Séminaire de théorie des nombres de Bordeaux

Michel Waldschmidt

Transcendance et indépendance algébrique dans les groupes linéaires

Séminaire de théorie des nombres de Bordeaux (1970-1971), exp. nº 18, p. 1-10

<http://www.numdam.org/item?id=STNB_1970-1971____A18_0>

TRANSCENDANCE ET INDEPENDANCE ALGEBRIQUE DANS LES GROUPES LINEAIRES

par

Michel WALDSCHMIDT

-:-:-:-

§ 0. - NOTATIONS

Soient K un corps, A un anneau contenant K. Un élément α de A est algébrique sur K s'il existe un polynôme non nul $P \in K[X]$ tel que $P(\alpha) = 0$; sinon, il est transcendant sur K.

De même, si $\alpha_1, \ldots, \alpha_n$ sont des éléments de A, on dira qu'ils sont algébriquement dépendants s'il existe un polynôme non nul $P \in K[X_1, \ldots, X_n]$ tel que $P(\alpha_1, \ldots, \alpha_n) = 0$. La dimension algébrique (ou le degré de transcendance [10] § 74) de A sur K est le nombre maximum d'éléments de A algébriquement indépendants sur K. Si A est une K algèbre de type fini, la dimension algébrique de A sur K est finie.

Soient $\mathbb{C}$ le corps des nombres complexes, $M_n(\mathbb{C})$ l'anneau des matrices carrées d'ordre n à coefficients dans $\mathbb{C}$, $GL_n(\mathbb{C})$ le groupe linéaire de $\mathbb{C}$, c'est-à-dire le groupe multiplicatif des éléments inversibles de $M_n(\mathbb{C})$.

Soit f la bijection canonique de $M_n(\mathbb{C})$ sur $\mathbb{C}^{n^2}$. On munit $M_n(\mathbb{C})$ de la topologie qui fait de f un homéomorphisme. Alors $GL_n(\mathbb{C})$ devient un groupe topologique, ouvert dans $M_n(\mathbb{C})$.

§ 1. - ETUDE DES SOUS-GROUPES A UN PARAMETRE DANS LE GROUPE LINEAIRE

DEFINITION 1. On appelle sous-groupe à un paramètre de $GL_n(\mathbb{C})$ tout homomorphisme différentiable de $\mathbb{C}$ dans $GL_n(\mathbb{C})$.

Soit φ un sous-groupe à un paramètre de $GL_n(\mathbb{C})$:

$$\varphi(t+s) = \varphi(t) \,.\, \varphi(s) \qquad \text{pour tout } s\,,\ t \in \mathbb{C}\,.$$

Soit $M = \varphi'(0)$ (un vecteur tangent à l'origine).

Alors, pour tout $t \in \mathbb{C}$, on a : $\varphi(t) = \exp Mt$.

En effet, pour tout $t \in \mathbb{C}$, on a :

$$\varphi'(t) = \lim_{h \to 0} \frac{1}{h}\,[\varphi(t+h) - \varphi(t)] = \lim_{h \to 0} \frac{1}{h}\,(\varphi(h) - \varphi(0))\varphi(t) = M\,\varphi(t)\,.$$

Comme $\varphi(0) = 1$, ceci entraîne $\varphi(t) = \exp Mt$.

DEFINITION 2. Soit φ un sous-groupe à un paramètre de $GL_n(\mathbb{C})$:

$$\varphi(t) = (\varphi_{i,j}(t)) \qquad \text{pour } t \in \mathbb{C}\,.$$

On appellera dimension algébrique de φ le degré de transcendance sur $\mathbb{C}$ de l'anneau

$$\mathbb{C}[\{\varphi_{i,j}\}]$$

obtenu en adjoignant à $\mathbb{C}$ les n^2 éléments $\varphi_{i,j}$ de $\mathbb{C}^{\mathbb{C}}$.

(C'est la dimension de la plus petite sous-variété de groupe de $GL_n(\mathbb{C})$ contenant $\varphi(\mathbb{C})$).

