$  as a linear combination with integer coefficients of  $\Lambda_k(1, \vartheta_1, \dots, \vartheta_m)$ ,  $1 \leq k \leq m$ . The choice of  $\epsilon$  yields the contradiction  $|\Delta| < 1$ .

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

**Proposition 14.** *Let  $\vartheta_1, \dots, \vartheta_m$  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*

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

*Proof.* For  $0 \leq k \leq m$ , 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  $\underline{L}$  be the regular  $(m + 1) \times (m + 1)$  matrix  $(\ell_{ki})_{0 \leq k, i \leq m}$ . Using the relation

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

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

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

Proposition 14 follows. □

An straightforward consequence of Proposition 14 is the following:

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

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

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

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

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

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

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

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

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

*Proof.* One can deduce Corollary 16 from Proposition 14 as follows: consider  $m - r$  linearly independent linear relations among  $1, \vartheta_1, \dots, \vartheta_m$ . Denote by  $\tilde{L}_{r+1}, \dots, \tilde{L}_m$  these linear forms and by  $c$  their maximal height. Take  $0 < \epsilon < 1/((m+1)!c^{m-r})$ . Select  $r+1$  linear forms  $\tilde{L}_0, \dots, \tilde{L}_r$  among  $L_0, \dots, L_m$  to get a maximal system of  $m+1$  linearly independent linear forms  $\tilde{L}_0, \dots, \tilde{L}_m$ . From Proposition 14 one deduces

$$\begin{aligned} \frac{1}{(m+1)!c^{m-r}H(\tilde{L}_0) \cdots H(\tilde{L}_r)} &\leq \frac{1}{(m+1)!H(\tilde{L}_0) \cdots H(\tilde{L}_m)} \\ &\leq \max_{0 \leq k \leq m} \frac{|\tilde{L}_k(1, \vartheta_1, \dots, \vartheta_m)|}{H(\tilde{L}_k)} \\ &\leq \max_{0 \leq k \leq r} \frac{|\tilde{L}_k(1, \vartheta_1, \dots, \vartheta_m)|}{H(\tilde{L}_k)} \\ &\leq \max_{0 \leq k \leq m} \frac{|L_k(1, \vartheta_1, \dots, \vartheta_m)|}{H(L_k)}. \end{aligned} \tag{17}$$

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

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

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

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

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

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

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

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

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

with

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

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

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

Since  $1, \xi_1, \dots, \xi_r$  are  $\mathbf{Q}$ -linearly independent, the  $r+1$  columns of the  $(m+1) \times (r+1)$  matrix  $(a_{hj})_{\substack{0 \leq h \leq m \\ 0 \leq j \leq r}}$  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

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

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

$$\max_{0 \leq k \leq m} |\Lambda_k(1, \xi_1, \dots, \xi_r)| \geq \frac{1}{(r+1)! \tilde{H}^r}$$

with

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

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

Corollary 16 follows. □

### 2.3.2 Nesterenko's Criterion for linear independence

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

The main reference for this section is [1].

**Theorem 18** (Nesterenko linear independence criterion). *Let  $c_1, c_2, \tau_1, \tau_2$  be positive real numbers and  $\sigma(n)$  a non-decreasing positive function such that*

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

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

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

*which satisfies the conditions*

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

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

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

**Theorem 19.** *Let  $\underline{\xi} = (\xi_i)_{i \geq 0}$  be a sequence of real numbers with  $\xi_0 = 1$ ,  $(r_n)_{n \geq 0}$  a non-decreasing sequence of positive integers,  $(Q_n)_{n \geq 0}$ ,  $(A_n)_{n \geq 0}$  and  $(B_n)_{n \geq 0}$  sequences of positive real numbers such that  $\lim_{n \rightarrow \infty} A_n^{1/r_n} = \infty$  and, for all sufficiently large integers  $n$ ,*

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

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

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

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

One deduces from Theorem 19 a slight refinement of Theorem 18 where the condition  $\limsup_{n \rightarrow \infty} \frac{\sigma(n+1)}{\sigma(n)} = 1$  is relaxed, the cost being to replace  $\sigma(n)$  by  $\sigma(n+1)$  in the upper bound for  $|L_n(1, \underline{\vartheta})|$ .

