YVES HELLEGOUARCH

Indépendance linéaire et algébrique de logarithmes

Groupe d'étude en théorie analytique des nombres, tome 1 (1984-1985), exp. nº 20, p. 1-8
<http://www.numdam.org/item?id=TAN_1984-1985__1__A3_0>

Groupe d'étude en
THÉORIE ANALYTIQUE DES NOMBRES
1re-2e années, 1984-1985, n° 20, 8 p.

INDÉPENDANCE LINÉAIRE ET ALGÉBRIQUE DE LOGARITHMES

par Yves HELLEGOUARCH (*)

1. Motivations.

Soient r nombres premiers $p_1 , \dots , p_r$. Dans [4], j'ai introduit la notion de "comma" du sous-groupe multiplicatif G de $\mathbb{Q}^*$ engendré par $p_1 , \dots , p_r$ de la manière suivante.

Si $a \in G$, alors $a = p_1^{a_1} , \dots , p_r^{a_r}$ avec $(a_1 , \dots , a_r) \in \mathbb{Z}^r$. On pose

$$\|a\| = \sup_{i=1,\dots,r} \{|a_i|\} ,$$

et on dira que $a \in G \setminus \{1\}$ est un "comma" de G si, pour tout $b \in G \setminus \{1\}$, les conditions $\|b\| \leqslant \|a\|$ et $|\mathrm{Log}\, b| \leqslant |\mathrm{Log}\, a|$ entraînent $b \in \{a , a^{-1}\}$.

Il est tentant de vouloir prolonger cette définition au "module engendré" par des polynômes irréductibles $P_1(X) , \dots , P_r(X)$ tels que $P_i(0) = 1$. Ce "module" est en fait un sous-groupe multiplicatif G du corps $k((X))$ des séries formelles.

Nous allons définir G lorsque k est un corps de caractéristique zéro.

Pour commencer, on pose

$$\begin{aligned}\mathrm{Log}[P(X)] &= \mathrm{Log}[1 + P(X) - 1] \\ &= \sum(-1)^{n-1} \frac{[P(X) - 1]^n}{n} \\ &= -\sum\frac{[1 - P(X)]^n}{n} \in (X) ,\end{aligned}$$

(X) étant l'idéal engendré par X dans $k((X))$. $A_1(X) , \dots , A_r(X)$ étant des polynômes quelconques de $k[X]$, on peut définir $P_1^{A_1} , \dots , P_r^{A_r}$ par la formule

$$P_1^{A_1} , \dots , P_r^{A_r}(X) = \exp[\sum_{i=1}^r A_i(X) \mathrm{Log}\, P_i(X)] .$$

Il est clair que $P_1^{A_1} , \dots , P_r^{A_r}(0) = 1$. Par définition, G sera $\langle P_1,\dots,P_r\rangle$ c'est-à-dire l'ensemble des $A = P_1^{A_1} , \dots , P_r^{A_r}$ pour tous les $(A_1,\dots,A_r)\in(k[X])^r$.

Pour prolonger la définition rappelée ci-dessus, il est necessaire de définir $\|A\|$, et l'on est tenté de poser

$$\|A\| = \sup_{i=1,\dots,r}\{\deg A_i(X)\} .$$

(*) Yves HELLEGOUARCH, 4 rue du Docteur Rayer, 14000 CAEN

Mais pour que cette définition ait un sens, il est nécessaire que les séries $\operatorname{Log} P_1(X)$, ... , $\operatorname{Log} P_r(X)$ soient linéairement indépendantes sur $k(X)$.

Les résultats qui suivent donnent des conditions qui assurent l'indépendance linéaire de ces séries, et le fait le plus surprenant est qu'elles en assurent aussi l'indépendance algébrique.

Tout ceci était "bien connu" (voir [5] et [1]), mais l'approche qu'on propose ici est entièrement élémentaire.

Finalement, et pour conclure cette introduction, il serait peut-être normal de donner la définition d'un comma de G !