LEMME 1. Soit $\varphi : t \to (\varphi_{i,j}(t))$ un sous-groupe à un paramètre de $GL_n(\mathbb{C})$ de dimension algébrique d. Soit K un corps algébriquement clos tel que $M = \varphi'(0) \in M_n(K)$. Soit $\alpha_1, \dots, \alpha_\delta$ une base du $\mathbb{Z}$-module engendré par les valeurs propres de M.

1) Si M est diagonalisable, alors

$$K[\{\varphi_{i,j}\}] = K[e^{\alpha_1 t}, \dots, e^{\alpha_\delta t}].$$

Donc $d = \delta$.

2) Si M n'est pas diagonalisable, alors

$$K[\{\varphi_{i,j}\}] = K[t, e^{\alpha_1 t}, \dots, e^{\alpha_\delta t}].$$

Donc $d = \delta + 1$.

Démonstration.

a) Soit $P \in GL_n(K)$. On pose

$$\psi(t) = P . \varphi(t) = (\psi_{i,j}(t)).$$

On a alors

$$K[\{\varphi_{i,j}\}] = K[\{\psi_{i,j}\}].$$

Donc la dimension algébrique de φ est égale à la dimension algébrique du sous-groupe à un paramètre :

$$t \to P^{-1}(\exp Mt)\, P = \exp P^{-1} M P\, t.$$

Il suffit donc d'étudier les deux cas : M diagonale ou M réduite sous forme "normale" ([10] t. 2) (réduites de Jordan).

b) Si M est diagonale, soit $M = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$, alors $e^M = \begin{pmatrix} e^{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & e^{\lambda_n} \end{pmatrix}$ et

$$K[e^{\lambda_1 t}, \dots, e^{\lambda_n t}] = K[e^{\alpha_1 t}, \dots, e^{\alpha_\delta t}].$$

c) Si $M = \begin{pmatrix} M_1 & & 0 \\ & \ddots & \\ 0 & & M_r \end{pmatrix}$, où $M_i = \begin{pmatrix} \lambda_i & 1 & 0 \\ & \ddots & \ddots 1 \\ 0 & & \lambda_i \end{pmatrix}$, alors $e^M = \begin{pmatrix} e^{M_1} & & 0 \\ & \ddots & \\ 0 & & e^{M_r} \end{pmatrix}$,

où $e^{M_i} = e^{\lambda_i} \begin{pmatrix} 1 & t & \frac{t^2}{2!} & \dots \\ & 1 & t & \dots \\ 0 & & & 1 \end{pmatrix}$.

Si l'une au moins des matrices M_i est d'ordre supérieur à 1, alors

$$K[\{\varphi_{i,j}\}] = K[t, e^{\alpha_1 t}, \dots, e^{\alpha_\delta t}].$$

d) Il nous reste à montrer que les $\delta+1$ fonctions $t, e^{\alpha_1 t}, \dots, e^{\alpha_\delta t}$ sont algébriquement indépendantes. Ceci résulte du :

LEMME 2. [4] - <u>Soient</u> $P_o, \dots, P_{\ell-1}$ <u>des polynômes de</u> $\mathbb{C}[X]$, <u>linéairement indépendants sur</u> $\mathbb{C}$, <u>de degré inférieur à</u> ℓ. <u>Soient</u> $\omega_1, \dots, \omega_m$ <u>des nombres complexes non nuls distincts deux à deux. Alors le déterminant</u>

$$\Delta = |P_i(k)\ \omega_j^k|_{\binom{0\le i\le \ell-1}{1\le j\le m}},\ (0\le k\le m\ell-1)$$

<u>est non nul.</u>

Si K est le corps obtenu en adjoignant à $\mathbb{Q}$ les coefficients des polynômes P_i, $0\le i\le \ell-1$, alors Δ et ses cofacteurs appartiennent à $K(\omega_1, \dots, \omega_m)$.

Le calcul effectif de ces cofacteurs, quand $P_i(x) = (a_o x)^i$, $a_o \neq 0$, est donné dans [4] I, lemme 7.

