Groupe d'étude en théorie analytique des nombres

Roger Paysant Le Roux

X-unités de certains corps de fonctions algébriques, I

Groupe d'étude en théorie analytique des nombres, tome 1 (1984-1985), exp. n° 18, p. 1-7

<http://www.numdam.org/item?id=TAN_1984-1985__1__A1_0>

Groupe d'étude en
THÉORIE ANALYTIQUE DES NOMBRES
1re-2e années, 1984-1985, n° 18, 7 p.

5novembre 1984

X-UNITÉS DE CERTAINS CORPS DE FONCTIONS ALGÉBRIQUES, I

par Roger PAYSANT LE ROUX (*)

1. Equation de Pell généralisée et unités.

Soit

$$D(X) = X^{3n} + a_{2n-1} X^{2n-1} + \ldots + a_0 \in K = \mathbb{Q}(X) .$$

On se propose de trouver les triplets (U_0 , U_1 , U_2) de polynômes à coefficients rationnels tels que :

$$U_0^3 + U_1^3 D + U_2^3 D^2 - 3 U_0 U_1 U_2 D = Cte \neq 0 . \tag{1}$$

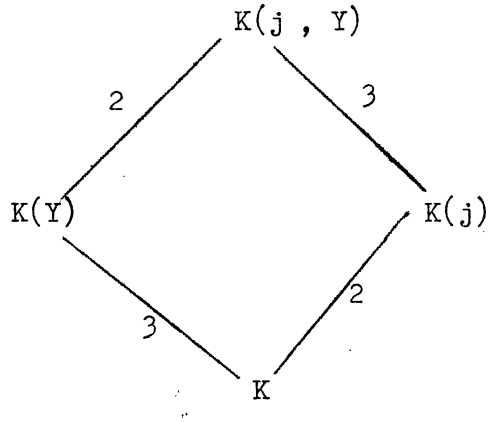
On fait l'hypothèse que D n'est pas un cube dans $A = \mathbb{Q}[X]$. Le problème posé revient à chercher les unités de l'anneau $B = A + AY + AY^2$ du corps des fonctions $E = K(Y)$, où Y vérifie l'équation $Y^3 = D$. En effet, si l'on pose

$$\varphi = U_0 + U_1 Y + U_2 Y^2 , \quad U_i \in A \quad (i = 0 , 1 , 2) ,$$

alors (1) s'écrit :

$$\pi_{E/K} \varphi(U) = Cte \neq 0 .$$

Si j désigne une racine 3e de l'unité différente de 1 , on a le diagramme :



On peut montrer que B est la fermeture intégrale de A dans E quand D n'a que des racines simples.

Si on désigne par $\mathcal{U}(B)$ l'ensemble des unités de l'anneau B , on a :

$$\varphi \in \mathcal{U}(B) \text{ si et seulement si } \pi \varphi \in \mathbb{Q}^* .$$

$\varphi_1 , \varphi_2 \in \mathcal{U}(B)$, nous dirons que $\varphi_1 \sim \varphi_2$ s'il existe

---

(*) Roger PAYSANT LE ROUX, 13 allée du Bec Hellouin, 14000 CAEN.

$$\lambda \in \mathbb{Q}^* \quad \text{tel que} \quad \varphi_1 = \lambda \varphi_2 .$$

On pose $\mathcal{S} = \mathcal{U}(B)/\mathbb{Q}^*$.

2. Rang du groupe des unités.

Soit Δ la solution "réelle" $X^n + \ldots$ dans le corps des séries formelles $\mathbb{Q}((\frac{1}{X}))$ de l'équation $Y^3 = D$.

On définit le degré d'une fonction $\varphi(U) = U_0 + U_1 \Delta + U_2 \Delta^2$ de la façon suivante: si on développe $\varphi(U)$ en série formelle en $1/X$, on obtient

$$\varphi = \sum_{m \geq m_0} \alpha_{-m} X^{-m} ,$$

$\alpha_m \in \mathbb{Q}$, où m_0 est tel que $\alpha_{m_0} \neq 0$, alors $-m_0$ est appelé le degré de φ et on le note $\deg \varphi$.

On définit de façon similaire le degré de

$$\sigma\, \varphi(U) = U_0 + j\, U_1 \Delta + j^2 U_2 \Delta^2$$

et le degré de

$$\sigma^2\, \varphi(U) = U_0 + U_1\, j^2 \Delta + U_2\, j\, \Delta .$$

THÉORÈME 1. - Le groupe $\mathcal{S}$ est soit trivial soit cyclique infini.