Dans ce but, on introduira une valeur absolue sur $k((X))$ en demandant qu'elle soit triviale sur k et que $|X| < 1$.

Et dans ces conditions, on dira que $A \in G$ est un "comma" de G si, et seulement si,

1° $A \in G \setminus \{1\}$,

2° pour tout $B \in G \setminus \{1\}$, tel que

$$\|B\| \leqslant \|A\| \quad \text{et} \quad |\operatorname{Log} B| \leqslant |\operatorname{Log} A| ,$$

on a $B = A^{\lambda}$, avec $\lambda \in k^*$.

Remarques.

1° On peut remplacer $|\operatorname{Log} B| \leqslant |\operatorname{Log} A|$ par $|B - 1| \leqslant |A - 1|$.

2° La même "philosophie" conduit à la définition de notions analogues dans les corps de nombres et de fonctions algébriques [2].

3° On trouvera un exposé plus complet dans [3].

2. Indépendance linéaire.

THÉORÈME. - *Si k est un corps de caractéristique zéro et si $P_1(X)$, ... , $P_r(X)$ sont des polynômes premiers entre eux deux à deux de $k[X]$ non constants et, tels que $P_i(0) = 1$ pour $i = 1$, ... , r ; alors les séries formelles 1 , $\operatorname{Log} P_1(X)$, ... , $\operatorname{Log} P_r(X)$ sont linéairement indépendantes sur $k(X)$.*

2.1. Nous commencerons par examiner un cas particulier.

LEMME. - *Soient r éléments distincts λ_1 , ... , λ_r de k^* . Alors les séries formelles 1 , $\operatorname{Log}(1 - \lambda_1 X)$, ... , $\operatorname{Log}(1 - \lambda_r X)$ sont linéairement indépendantes sur $k(X)$.*

Preuve.

1° La question revient à démontrer que si les polynômes $A_i(X) \in k[X]$, $i=0,\dots,r$ sont tels que

(I) $$\sum_{i=1}^{r} A_i(X) \operatorname{Log}(1 - \lambda_i X) = A_0(X) ,$$

alors tous les $A_i(X)$ sont nuls.

2° Nous allons poser $n = \sup_{i=0,\ldots,r}$ (degré $A_i(X)$), et nous allons dériver $n+1$ fois la relation précédente. Dans toute la suite, on désignera par N le noyau de la dérivation à l'ordre $n+1$, et on travaillera modulo N .

Nous poserons aussi $u_{i,k} = (X - \frac{1}{\lambda_i})^k \operatorname{Log}(1 - \lambda_i X)$, de sorte que la dérivée de $u_{i,0}$ sera égale à $\lambda_i/(\lambda_i X - 1)$; nous poserons $v_i = 1/(X - \frac{1}{\lambda_i})$, et nous allons montrer que la dérivée à l'ordre $n+1$ de la relation (I) est

(II) $$\sum_{j=1}^{n} \sum_{i=1}^{r} A^{(j)} (\tfrac{1}{\lambda_i}) v^{(n-j)} = 0 .$$

3° Pour faire ce calcul nous laisserons tomber l'indice i , et nous développerons le polynôme $A(X)$ par la formule de Taylor appliquée au point $1/\lambda$

(III) $$A(X) = A(\tfrac{1}{\lambda}) + (X - \tfrac{1}{\lambda}) A'(\tfrac{1}{\lambda}) + \ldots + \tfrac{1}{n!}(X - \tfrac{1}{\lambda}) A^{(n)}(\tfrac{1}{\lambda}) .$$

Nous nous proposons de dériver $A(X) \operatorname{Log}(1 - \lambda X)$ à l'ordre $n+1$.