LEMME 3. <u>Soit</u> $\varphi : t \to (\varphi_{i,j}(t))$ <u>un sous-groupe à un paramètre de</u> $GL_n(\mathbb{C})$, $\lambda_1, \dots, \lambda_n$ <u>les valeurs propres de</u> $\varphi'(0)$, $\alpha_1, \dots, \alpha_\delta$ <u>une base du sous-Z-module de</u> $\mathbb{C}$ <u>engendré par</u> $\lambda_1, \dots, \lambda_n$. <u>Soit</u> $\gamma \in \mathbb{C}$ <u>tel que</u>

$$\lambda_i \neq \lambda_j \Rightarrow e^{\gamma\lambda_i} \neq e^{\gamma\lambda_j}.$$

<u>Soit</u> K <u>un corps algébriquement clos tel que</u> $\varphi(\gamma) \in GL_n(K)$. <u>Alors</u> $K[\{\varphi_{i,j}\}] \subset K[\frac{t}{\gamma}, e^{\alpha_1 t}, \dots, e^{\alpha_\delta t}]$. <u>De plus, si</u> $d = \delta$, <u>alors</u> $K[\{\varphi_{i,j}\}] = K[e^{\alpha_1 t}, \dots, e^{\alpha_\delta t}]$

<u>Démonstration</u>. Soit $P \in GL_n(K)$ tel que $P^{-1}\varphi(\gamma)P$ soit diagonale si $d = \delta$, de Jordan si $d = \delta+1$. On pose : $M_1 = P^{-1}\varphi'(0)\,P$

$$(\psi_{i,j}(t)) = P^{-1}.\ \varphi(t).\ P = \exp M_1 t .$$

Alors $K[\{\psi_{i,j}\}] = K[\{\varphi_{i,j}\}]$.

La matrice M_1 se décompose sous la forme $M_1 = S+N$, où $S \in M_n(\mathbb{C})$ est diagonalisable, et $N \in M_n(\mathbb{C})$ nilpotente. Soit $B \in GL_n(\mathbb{C})$ tel que $B^{-1}SB$ soit diagonale :

$$\exp B^{-1}SBt = \begin{pmatrix} e^{\lambda_1 t} & & 0 \\ & \ddots & \\ 0 & & e^{\lambda_n t} \end{pmatrix}.$$

D'où

$$(\psi_{i,j}(t)) = B(\exp B^{-1}SBt)\, B^{-1} \exp Nt \ .$$

Comme les coefficients de la matrice $\exp Nt$ sont des polynômes en t, on en déduit :

$$(\psi_{i,j}(t) = \sum_{k=1}^{n} P_{i,j,k}(t)\, e^{\lambda_k t} \ , \quad \text{où} \quad P_{i,j,k} \in \mathbb{C}[X].$$

Pour $t \in \mathbb{Z}$, on remarque que la diagonale de $\exp M_1 \gamma t$ est : $(e^{\lambda_1 \gamma t}, \ldots, e^{\lambda_n \gamma t})$.

D'où

$$\psi_{i,i}(\gamma t) = e^{\lambda_i \gamma t} \qquad \text{pour } t \in \mathbb{Z} \ , \quad 1 \leq i \leq n \ .$$

On obtient ainsi une relation de la forme

$$\sum_{k=1}^{n} \sum_{h=1}^{n} b_{k,h}\, t^{k-1}\, e^{\lambda_h \gamma t} = 0 \qquad \text{pour tout } t \in \mathbb{Z} \ .$$

Comme $\lambda_i \neq \lambda_j \Rightarrow e^{\gamma\lambda_i} \neq e^{\gamma\lambda_j}$, le lemme 2 montre que l'on a

$$\sum_{k=1}^{n} \sum_{h=1}^{n} b_{k,h}\, t^{k-1}\, e^{\lambda_h \gamma t} = 0 \qquad \text{pour tout } t \in \mathbb{C} \ .$$

D'où

$$\psi_{i,i}(t) = e^{\lambda_i t} \qquad \text{pour } t \in \mathbb{C} \ , \ 1 \leq i \leq n \ .$$

