

SÉMINAIRE N. BOURBAKI

GÉRARD RAUZY

Points transcendants sur les variétés de groupe

Séminaire N. Bourbaki, 1964, exp. n° 276, p. 453-460

http://www.numdam.org/item?id=SB_1962-1964__8__453_0

© Association des collaborateurs de Nicolas Bourbaki, 1964, tous droits réservés.

L'accès aux archives du séminaire Bourbaki (<http://www.bourbaki.ens.fr/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

POINTS TRANSCENDANTS SUR LES VARIÉTÉS DE GROUPE

par Gérard RAUZY

(d'après Serge LANG [1])

Il est bien connu que si α est algébrique, et $\neq 0$, e^α est transcendant (voir SCHNEIDER [3], chap. 2, p. 43). Nous nous proposons de donner la démonstration par S. LANG d'une conjecture de CARTIER généralisant ce résultat :

THÉORÈME 1. - Soit G une variété de groupe définie sur le corps des nombres algébriques \underline{K} . Soit \mathfrak{g} son algèbre de Lie à l'origine. Soit $\alpha \in \mathfrak{g}$, $\alpha \neq 0$ rationnel sur \underline{K} , et soit \exp_G la fonction exponentielle de G . Si $\exp_G(t\alpha)$ n'est pas une fonction algébrique de t , alors $\exp_G(\alpha)$ est transcendant sur \underline{K} .

1. Forme équivalente du théorème.

Nous allons ramener la démonstration du théorème à celle d'un théorème sur les variétés abéliennes. Pour cela, considérons tout d'abord le cas où G est un groupe linéaire : un vecteur tangent à l'origine est alors une matrice M , et $\exp(M)$ est donnée par $\exp(M) = \sum M^v/v!$.

L'hypothèse signifie alors que M est à coefficients algébriques, et que toutes les valeurs propres de M ne sont pas nulles (sinon M serait nilpotente, et $\exp(tM)$ serait un polynôme). Les valeurs propres sont elles-mêmes des nombres algébriques $\alpha_1, \dots, \alpha_s$, et on peut trouver une matrice B , inversible, rationnelle sur \underline{K} telle que

$$B^{-1} M B = \begin{pmatrix} M_1 & & 0 \\ & \ddots & \\ 0 & & M_s \end{pmatrix}$$

où $M_\sigma = \begin{pmatrix} \alpha_\sigma & & N_\sigma \\ & \ddots & \\ 0 & & \alpha_\sigma \end{pmatrix}$ est triangulaire.

D'autre part, $\exp(M)$ est rationnelle sur $\underline{K} \iff B^{-1} \exp(M) B = \exp(B^{-1} M B)$ est rationnelle sur \underline{K} , il suffit donc de montrer que $\exp(B^{-1} M B)$ ne peut pas être rationnelle sur \underline{K} .

Mais

$$\exp(B^{-1} M B) = \begin{pmatrix} \exp M_1 & & 0 \\ & \ddots & \\ 0 & & \exp M_* \end{pmatrix} \text{ et } \exp M_\sigma = \begin{pmatrix} e^{\alpha_\sigma} & & N'_\sigma \\ & \ddots & \\ 0 & & e^{\alpha_\sigma} \end{pmatrix}$$

en prenant l'un des α_σ différent de 0, on est ramené au résultat classique sur la fonction exponentielle ordinaire.

Dans le cas général, G contient un sous-groupe linéaire maximal L tel que $G/L = A$ soit une variété abélienne. Soit $\pi : G \rightarrow A$ la projection canonique, π est algébrique. Soit π_* l'homomorphisme induit sur les algèbres de Lie : $\pi_*(\alpha)$ est rationnel sur \underline{K} .

Si $\pi_*(\alpha) = 0$, α est contenu dans l'algèbre de Lie de L , et on retombe dans le cas linéaire.