**Corollary 20.** *Let  $\tau_1, \tau_2$  be positive real numbers and  $\sigma(n)$  a non-decreasing positive function such that  $\lim_{n \rightarrow \infty} \sigma(n) = \infty$ . Let  $\underline{\vartheta} = (\vartheta_1, \dots, \vartheta_m) \in \mathbf{R}^m$ . Assume that, for all sufficiently large integers  $n$ , there exists a linear form with integer coefficients in  $m + 1$  variables*

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

which satisfies the conditions

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

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

Further consequences of Theorem 19 are given in [1]. See also Corollary 30 below;

### 3 Criteria for transcendence

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

#### 3.1 Liouville's inequality

Recall that the ring  $\mathbf{Z}[X]$  is factorial, its irreducible elements of positive degree are the non-constant polynomials with integer coefficients which are irreducible in  $\mathbf{Q}[X]$  (i.e. not a product of two non-constant polynomials

in  $\mathbf{Q}[X]$ ) and have content 1. The *content* of a polynomial in  $\mathbf{Z}[X]$  is the greatest common divisor of its coefficients.

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

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

**Lemma 21.** *Let  $\alpha$  be a real 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  $q \geq q_0$ ,*

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

*Proof.* Let  $q$  be a sufficiently large positive integer and let  $p$  be the nearest integer to  $q\alpha$ . In particular

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

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

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

and

$$q^d P(p/q) = a_0 q^d \prod_{i=1}^d \left( \frac{p}{q} - \alpha_i \right). \quad (22)$$

Also

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

The left hand side of (22) is a rational integer. It is not zero because  $P$  is irreducible of degree  $\geq 2$ . For  $i \geq 2$  we use the estimate

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

We deduce

$$1 \leq q^d a_0 \left| \alpha - \frac{p}{q} \right| \prod_{i=2}^d \left( |\alpha_i - \alpha| + \frac{1}{2q} \right).$$

For sufficiently large  $q$  the right hand side is bounded from above by

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

□

The same proof yields the next result.

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

**Proposition 23** (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, [4, 16]), but this is not relevant here.

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

**Corollary 24.** *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  $\lim_{n \rightarrow \infty} \sigma(n) = \infty$  and  $\lim_{n \rightarrow \infty} \lambda(n)/\sigma(n) = \infty$ . 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  $n$ ,*

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

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

### 3.2 Transcendence criterion of A. Durand

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



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

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

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

**Proposition 25.** *Let  $\vartheta$  be a complex number. The following conditions are equivalent*

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

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

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

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

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

## 4 Criteria for algebraic independence

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

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

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

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

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

**Theorem 26** (Gel'fond's transcendence Criterion). *Let  $\vartheta \in \mathbf{C}$  and let  $\gamma$  be a real number with  $\gamma > 1$ . Let  $(d_n)_{n=1}^{\infty}$  and  $(t_n)_{n=1}^{\infty}$  be two non-decreasing sequences of real numbers with  $\lim_{n \rightarrow \infty} t_n = \infty$ . Assume that there exists a sequence  $(P_n)_{n \geq 0}$  of polynomials in  $\mathbf{Z}[X]$  with  $P_n$  of degree  $\leq d_n$  and size  $t(P_n) \leq t_n$  such that, for all sufficiently large integer  $n$ ,*

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

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

A consequence is Lemma 3.5 of [11].

**Corollary 27.** *Let  $\vartheta \in \mathbf{C}$  and let  $\sigma(n)$  be a non-decreasing unbounded positive real function. Assume that there exists a sequence  $(P_n)_{n \geq 0}$  of polynomials in  $\mathbf{Z}[X]$  with  $P_n$  of size  $t(P_n) \leq \sigma(n)$  such that, for all sufficiently large integer  $n$ ,*

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

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

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

**Corollary 28.** *Let  $\vartheta_1, \dots, \vartheta_m$  be complex numbers  $\mathbf{C}$ . Let  $\sigma(n)$  and  $\lambda(n)$  be two non-decreasing positive real function with  $\lim_{n \rightarrow \infty} \sigma(n) = \infty$  and  $\lim_{n \rightarrow \infty} \lambda(n)/\sigma(n+1)^2 = \infty$ . Assume that there exists a sequence  $(P_n)_{n \geq 0}$  of polynomials in  $\mathbf{Z}[X_1, \dots, X_m]$ , with  $P_n$  of degree  $\leq \sigma(n)$  and height  $H(P_n) \leq e^{\sigma(n)}$ , such that, for all sufficiently large  $n$ ,*

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

*Then one at least two of the numbers  $\vartheta_1, \dots, \vartheta_m$  are algebraically independent.*

One should stress the following differences with Corollary 24: the conclusion of Theorem 26 is that the transcendence degree of the field  $\mathbf{Q}(\vartheta_1, \dots, \vartheta_m)$  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  $\lim_{n \rightarrow \infty} \lambda(n)/\sigma(n+1)^2 = \infty$  is stronger than the assumption  $\lim_{n \rightarrow \infty} \lambda(n)/\sigma(n) = \infty$  in Corollary 24 (what is important is the square, not the  $n+1$  in place of  $n$ ). On the other hand, Liouville's assumption is assumed to be satisfied for infinitely many  $n$ , while Gel'fond requires it for all sufficiently large  $n$ .