Ainsi

$$K[\{\psi_{i,j}\}] \supset K[e^{\alpha_1 t}, \ldots, e^{\alpha_\delta t}] \ .$$

Si M_1 est diagonalisable, c'est-à-dire $d = \delta$, on a $\psi_{i,j}(\gamma x) = 0$ pour tout x dans $\mathbb{Z}$, et $i \neq j$; donc $\psi_{i,j}(t) = 0$ pour tout $t \in \mathbb{C}$ et

$$K[\{\varphi_{i,j}\}] = K[e^{\alpha_1 t}, \ldots, e^{\alpha_\delta t}] \ .$$

Supposons $d = \delta + 1$.

Soit f l'une des fonction $\varphi_{i,j}$:

$$f(t) = \sum_{k=1}^{n} P_k(t)\, e^{\lambda_k t} \quad ; \quad t \in \mathbb{C} \ .$$

On a $f(\gamma x) \in K$ pour $x \in \mathbb{Z}$.

On obtient ainsi un système d'équations :

$$\sum_{i=1}^{n} \sum_{j=1}^{n} a_{i,j} \gamma^{i-1} t^{i-1} e^{\lambda_j \gamma t} \in K \quad , \quad t \in \mathbb{Z} .$$

On utilise le lemme 2 : les relations précédentes montrent que $a_{i,j} \gamma^{i-1} \in K$. Donc

$$f(t) = \sum_{k=1}^{n} Q_k(\tfrac{t}{\gamma}) \, e^{\lambda_k t} \qquad \text{pour } t \in \mathbb{C} \ , \ \text{avec} \ Q_k \in K[X].$$

Donc

$$f(t) \in K[\tfrac{t}{\gamma}, e^{\alpha_1 t}, \ldots, e^{\alpha_\delta t}]$$

on en déduit

$$K[\{\varphi_{i,j}\}] \subset K[\tfrac{t}{\gamma}, e^{\alpha_1 t}, \ldots, e^{\alpha_\delta t}] .$$

§ 2. - POINTS TRANSCENDANTS DANS LES GROUPES LINEAIRES

Nous allons rappeler les principaux théorèmes de transcendance concernant la fonction exponentielle complexe et énoncer leur équivalent dans les groupes linéaires.

a) Commençons par le théorème de Hermite-Lindemann [8]

Si α est un nombre algébrique non nul, alors e^{α} est transcendant. D'après le lemme 1, ce théorème est équivalent au suivant :

Soit φ un sous-groupe à un paramètre de $GL_n(\mathbb{C})$, tel que $\varphi'(0) \in M_n(\overline{\mathbb{Q}})$. S'il existe un nombre algébrique $\alpha \neq 0$ tel que $\varphi(\alpha) \in GL_n(\overline{\mathbb{Q}})$, alors les coefficients de la matrice $\varphi(t)$ sont des polynômes en t .

b) Transcendance de α^{β}

Le théorème de Gel'fond - Schneider sur la transcendance de α^{β} s'énonce [8]:

Si α et β sont des nombres algébriques, $\alpha \neq 0$, $\alpha \neq 1$ et $\beta \notin \mathbb{Q}$, alors α^{β} est transcendant.

D'après le lemme 1, les théorèmes de Hermite - Lindemann et de Gel'fond - Schneider entraînent le

THEOREME 1. [5, 8, 9] - Soit φ un sous-groupe à un paramètre de $GL_n(\mathbb{C})$ de dimension algébrique supérieure à un, et tel que $\varphi'(0) \in M_n(\overline{\mathbb{Q}})$. Alors, pour tout $u \in \mathbb{C}$, $u \neq 0$, $\varphi(u) \notin GL_n(\overline{\mathbb{Q}})$.

D'autre part, le théorème 1 entraîne le théorème de Gel'fond-Schneider (dans le cas où $\varphi'(0)$ est diagonalisable) et le théorème de Hermite-Lindemann (dans le cas où $\varphi'(0)$ n'est pas diagonalisable).

c) Transcendance de $e^{x_i y_j}$

S. Lang a démontré [6, 7, 8], que si x_1, x_2 (resp. y_1, y_2, y_3) sont des nombres complexes $\mathbb{Q}$-linéairement indépendants, l'un au moins des six nombres

$$e^{x_i y_j} \quad , \quad i = 1,2 \ ; \ j = 1,2,3$$

est transcendant.