Si $\pi_*(\alpha) \neq 0$, il suffit de prouver que $\pi \circ \exp_G(\alpha)$ est transcendant (car si $\exp_G(\alpha)$ est rationnel sur \underline{K} , il en est de même de $\pi \circ \exp_G(\alpha)$). Mais

$$\pi \circ \exp_G(\alpha) = \exp_A(\pi_*(\alpha)) ,$$

on est donc ramené à prouver le théorème pour une variété abélienne A .

Dans ce cas, il existe un homomorphisme holomorphe $\Theta : \underline{\mathbb{C}}^d \rightarrow A$ induisant un isomorphisme holomorphe de $\underline{\mathbb{C}}^d/\Lambda$ sur A (Λ lattice période). Si (z_1, \dots, z_d) sont les coordonnées dans $\underline{\mathbb{C}}^d$, les dérivées partielles $\partial/\partial z_i$ forment une base de l'algèbre de Lie des dérivations invariantes sur A . Après un changement convenable de coordonnées, on peut supposer que cette base est définie sur \underline{K} , c'est-à-dire que si f est une fonction méromorphe sur A définie sur K , alors $\partial f/\partial z_i$ est définie sur \underline{K} pour tout i . Un vecteur tangent est représenté par ses coordonnées $\alpha = (\alpha_1, \dots, \alpha_d)$, et est rationnel sur \underline{K} si tous les α_i sont des nombres algébriques. La fonction exponentielle est donnée par $\exp_A(t\alpha) = \Theta(t\alpha)$ (Remarquons alors que, dans ce cas, la fonction exponentielle est toujours une fonction transcendante).

On est donc ramené à prouver le théorème suivant :

THÉORÈME 2. - Soit A une variété abélienne de dimension d définie sur \underline{K} . Soit Θ l'homomorphisme donné par les fonctions thêta, induisant un isomorphisme du tore $\underline{\mathbb{C}}^d/\Lambda$ sur A . Supposons les dérivations $\frac{\partial}{\partial z_i}$ définies sur \underline{K} . Si $\alpha \in \underline{\mathbb{C}}^d$ est un vecteur complexe non nul, à coordonnées dans \underline{K} , alors $\Theta(\alpha)$ est transcendant sur K . En particulier, les périodes sont transcendentes.

2. Démonstration du théorème 2.

Supposons $\Theta(\alpha)$ rationnel sur \underline{K} , nous allons en déduire une contradiction en suivant une méthode analogue à celle de SCHNEIDER pour les courbes elliptiques, remplaçant les fonctions p et p' par les fonctions Θ . Tout d'abord on peut toujours supposer, sans restreindre la généralité, que α , $\Theta(\alpha)$ et la loi de groupe de A sont rationnels sur une extension finie K de \underline{Q} .

Mais alors $\Theta(t\alpha)$ est rationnel sur K pour t entier : choisissons une fois pour toutes m points de cette sorte (par exemple $\alpha, \dots, m\alpha$) avec $m > 4[K : \underline{Q}]$

Soient d'autre part $\Theta = (\theta_1, \dots, \theta_N)$ les coordonnées projectives de la représentation.

Quitte à faire un changement de coordonnées, on peut supposer que θ_1 ne s'annule en aucun des m points choisis. Soit alors $f_i = \theta_i/\theta_1$ ($i = 2, \dots, N$), les f_i sont holomorphes aux m points choisis, en outre les dérivées $\partial f_i/\partial z_j$ étant holomorphes quand les f_i le sont, elles appartiennent à l'anneau $K[f_1, \dots, f_N]$

Soient alors $\bar{f}_2, \dots, \bar{f}_N$ les fonctions d'une variable obtenues en prenant $\Theta(t\alpha)$: l'anneau $K[\bar{f}_1, \dots, \bar{f}_N]$ est stable pour la dérivation $D = d/dt$.

D'autre part, $\Theta(t\alpha)$ n'est pas une fonction algébrique de t , le degré de transcendance du corps $K(t, \bar{f}_2, \dots, \bar{f}_N)$ est donc ≥ 2 . Par ailleurs, les fonctions $\bar{f}_2, \dots, \bar{f}_N$ sont méromorphes dans tout le plan, et d'ordre inférieur ou égal à 2 (c'est-à-dire peuvent être représentées comme quotient de deux fonctions entières d'ordre ≤ 2 , en l'occurrence les fonctions θ).