## 4.2 Large transcendence degree

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

One might hope that assuming  $\lim_{n \rightarrow \infty} \lambda(n)/\sigma(n+1)^k = \infty$  in Corollary 28 would suffice to prove that the transcendence degree of the field

$\mathbf{Q}(\vartheta_1, \dots, \vartheta_m)$  is at least  $k$ . However this is not the case, as an example from Khinchine (reproduced in Cassels book on Diophantine approximation) shows. The first one to obtain a criterion for large transcendence degree was G.V. Chudnovskii in 1976. The original criterion was not sharp, the estimate for the transcendence degree was the logarithm of the expected one. A few years later Philippon reached the optimal exponent.

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

**Theorem 29.** *Let  $\vartheta_1, \dots, \vartheta_m$  be complex numbers,  $\sigma(n)$  and  $S(n)$  be two non-decreasing positive real functions and  $k$  be a real number in the range  $1 \leq k \leq m$ . Assume that the functions*

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

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

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

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

The special case  $k = 1$  of this result is close (but weaker) than Corollary 24, the special case  $k = 2$  of this result is close (but weaker) than Theorem 26 (where no lower bound was requested).

It is interesting to compare with the following criterion for algebraic independence (Corollary 3.6 of [1]), which is a corollary of Theorem 19.

**Corollary 30.** *Let  $\vartheta_1, \dots, \vartheta_t$  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  $\mathbf{Z}[X_1, \dots, X_t]$ , where  $P_n$  has degree  $\leq d$  and length  $\leq e^{\sigma(n)}$ , such that, for  $n \geq n_0(d)$ ,*

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

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

The proof of Corollary 30 is much easier than the proof of Theorem 29, since it relies on linear elimination instead of polynomial elimination. Unfortunately, Corollary 30 does not seem to suffice for the proof of Nesterenko's algebraic independence Theorem on  $q$ ,  $P(q)$ ,  $Q(q)$  and  $R(q)$  (Theorem 4.2 of [11]).

### 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 so find the intersection point (unique in general) of  $n$  hyperplanes in dimension  $n$  by means of a determinant.

Given two plane curves

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

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

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

It is useful to work with a ring  $A$  more general than  $A_0[Y]$ . Let  $A$  be a commutative ring with unit. Denote by  $S$  the ring  $A[X]$  of polynomials in

one variable with coefficients in  $A$ . For  $d$  a non-negative integer, let  $S_d$  be the  $A$ -module of elements in  $S$  of degree  $\leq d$ . Then  $S_d$  is a free  $A$ -module of rank  $d + 1$  with a basis  $1, X, \dots, X^d$ .

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

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

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:

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

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

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

$$U_0 + U_1X + \dots + U_pX^p, \quad \text{et} \quad V_0 + V_1X + \dots + V_qX^q,$$

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

The above determinant suffices to deduce:

**Proposition 31.** *The universal resultant is a polynomial in*

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

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

**Proposition 32.** *There exist two polynomials  $U$  and  $V$  in  $S$ , of degrees  $< q$  and  $< p$  respectively, such that the resultant  $R = \text{Res}(P, Q)$  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  $\text{Res}(P, Q) = 0$ . The converse is true. It uses the following easy property, whose is left as an exercise.

**Proposition 33.** *Let  $A_0$  be a ring,  $A = A_0[Y_1, \dots, Y_n]$  the ring of polynomials in  $n$  variables with coefficients in  $A_0$ , and  $P, Q$  elements in  $A_0[Y_0, \dots, Y_n]$ , homogeneous of degrees  $p$  and  $q$  respectively. Consider  $P$  and  $Q$  as elements in  $A[Y_0]$  and denote by  $R = \text{Res}_{Y_0}(P, Q) \in A$  their resultant with respect to  $Y_0$ . Then  $R$  is homogeneous of degree  $pq$  in  $Y_1, \dots, Y_n$ .*

From these properties we deduce:

**Proposition 34.** . - *If*

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

*then*

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

*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  $R = \text{Res}(P, Q)$  (indeed, if one specializes  $\alpha_i = \beta_j$ , then the resultant vanishes). Now

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

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

**Corollary 35.** *Let  $K$  be a field containing  $A$  in which  $P$  and  $Q$  completely split in factors of degree 1. Then the resultant  $\text{Res}(P, Q)$  is zero if and only if  $P$  and  $Q$  have a common zero in  $K$ .*

**Corollary 36.** *If the ring  $A$  is factorial, then  $\text{Res}(P, Q) = 0$  if and only if  $P$  and  $Q$  have a common irreducible factor.*

## References

- [1] A. CHANTANASIRI, *On the criteria for linear independence of Nesterenko, Fischler and Zudilin.* manuscript.
- [2] A. DURAND, *Un critère de transcendance*, in Séminaire Delange-Pisot-Poitou (15e année: 1973/74), Théorie des nombres, Fasc. 2, Exp. No. G11, Secrétariat Mathématique, Paris, 1975, p. 9.
- [3] ———, *Indépendance algébrique de nombres complexes et critère de transcendance*, *Compositio Math.*, 35 (1977), pp. 259–267.
- [4] N. I. FEL'DMAN AND Y. V. NESTERENKO, *Transcendental numbers*, in *Number Theory, IV*, vol. 44 of *Encyclopaedia Math. Sci.*, Springer, Berlin, 1998.
- [5] S. FISCHLER AND W. ZUDILIN, *A refinement of Nesterenko's linear independence criterion with applications to zeta values.* <http://www.mpim-bonn.mpg.de/preprints/send?bid=4020>.
- [6] C. HERMITE, *Sur la fonction exponentielle*, *C. R. Acad. Sci. Paris*, 77 (1873), pp. 18–24, 74–79, 226–233, 285–293. Œuvres de Charles Hermite, Paris: Gauthier-Villars, 1905-1917. University of Michigan Historical Math Collection <http://name.umd.umich.edu/AAS7821.0001.001>.
- [7] S. LANG, *Introduction to transcendental numbers*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1966. Collected papers. Vol. I (1952–1970), Springer-Verlag 2000, p. 396–506.
- [8] M. LAURENT, *Cours de DEA à l'Université de Marseille, IML (Institut de Mathématiques de Luminy)*. Unpublished manuscript notes, 2007.
- [9] Y. NESTERENKO AND P. PHILIPPON, eds., *Introduction to algebraic independence theory*, vol. 1752 of *Lecture Notes in Mathematics*, Springer-Verlag, Berlin, 2001.

- [10] Y. V. NESTERENKO, *Linear independence of numbers*, Vestnik Moskov. Univ. Ser. I Mat. Mekh., (1985), pp. 46–49, 108.
- [11] ———, *Algebraic Independence*, TIFR Mumbai - Narosa, 2009.
- [12] D. ROY, *Philippon's criterion for algebraic independence (lectures 3 and 4)*. Summer School in Analytic Number Theory and Diophantine Approximation University of Ottawa, Ontario Canada, June 30-July 11, 2008 [http://aix1.uottawa.ca/~droy/summer-school-2008/droy\\_lecture3-4.pdf](http://aix1.uottawa.ca/~droy/summer-school-2008/droy_lecture3-4.pdf).
- [13] W. M. SCHMIDT, *Diophantine approximation*, vol. **785**, Lecture Notes in Mathematics. Berlin-Heidelberg-New York: Springer-Verlag, 1980, new ed. 2001.
- [14] C. L. SIEGEL, *Über einige Anwendungen diophantischer Approximationen*, Abhandlungen Akad. Berlin, Nr. 1 (1929), p. 70 S.
- [15] M. WALDSCHMIDT, *Nombres transcendants*, Springer-Verlag, Berlin, 1974. Lecture Notes in Mathematics, Vol. 402.
- [16] ———, *Diophantine approximation on linear algebraic groups*, vol. 326 of Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Springer-Verlag, Berlin, 2000. Transcendence properties of the exponential function in several variables.
- [17] ———, *An introduction to irrationality and transcendence methods*. Course at the 2008 Arizona Winter School and Ottawa Fields Institute. <http://people.math.jussieu.fr/~miw/articles/pdf/Ottawa2008part1.pdf>  
<http://people.math.jussieu.fr/~miw/articles/pdf/Ottawa2008part2.pdf>, 2008.

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

<http://www.math.jussieu.fr/~miw/>

This text is available on the internet at the address

<http://www.math.jussieu.fr/~miw/enseignements.html>