Pour énoncer ce résultat dans les groupes linéaires, on ne suppose plus le sous-groupe normalisé pour avoir une dérivée algébrique à l'origine.

THEOREME 2. [6, 7, 8] - Soit φ un sous-groupe à un paramètre de $GL_n(\mathbb{C})$, de dimension algébrique supérieure à un. Soit Γ un sous-groupe de $\mathbb{C}$ tel que $\varphi(\Gamma) \subset GL_n(\overline{\mathbb{Q}})$. Alors le rang de Γ sur $\mathbb{Z}$ est inférieur à 3.

Pour terminer ce paragraphe, précisons que les théorèmes précédents s'étendent aux variétés abéliennes (ce qui n'est pas encore le cas pour les théorèmes qui suivent). D'autre part on peut généraliser le théorème 1 aux sous-groupes à d paramètres de $GL_n(\mathbb{C})$ [2].

§ 3. - INDEPENDANCE ALGEBRIQUE

a) Le théorème de Lindemann-Weierstrass s'énonce [8] :

Si $\alpha_1, \ldots, \alpha_n$ sont des nombres algébriques $\mathbb{Q}$-linéairement indépendants, alors les nombres $e^{\alpha_1}, \ldots, e^{\alpha_n}$ sont algébriquement indépendants.

Dans le groupe linéaire, ce théorème s'écrit de la manière suivante :

THEOREME 3. Soit φ un sous-groupe à un paramètre de $GL_n(\mathbb{C})$ de dimension algébrique d, tel que $\varphi'(0) \in M_n(\bar{\mathbb{Q}})$. Soient K un corps algébriquement clos et α un nombre algébrique non nul tels que $\varphi(\alpha) \in GL_n(K)$. Alors le degré de transcendance de K sur $\mathbb{Q}$ est supérieur ou égal à $d-1$.

b) Une conjecture très générale, due à Schanuel [1, 2], et qui contient tous les résultats et toutes les conjectures actuelles concernant la transcendance et l'indépendance algébrique des valeurs de la fonction exponentielle, est la suivante :

Si $\alpha_1, \dots, \alpha_n$ sont des nombres complexes $\mathbb{Q}$-linéairement indépendants, le degré de transcendance sur $\mathbb{Q}$ du corps $\mathbb{Q}(\alpha_1, \dots, \alpha_n, e^{\alpha_1}, \dots, e^{\alpha_n})$ est supérieur ou égal à n.

Dans les groupes linéaires, ceci revient à remplacer, dans le théorème 3, la condition $\varphi'(0) \in M_n(\bar{\mathbb{Q}})$ par $\varphi'(0) \in M_n(K)$.

c) Indépendance algébrique des nombres $e^{x_i y_j}$

Rappelons le théorème dans le cas complexe :[11]
Soient $x_1, \dots, x_n$ (resp. $y_1, \dots, y_m$) des nombres complexes $\mathbb{Q}$-linéairement indépendants.

Si $mn \geq 2(m+n)$, alors deux des nombres

$$e^{x_i y_j}, \quad 1 \leq i \leq n \; ; \; 1 \leq j \leq m$$

sont algébriquement indépendants.

Si $mn \geq m+2n$, alors deux des nombres

$$y_j, e^{x_i y_j}, \quad 1 \leq i \leq n \; ; \; 1 \leq j \leq m$$

sont algébriquement indépendants.

Si $mn > m+n$, alors deux des nombres

$$x_i, y_j, e^{x_i y_j}, \quad 1 \leq i \leq n \; ; \; 1 \leq j \leq m$$

sont algébriquement indépendants.