Cela permet de conclure grâce au théorème suivant qui constitue l'essentiel de la démonstration.

THÉORÈME 3. - Soient g_1, \dots, g_N des fonctions méromorphes d'ordre fini $\leq \rho$. Soit K une extension algébrique finie de \underline{Q} . Supposons que la différentiation $D = d/dt$ laisse stable l'anneau $K[g_1, \dots, g_N]$ et que le corps des quotients soit de degré de transcendance ≥ 2 par rapport à K . Soit S un ensemble de points du plan complexe ne contenant pas les pôles des g_i et tel que

$$w \in S \Rightarrow g_i(w) \in K .$$

Alors S est fini, et le nombre d'éléments de S est $\leq 2\rho[K : \underline{Q}]$.

3. Démonstration du théorème 3.

Supposons que S contienne m points avec $m > 2\rho[K : \underline{Q}]$, nous allons en déduire une contradiction. Nous appelons T l'ensemble des points $(g_1(w), \dots, g_N(w))$

avec $w \in S$. Leurs coordonnées sont dans K . On va faire la démonstration en trois étapes, comme dans les démonstrations de SIEGEL, GEL'FAND, SCHNEIDER.

Notations. - Etant donné un polynôme $P(x_1, \dots, x_N)$, nous définissons l'opérateur \mathcal{O} tel que

$$\mathcal{O}P(x_1, \dots, x_N) = \sum_{i=1}^N \frac{\partial P}{\partial x_i} Q_i(x_1, \dots, x_N),$$

où les Q_i sont des polynômes à coefficients dans K tels que $\frac{dg_i}{dt} = Q_i(g_1, \dots, g_N)$, on a donc

$$(\mathcal{O}^\lambda P)(g_1, \dots, g_N) = \Gamma^\lambda(P(g_1, \dots, g_N)).$$

D'autre part, étant donné un nombre algébrique $\alpha \in K$, nous notons $|\alpha|$ le maximum des valeurs absolues des conjugués de α . De même, si $\underline{\alpha} = (\alpha_1, \dots, \alpha_N)$ est un système de nombres $\alpha_v \in K$, on notera $|\underline{\alpha}|$ le maximum des $|\alpha_v|$. Si P est un polynôme à coefficients dans K , $|\overline{P}|$ désignera le maximum des hauteurs de ses coefficients.

On appellera dénominateur pour un nombre $\alpha \in K$, pour un système de nombres $\alpha_v \in K$ ou pour un polynôme, un entier rationnel d tel que toutes les quantités $d\alpha$ intervenant soient des entiers algébriques.

Enfin on introduit, pour $P \in K[x_1, \dots, x_N]$, la notation $P < P^*$, où $P^* \in \mathbb{R}[x_1, \dots, x_N]$ si tous les coefficients de P^* (nombres réels ≥ 0) majorent la hauteur des coefficients correspondants de P . Pour un tel polynôme P^* , on notera $|\overline{P^*}|$ le maximum de ses coefficients. De même, si $\alpha \in K$, $\alpha^* \in \mathbb{R}$, on écrira : $\alpha < \alpha^*$ si $|\alpha| \leq \alpha^*$, et on posera $|\overline{\alpha^*}| = \alpha^*$. Définitions analogues pour un système de nombres de K . On vérifie alors que toutes les opérations effectuées sur des polynômes : addition, multiplication, dérivation partielle, substitution d'un système de valeurs aux variables, laissent stables les relations $<$.

LEMME. - Nous nous donnons un polynôme $P(x_1, \dots, x_N)$ à coefficients entiers algébriques de K , de degré au plus r par rapport à chaque variable, et un nombre λ entier ≥ 0 . Soit σ entier $> \max(r, \lambda)$, nous noterons C toutes les quantités ne dépendant pas de σ ni de $|\overline{P}|$.