Comme $u_k = (X - \frac{1}{\lambda})^k \operatorname{Log}(1 - \lambda X)$, on a

$$u'_k = k(X - \tfrac{1}{\lambda})^{k-1} \operatorname{Log}(1 - \lambda X) - \frac{1}{1 - \lambda X}(X - \tfrac{1}{\lambda})^k = k\, u_{k-1} + (X - \tfrac{1}{\lambda})^{k-1} .$$

Compte tenu du but que l'on s'est fixé, on écrira

$$u'_k \equiv k\, u_{k-1} \quad (\text{modulo } N) .$$

Comme $A(X) \operatorname{Log}(1 - \lambda X) = A(\frac{1}{\lambda}) u_0 + A'(\frac{1}{\lambda}) u_1 + \ldots + \frac{1}{n!} A^{(n)} (\frac{1}{\lambda}) u_n$, on a donc

$$\begin{aligned}[A(X) \operatorname{Log}(1 - \lambda X)]^{(n+1)} &= A(\tfrac{1}{\lambda}) u_0^{(n+1)} + A'(\tfrac{1}{\lambda}) u_0^{(n)} + \\ &\quad + A''(\tfrac{1}{\lambda}) u_0^{(n-1)} + \ldots + A^{(n)}(\tfrac{1}{\lambda}) u'_0 \\ &= A(\tfrac{1}{\lambda}) v^{(n)} + A'(\tfrac{1}{\lambda}) v^{(n-1)} + \ldots + A^{(n)}(\tfrac{1}{\lambda}) v .\end{aligned}$$

4° Si l'on interprête maintenant la relation (II) comme la décomposition de la fraction rationnelle 0 en éléments simples, le théorème d'unicité de cette décomposition montre que, pour $i = 1 , \ldots , r$ et $j \in \{1 , \ldots , n\}$, on a $A^{(j)} (\frac{1}{\lambda_i})=0$

Maintenant la formule de Taylor (III), appliquée avec i fixé, montre que $A_i(X) = 0$ pour $i = 1 , \ldots , r$.

2.2 Il ne reste plus qu'à examiner le cas général.

<u>Démonstration.</u>

1° On sait que k peut être plongé dans un corps K dans lequel les $P_i(X)$ sont scindés (par exemple $k = \mathbb{Q}$ peut être plongé dans $K = \mathbb{C}$).

2° Soient $1/(\lambda_{i,j})$, $j = 1 , \dots , s_i$, les racines de $P_i(X)$ dans K , on peut écrire que

$$P_i(X) = \prod_{j=1}^{s_i} (1 - \lambda_{i,j} X)^{n_i} , \quad n_i > 0 .$$

D'après la propriété fondamentale du logarithme, on a

$$\operatorname{Log} P_i(X) = \sum_{j=1}^{s_i} n_i \operatorname{Log}(1 - \lambda_{i,j} X) .$$

3° Maintenant il est clair que $\lambda_{i,j} \neq \lambda_{i',j'}$ lorsque $i \neq i'$.

En effet, si on avait $\lambda_{i,j} = \lambda_{i',j'}$ avec $i \neq i'$, les polynômes P_i et $P_{i'}$ auraient une racine commune, ce qui est contraire à l'hypothèse.

4° Ainsi les séries formelles $\operatorname{Log}(1 - \lambda_{i,j} X)$ sont linéairement indépendantes et si l'on a $\sum_{i=1}^{r} A_i(X) \operatorname{Log} P_i(X) = A_0(X)$, on en déduit que

$$\sum_{i=1}^{r} \sum_{j=1}^{s_i} n_i A_i(X) \operatorname{Log}(1 - \lambda_{i,j} X) = A_0(X) ,$$

donc tous les $A_i(X)$ sont nuls,

c. q. f. d.

3. Indépendance algébrique.

Dans le paragraphe précédent on a donné des conditions suffisantes sur les polynômes P_1 , P_2 , ... de $k[X]$, pour que les séries formelles 1 , $\operatorname{Log} P_1$, $\operatorname{Lof} P_2$, soient linéairement indépendantes sur le corps des fractions rationnelles $k(X)$.

En utilisant ce résultat, D. L. Mc QUILLAN a réussi à prouver que les séries formelles $\operatorname{Log} P_1$, $\operatorname{Log} P_2$, ... sont algébriquement indépendantes sur $k(X)$ (voir [3]).