D'après le lemme 3 , on obtient le résultat suivant :

THEOREME 4. Soit K un sous-corps de $\mathbb{C}$, algébriquement clos, de degré de transcendance sur $\mathbb{Q}$ inférieur ou égal à 1 . Soit $\varphi : \mathbb{C} \to GL_n(\mathbb{C})$ un sous-groupe à un paramètre de dimension algébrique $d \geq 1$. Soit Γ un sous-groupe de $\mathbb{C}$ contenant au moins m éléments $\mathbb{Q}$-linéairement indépendants, et tel que $\varphi(\Gamma) \subset GL_n(K)$. Alors $md < 2(m+d)$. De plus, si $\Gamma \subset K$, alors $md < 2(m+d-1)$; si $\varphi'(0) \in M_n(K)$, alors $md < 2m+d$.

Remarque. Les théorèmes 1, 2, 3 précédents s'étendent au cas p-adique. Dans ce cas les théorèmes sont locaux dans un disque autour de l'origine ([6] p. 369 remarque 1, et [8] appendice théorème 2) . Pour le théorème 4, l'analogue p-adique est le suivant :

THEOREME 5. Soit Ω un corps algébriquement clos, complet pour une valuation ultramétrique, de caractéristique nulle, de caractéristique résiduelle p . Soit K un sous-corps de Ω , algébriquement clos, de degré de transcendance sur $\mathbb{Q}$ inférieur ou égal à 1 . Soit G un groupe linéaire sur Ω , et $\varphi : D \to G_\Omega$ un sous-groupe à un paramètre défini dans un disque D autour de l'origine dans Ω , de dimension algébrique d . Soit Γ un sous-groupe de D ayant au moins m éléments $\mathbb{Q}$-linéairement indépendants et tel que $\varphi(\Gamma) \subset G_K$. Alors

$$md \leq 2(m+d) .$$

De plus, si $\Gamma \leq K$, alors $md \leq 2(m+d-1)$;

si $\varphi'(0) \in G_K$, alors $md \leq 2(m+d)$;

si $\Gamma \subset K$ et $\varphi'(0) \in G_K$, alors $md < 2m+d$.

Enfin, en considérant des extensions de $\mathbb{Q}$ de type fini ayant un type de transcendance convenable ([8] , ch. V, § 3), on peut obtenir des résultats d'indépendance algébrique concernant des sous-groupes à d paramètres ([2] p. 13).

-:-:-:-

BIBLIOGRAPHIE

[1] AMICE Y. - Conjecture de Schanuel sur la transcendance d'exponentielles. Sém. Bourbaki, (1970-71), n° 382.

[2] BOMBIERI E. et LANG S. - Analytic subgroups of group varieties. Inventiones Math. 11 (1970) p. 1-14.

[3] CHEVALLEY C. - Theory of Lie groups. Princeton University Press, (1946).

[4] FEL'DMAN N. I. - Estimate for a linear form of logarithms of algebraic numbers ; I, Mat. U S S R. Sbornik, vol. 5 (1968) p. 291-307 ; II, id. vol. 6 (1968), p. 393-406.

[5] LANG S. - Transcendental points on group varieties. Topology, 1 (1962) p. 313-318.

[6] LANG S. - Algebraic values of meromorphic functions, I, topology, 3 (1965) p. 313-318 ; II, id. 5 (1966) p. 363-370.

[7] LANG S. - Nombres transcendants. Sém. Bourbaki, (1965-66) n° 305.

[8] LANG S. - Introduction to transcendental numbers. Addison Wesley, (1966).

[9] RAUZY G. - Points transcendants sur les variétés de groupes. Sém. Bourbaki (1963-64) n° 276.

[10] VAN DER WAERDEN B. L. - Modern Algebra, t. 1 Springer-Verlag (1966) 7e éd.

[11] WALDSCHMIDT M. - Indépendance algébrique des valeurs de la fonction exponentielle. Sém. Théorie des Nombres, Bordeaux, (1970-71), exposé n° 2, 18 p.

-:-:-:-

Michel WALDSCHMIDT
U. E. R. de Mathématiques
et d'Informatique
Université de Bordeaux 1
351, cours de la Libération
33 - TALENCE