On a alors :

$$\left\{ \begin{array}{l} \text{deg tot de } \mathcal{O}^\lambda P \leq C_\sigma \quad (\text{deg tot signifie le degré par rapport à l'ensemble des variables}) \\ |\overline{\mathcal{O}^\lambda P(\underline{\alpha})}| \leq |\overline{P}| (C_\sigma)^\sigma \quad \forall \underline{\alpha} = (\alpha_1, \dots, \alpha_N) \in \mathbb{T} \\ C^\sigma \text{ est un dénominateur pour tous les } \mathcal{O}^{(\lambda)} P(\alpha) \quad (C \text{ entier}) \end{array} \right.$$

En effet, $\exists C$ tel que $\forall i = 1, \dots, N$,

$$Q_i < C(1 + x_1 + \dots + x_N)^C$$

et d'autre part,

$$P < |\overline{P}| (1 + x_1 + \dots + x_N)^\sigma$$

donc

$$\begin{aligned} \mathbb{Q}P &< C(1 + x_1 + \dots + x_N)^C \sum_{i=1}^N |\overline{P}| \frac{\partial}{\partial x_i} (1 + x_1 + \dots + x_N)^\sigma \\ &< C^\sigma |\overline{P}| (1 + x_1 + \dots + x_N)^{C+\sigma} \end{aligned}$$

d'où par récurrence

$$\mathbb{Q}^\lambda P < (C^\sigma)^\lambda |\overline{P}| (1 + x_1 + \dots + x_N)^{\lambda C + \sigma} .$$

On en tire que

$$\text{deg tot } \mathbb{Q}^\lambda P < \lambda C + \sigma \leq C^\sigma .$$

En substituant $\underline{\alpha} < (C, \dots, C)$, pour $\underline{\alpha} \in T$, on obtient

$$|\mathbb{Q}^\lambda P(\underline{\alpha})| \leq (C^\sigma)^\lambda |\overline{P}|$$

Enfin, si C est un dénominateur pour les Q_i , C est dénominateur pour $\mathbb{Q}P$, donc par récurrence C^σ est dénominateur pour $\mathbb{Q}^\lambda P$. Si en même temps C est dénominateur pour les $\underline{\alpha} \in T$,

$$C^\sigma \times C^{\text{deg tot } \mathbb{Q}^\lambda P}$$

est dénominateur pour $\mathbb{Q}^\lambda P(\underline{\alpha})$, ce qui entraîne la dernière assertion.

Première étape. - Le degré de transcendance de $K[g_1, \dots, g_N]$ est ≥ 2 , il existe donc deux fonctions, soient g_1 et g_2 algébriquement indépendantes. Alors $\forall \sigma$ assez grand, il existe un polynôme $P(X_1, X_2)$ à coefficients entiers algébriques de K , non identiquement nul, tel que :

$$\left\{ \begin{array}{l} |\overline{P}| < (C^\sigma)^\sigma \\ \text{deg } P \text{ en } X_1 < [\sqrt{2m\sigma}] \text{ et } \text{deg } P \text{ en } X_2 < [\sqrt{2m\sigma}] \\ \mathbb{Q}^\lambda P(\underline{\alpha}) = 0, \quad \forall \lambda = 0, \dots, \sigma - 1 \text{ et } \forall \underline{\alpha} \in T \end{array} \right.$$

En effet, soit C^σ un dénominateur pour les $\mathbb{Q}^\lambda P(\underline{\alpha})$, posons

$$P(X_1, X_2) = \sum_{\substack{i=0, \dots, r \\ j=0, \dots, r}} a_{ij} X_1^i X_2^j$$

et considérons les $m\sigma$ équations $C^\sigma \mathbb{Q}^\lambda P(\underline{\alpha}) = 0$, $\underline{\alpha} \in T$, $\lambda = 0, \dots, \sigma - 1$

aux inconnues les a_{ij} , c'est-à-dire à $(r+1)^2$ inconnues.