C'est pour l'essentiel la démonstration de D. L. Mc QUILLAN, un peu particularisée, que je reproduis dans l'exposé ci-dessous.

3.1 Dans toute la suite, k désigne un corps de caractéristique zéro et $P_1, P_2, \cdots$ sont des polynômes non constants de $k[X]$, premiers entre eux deux à deux et tels que $P_i(0) = 1$.

Pour simplifier les notations, on désignera par f_i la série formelle $\operatorname{Log} P_i$, et on posera $K_0 = k(X)$.

Le résultat que l'on a en vue est le suivant.

THÉORÈME 1. - *Soit* $n \geq 1$, *et soit* $V(Y_1 , \dots , Y_n)$ *un polynôme de* $K_0[Y_1, \cdots, Y_n]$. *Alors* $V(f_1 , \dots , f_n) = 0$ *entraîne* $V = 0$. (*On dit alors que* $f_1 , \dots , f_n$ *sont algébriquement indépendantes sur* K_0).

La méthode de démonstration est contenue dans un deuxième résultat, dû à D. L. Mc QUILLAN.

THÉORÈME 2. - Soit une famille de séries formelles (f_i) telle que $f_i' \in K_0$ pour tout i.

Si $1, f_1, f_2, \dots$ sont linéairement indépendantes sur K_0, alors $f_1, f_2, \dots$ sont algébriquement indépendantes sur K_0.

Dans la démonstration du théorème 2, nous utiliserons les notations suivantes

$R_0 = K_0$

Pour $m \geq 1$, $R_m = K_0[f_1, \dots, f_m]$, $K_m = K_0(f_1, \dots, f_m)$.

Si D désigne la dérivation de $k((X))$, il est clair que, pour tout m, $D(R_m) \subset R_m$ et $D(K_m) \subset K_m$.

Pour $m \geq 0$, T_m désigne le k-sous-espace vectoriel de $k((X))$ engendré par les f_i pour $i \geq m+1$.

Il est clair que :

$$R_0 \subset R_1 \subset R_2 \subset \dots$$

$$K_0 \subset K_1 \subset K_2 \subset \dots$$

$$T_0 \supset T_1 \supset T_2 \supset \dots$$

On fera cette démonstration par récurrence sur n.

Deux lemmes souligneront les principales étapes de la démonstration.

3.2 Commençons par $n = 1$, nous devons démontrer que si 1 et f_1 sont linéairement indépendantes sur K_0, alors $1, f_1, \dots, f_1^h$ sont linéairement indépendants sur K_0, mais nous remplacerons cet énoncé par un énoncé un peu plus général.

LEMME 1. - Soit $L \in T_0$ et soit $m \geq 0$. Supposons que 1 et L soient linéairement indédpendantes sur K_m, alors $1, L, \dots, L^h$ sont linéairement indépendantes sur K_m.

Preuve. - On va faire un raisonnement par récurrence sur h.

Pour $h = 1$, c'est évident.

Soit $h > 1$, et supposons que

$$\sum_{i=0}^h A_i L^i = 0 \text{ , avec } A_i \in K_m \text{ , } A_h \neq 0 \text{ .}$$

En dérivant, on obtient

$$\sum_{i=0}^h A_i' L^i + L' \sum_{i=0}^h iA_i L^{i-1} = 0 \text{ .}$$

En éliminant L^h entre ces deux équations, on obtient

$$\sum_{i=0}^{h-1} B_i L^i = 0 \text{ , avec } B_i \in K_m \text{ .}$$

D'après l'hypothèse de récurrence, tous les B_i sont nuls.

En particulier, on obtient $B_{h-1} = 0$, soit

$$A'_{h-1}\,A_h - A_{h-1}\,A'_h + hA_h^2\,L' = 0 \; .$$

En divisant par A_h^2 , on obtient $((A_{h-1})/A_h) + hL' = 0$, d'où $(A_{h-1})/A_h + hL = c\ k$, d'où

$$\left(\frac{A_{h-1}}{A_h} - c\right) + hL = 0 \; ,$$

ce qui contredit l'indépendance linéaire de 1 et L sur K_m .