Les $C^\sigma \omega^\lambda P(\underline{\alpha})$ sont des formes linéaires à coefficients entiers algébriques de K , par rapport aux a_{ij} . D'autre part, on a, $\forall P$, si $r \leq \sigma$:

$$|\overline{\omega^\lambda P(\underline{\alpha})}| \leq (C\sigma)^\sigma |\overline{P}|.$$

En prenant pour polynôme particulier le polynôme $X_1^i X_2^j$, on voit que la hauteur du coefficient de a_{ij} dans $\omega^\lambda P(\underline{\alpha})$ est bornée par $(C\sigma)^\sigma$, donc les $m\sigma$ équations $C^\sigma \omega^\lambda P(\underline{\alpha})$ sont à coefficients entiers dans K et de hauteur bornée par $(C\sigma)^\sigma$. D'après le lemme 31, page 142, de SCHNEIDER [3]

si nous supposons $(r+1)^2 > m\sigma$, il existe une solution à ce système d'équations en a_{ij} entiers de K non tous nuls, et avec

$$|\overline{P}| \leq (C(r+1)^2 (C\sigma)^{m\sigma}) / ((r+1)^{2-m\sigma})$$

en particulier en prenant $r = [\sqrt{2m\sigma}]$, on a bien $|\overline{P}| \leq (C\sigma)^\sigma$.

Deuxième étape. - Soit τ l'entier minimum tel que $\exists \underline{\alpha} \in T$, $\omega^\lambda P(\underline{\alpha}) \neq 0$ et soit $\gamma = \omega^\lambda P(\underline{\alpha})$ pour cet $\underline{\alpha}$ (P étant le polynôme construit dans la 1re étape, $\tau \geq \sigma$).

Alors on a $|\gamma| \geq (C\tau)^{-\tau(s-1)}$ où $s = [K : \mathbb{Q}]$.

En effet, toujours d'après le lemme, en faisant jouer à τ le rôle de σ , on a $C^\tau \gamma$ entier de K et

$$|C^\tau \omega^\tau P(\underline{\alpha})| \leq (C\tau)^\tau.$$

Si $\gamma_1 = \gamma, \gamma_2, \dots, \gamma_s$ sont les conjugués de γ , on a, puisque γ n'est pas nul et $C^\tau \gamma$ entier,

$$C^{\tau s} |\gamma| \prod_{t=2}^s |\gamma_t| \geq 1.$$

Mais $|\gamma_t| \leq |\overline{\gamma}| \leq (C\tau)^\tau$, d'où finalement

$$|\gamma| \geq (C\tau)^{-\tau(s-1)}.$$

Troisième étape. - On a $|\gamma| \leq C^\tau \tau^{1-(m/2(\rho+\epsilon))}$, $\forall \epsilon > 0$, dès que $\tau > C(\epsilon)$.

En effet, soit $F(z) = P(g_1(z), g_2(z))$, la fonction $F(z)$ est méromorphe dans tout le plan holomorphe aux points $w \in S$, et l'on a, $\forall w \in S$, $D^\lambda F(w) = 0$ pour $\lambda = 0, \dots, \tau-1$, mais $\exists w_0 \in S$, $D^\tau F(w_0) \neq 0$ et $\gamma = D^\tau F(w_0)$.

D'autre part, il existe une fonction $\theta(z)$ entière d'ordre $\leq \rho$, telle que $g_1 \theta$ et $g_2 \theta$ soient entières d'ordre $\leq \rho$, la fonction $E(z) = \theta^{2r} P(g_1, g_2)$ est donc entière.