3.3 Passons maintenant à la récurrence proprement dite.

LEMME 2. - <u>Soit</u> $L \in T_m$ $L \neq 0$ <u>avec</u> $m \geq 0$. <u>Supposons</u> 1 , f_1 , f_2 , ... <u>linéairement indépendantes sur</u> K_0 . <u>Alors</u> 1 , L , ... , L^h <u>sont linéairement indépendantes sur</u> K_m .

<u>Preuve</u>. - On va faire un raisonnement par récurrence sur m . Pour $m = 0$, cela résulte du lemme 1 (avec $m = 0$).

Soit $m \geq 1$, et supposons que le résultat a été démontré par $m - 1$.

D'après le lemme 1, il suffit de démontrer que 1 et L sont linéairement indépendants sur K_m .

Soit donc $U_0 + U_1 L = 0$, avec $U_i \in K_m$.

Si f_m n'apparaît pas dans U_0 et U_1 , alors U_0 et $U_1 \in K_{m-1}$ et l'hypothèse de récurrence $(L \in T_m \subset T_{m-1})$ entraîne que $U_0 = U_1 = 0$.

Supposons donc que f_m apparaisse dans U_0 ou U_1 ; quitte à chasser les dénominateurs, on peut supposer que U_0 et U_1 sont dans R_m , et on écrit

$$(1) \qquad U_0 = \textstyle\sum_{i=0}^h A_i\, f_m^i \; , \quad U_1 = \sum_{i=0}^h B_i\, f_m^i$$

avec A_i , $B_i \in R_{m-1}$ et $(A_h , B_h) \neq (0 , 0)$.

En dérivant la relation $U_0 + U_1 L = 0$, on obtient $U'_0 + U_1 L' + U'_1 L = 0$, et en éliminant L

$$(2) \qquad U'_0\,U_1 - U_0\,U'_1 + L'\,U_1^2 = 0 \; .$$

En utilisant les expressions (1), et en les portant dans (2), on obtient

$$(3) \quad (\textstyle\sum_{i=0}^h B_i\, f_m^i)(\sum_{i=0}^h A'_i\, f_m^i) - (\sum_{i=0}^h A_i\, f_m^i)(\sum_{i=0}^h B'_i\, f_m^i)$$
$$+ f'_m\{(\textstyle\sum_{i=0}^h B_i\, f_m^i)(\sum_{i=0}^h iA_i\, f_m^{i-1}) - (\sum_{i=0}^h A_i\, f_m^i)(\sum_{i=0}^h iB_i\, f_m^{i-1})\}$$
$$+ L'(\textstyle\sum_{i=0}^h B_i\, f_m^i)^2 = 0$$

La relation (3) est une relation linéaire entre les puissances 1 , f_m , ... , f_m^{2h} à coefficients dans K_{m-1} puisque f'_m , L' , A_i , B_i , A'_i , $B'_i \in K_{m-1}$.

Mais comme $f_m \in T_{m-1}$, l'hypothèse de récurrence entraîne que tous les coefficients

$c_0 , c_1 , \dots , c_{2h}$ de cette relation sont nuls.

Nous allons en déduire que tous les B_i sont nuls. Commençons par les termes de plus haut degré. Nous avons $c_{2h} = B_h A'_h - B'_h A_h + L' B_h^2 = 0$.

Si B_h n'était pas nul, on aurait (en divisant par B_h^2) $(A_h/B_h)' + L' = 0$, d'où $A_h/B_h + L = c_0 \in k$

Comme $L \in T_m \subset T_{m-1}$ et que $A_h/B_h - c_0 \in K_{m-1}$, on a une contradiction avec l'hypothèse de récurrence.

Puisque $B_h = 0$ et que $(A_h , B_h) \neq (0 , 0)$, A_h n'est pas nul. Dans toute la suite, nous remplacerons B_h par zéro. Passons à c_{2h-1} , nous avons

$$c_{2h-1} = B_{h-1} A'_h - B'_{h-1} A_h = 0 .$$

En divisant par A_h^2 , $(B_{h-1}/A_h)' = 0$, d'où $B_{h-1}/A_h = c \in k$.

Passons à c_{2h-2} , nous avons

$$c_{2h-2} = (B_{h-2} A'_h - B'_{h-2} A_h) + (B_{h-1} A'_{h-1} - B'_{h-1} A_{h-1})$$
$$+ f'_m(hB_{h-1} A_h - (h - 1) B_{h-1} A_h) + L' B_{h-1}^2 = 0 .$$

En divisant par A_h^2 , et en utilisant $B_{h-1} = cA_h$, on obtient

$$- (\frac{B_{h-2}}{A_h})' + c(\frac{A_{h-1}}{A_h}) + cf'_m + c^2 L' = 0 ,$$

d'où

$$- \frac{B_{h-2}}{A_h} + c \frac{A_{h-1}}{A_h} + cf_m + c^2 L = c_1 \in k ,$$

mais $f_m + cL \in T_{m-1}$, et les autres termes sont dans K_{m-1} , donc l'hypothèse de récurrence entraîne $c = 0$, d'où $B_{h-1} = 0$.

Nous allons maintenant supposer que nous avons $B_h = B_{h-1} = \dots = B_{h-r+1} = 0$ avec $r \geqslant 2$, et nous allons montrer que $B_{h-r} = 0$. Nous allons utiliser les relations $c_{2h-r} = c_{2h-(r+1)} = 0$.

Comme $2h - r > 2h - (r + 1) > 2(h - r)$, le terme $L'(\sum_{i=0}^{h-r} B_i f_m^i)^2$ n'intervient pas dans le calcul.

On a donc $c_{2h-r} = B_{h-r} A'_h - B'_{h-r} A_h = 0$, d'où $B_{h-r} = c_2 A_h$, avec $c_2 \in k$.

On a aussi

$$c_{2h-r-1} = (B_{h-r-1} A'_h - B'_{h-r-1} A_h)$$
$$+ (B_{h-r} A'_{h-1} - B'_{h-r} A_{h-1})$$
$$+ f'_m(hB_{h-r} A_h - (h - r) B_{h-r} A_h) = 0 .$$

En dérivant par A_h^2 , et en posant $B_{h-r} = c_2 A_h$, on obtient

$$- \left(\frac{B_{h-r-1}}{A_h}\right)' + c_2\left(\frac{A_{h-1}}{A_h}\right)' + c_2\, rf'_m = 0$$

d'où

$$- \frac{B_{h-r-1}}{A_h} + c_2 \frac{A_{h-1}}{A_h} + c_2\, rf_m = c_3 \in k\ .$$

En raisonnant comme plus haut, on obtient $c_2\, r = 0$, d'où $c_2 = 0$ et $B_{h-r} = 0$. Finalement $U_1 = 0$, d'où $U_0 = 0$ et le lemme 2 est démontré.

RÉFÉRENCES

[1] AX (J.). - On Schanuel's conjectures and Skolem's method "1969 number theory institute", p. 206-212. - Providence, American mathematical Society, 1971 (Proceedings of Symposia in pure Mathematics, 20).

[2] HELLEGOUARCH (Y.), PAYSANT LE ROUX (R.). - Commas, points extrémaux et arêtes des corps possédant une formule du produit, C. R. math. Acad. Sc. Canada.

[3] Mc QUILLAN (D. L.). - Some results on algebraic independence, University College, Dublin.

[4] Musique et mathématique, par B. Parzysz, suivi de Gammes naturelles, par Y. Hellegouarch. - Paris, Association des Professeurs de Mathématiques de l'Enseignement public, 1984 (Publications de l'APMEP, 53).

[5] OSTROWSKI (A.). - Sur les relations algébriques entre les intégrales indéfinies, Acta Math., Uppsala, t. 78, 1946, p. 315-318.