Plus précisément, on peut écrire, si R assez grand, et si $|z| \leq R$,

$$|E(z)| \leq (C\sigma)^\sigma e^{\tau R^{\rho+\varepsilon}} \leq (C\tau)^\tau e^{\sqrt{\tau} R^{\rho+\varepsilon}} \quad \forall \varepsilon > 0$$

On a évidemment $D^\lambda E(w) = 0$, $\forall w \in S$, $\lambda = 0, \dots, \tau - 1$, et, au point $w_0 \in S$ tel que $\gamma = D^\tau F(w_0)$,

$$\gamma = (\theta(w_0))^{2r} D^\tau E(w_0) .$$

La fonction

$$H(z) = \frac{E(z)}{\prod_{w \in S} (z - w)^\tau}$$

est donc une fonction entière, et l'on a

$$D^\tau E(w_0) = \tau! H(w_0) \prod_{w \neq w_0, w \in S} (w - w_0)^\tau$$

d'où finalement en majorant $\tau!$ par τ^τ

$$|\gamma| \leq (C\tau)^\tau |H(w_0)| .$$

On va majorer $H(w_0)$ en utilisant le principe du maximum, pour R assez grand, on a en effet, si $|z| = R$,

$$|z - w| \geq CR \quad \forall w \in S$$

d'où

$$|H(z)| \leq (C\tau)^\tau e^{\sqrt{\tau} R^{\rho+\varepsilon}} R^{-m\tau} \quad \forall |z| \leq R .$$

Prenons $R = \left(\frac{m\sqrt{\tau}}{\rho}\right)^{1/(\rho+\varepsilon)}$ on est assuré que, lorsque $\sigma \rightarrow \infty$, donc $\tau, R \rightarrow \infty$, on a alors

$$|\gamma| \leq (C\tau)^\tau e^{\sqrt{\tau}(m\sqrt{\tau})/\rho} \left(\frac{m\sqrt{\tau}}{\rho}\right)^{-m\tau/(\rho+\varepsilon)} \leq C\tau^\tau \{1 - m/2(\rho+\varepsilon)\}^\tau$$

En comparant les deux majorations, on obtient une contradiction si

$$(C\tau)^{-\tau(s-1)} \geq C\tau^\tau \tau^{1-(m/2(\rho+\varepsilon))}$$

$$1 \geq C\tau^\tau \tau^{(s-(m/2(\rho+\varepsilon)))}$$

ce qui a certainement lieu pour un $\varepsilon > 0$, dès que $m > 2s\rho$.

4. Remarques.

On peut démontrer un résultat plus général que le théorème 3 (LANG [2]) en utilisant une intégrale de Cauchy à n variables. On a alors le théorème :

Soient K un corps de nombres, ξ_1, \dots, ξ_M des fonctions méromorphes d'ordre

$\leq p$ des n variables z_1, \dots, z_n telles que l'anneau $K[g_1, \dots, g_M]$ est stable par les dérivations partielles $\frac{\partial}{\partial z_i}$ ($i = 1, \dots, n$). Supposons le degré de transcendance du corps $K(g_1, \dots, g_M) \geq n + 1$, et soit un ensemble S de points de \mathbb{C}^n , qu'on peut mettre après changement convenable du système de coordonnées, sous la forme d'un produit $S_1 \times \dots \times S_n$ où chaque S_i contient m nombres complexes distincts.

Alors, si pour tout point de S , on a $g_1(w), \dots, g_M(w)$ dans K , on a nécessairement

$$m \leq bp [K : \mathbb{Q}] \quad (b \text{ ne dépendant que de } n)$$

Sous cette forme, on peut démontrer directement un résultat de SCHNEIDER sur les périodes des fonctions thêta (SCHNEIDER [4]).

BIBLIOGRAPHIE

- [1] LANG (Serge). - Transcendental points on group varieties, *Topology*, t. 1, 1962, p. 313-318.
- [2] LANG (Serge). - Algebraic values of meromorphic functions. Columbia University.
- [3] SCHNEIDER (Theodor). - Einführung in die transzendenten Zahlen. - Berlin, Springer-Verlag, 1957 (Die Grundlehren der mathematischen Wissenschaften, 81); Introduction aux nombres transcendants. Traduit de l'Allemand par Pierre Eymard. - Paris, Gauthier-Villars, 1959.
- [4] SCHNEIDER (Theodor). - Zur Theorie der Abelschen Funktionen und Integrale, *J. für die reine und angew. Math.*, t. 183, 1941, p. 110-128.