Preuve. - On considère l'homomorphisme :

$$L : \mathcal{S} \longrightarrow \mathbb{Z}^3$$

$$\varphi \longmapsto (\deg \varphi , \deg \sigma\, \varphi , \deg \sigma^2\, \varphi) .$$

On va montrer

1° L est injective

2° $\mathcal{S} \simeq \operatorname{Im} L \subset \{(X_0 , X_1 , X_2) \in \mathbb{Z}^3 ; \ X_0 + X_1 + X_2 = 0 \ \text{et} \ X_1 = X_2\}$.

Cela résultera du lemme suivant.

LEMME. - On suppose $U \neq 0$ et on pose

$$\deg U = \max(\deg U_0 , \deg U_1 \Delta , \deg U_2 \Delta^2) .$$

(a) $\forall\, U \in A^3$, on a $\deg \sigma\, \varphi(U) = \deg \sigma^2\, \varphi(U)$,

(b) $\forall\, U \in A^3$,

(i) si $\deg \varphi < \deg U$, alors $\deg \sigma^i\, \varphi = \deg U (i = 1 , 2)$

(ii) si $\deg \sigma\, \varphi < \deg U$, alors $\deg \varphi = \deg U$.

Preuve du lemme.

(a) $$\sigma\varphi = \sum_{m \geqslant m_0} \alpha_{-m} X^{-m} , \quad \alpha_{-m} \in \underset{\sim}{Q}(j) , \quad \alpha_{-m_0} \neq 0$$

alors on a

$$\sigma^2 \varphi = \sum_{m \geqslant m_0} \bar{\alpha}_{-m} X^{-m} , \text{ avec } \bar{\alpha}_{-m_0} \neq 0 .$$

(b) Montrons (b - i) , pour cela posons

$$U_\ell \Delta^\ell = \beta^\ell X^{\deg U} + \dots , \quad \beta^{(\ell)} \in \underset{\sim}{Q}$$

$$\sigma^i \varphi = \gamma^{(i)} X^{\deg U} + \dots$$

alors on a

(2) $$\begin{cases} \gamma^{(0)} = \beta^{(0)} + \beta^{(1)} + \beta^{(2)} \\ \gamma^{(1)} = \beta^{(0)} + j\,\beta^{(1)} + j^2\,\beta^{(2)} \\ \gamma^{(2)} = \beta^{(0)} + j^2\,\beta^{(1)} + j\,\beta^{(2)} \end{cases}$$

si on suppose $\deg \varphi < \deg U$, on a $\gamma^{(0)} = 0$ et si on suppose de plus $\deg \sigma\varphi = \deg \sigma^2 \varphi < \deg U$, alors on a $\gamma^{(0)} = \gamma^{(1)} = \gamma^{(2)} = 0$ et d'après le système (2) $\beta^{(0)} = \beta^{(1)} = \beta^{(2)} = 0$ mais ceci contredit le fait que $U \neq 0$.

Remarque. - Si on prolonge l'homomorphisme L à $B^*/\underset{\sim}{Q}^*$, le lemme nous dit que L reste injective, ce qui est faux pour $E^*/\underset{\sim}{Q}^*$.

3. Définition de meilleures approximations.

On pose

$$\varphi_i(U) = \deg \sigma^i \varphi(U) \quad (i = 0 , 1 , 2)$$

$$N(U) = \deg \mathfrak{N} \varphi(U) .$$

Définition. - Soit $U \in A^3$, $U \neq 0$, on dit que $\varphi(U) = U_0 + U_1 \Delta + U_2 \Delta^2$ (ou U) est une meilleure approximation (ou en abrégé m. a.) de 1 , Δ , Δ^2 si U vérifie la propriété

$$\forall\, U' \in A^3 , \quad U' \neq 0 , \quad \varphi_i(U') \leqslant \varphi_i(U) \quad (i = 0 , 1 , 2) \Longrightarrow U' \sim U$$

$$(U' \sim U \text{ si } \varphi(U') \sim \varphi(U)) .$$

Propriétés des m. a.

1° Si $\varphi(U) \in \mathcal{U}(B)$, alors $\varphi(U)$ est une m. a.,

2° si on identifie un élément de A^3 à un point de $\underset{\sim}{Z}^3$ par l'homomorphisme injectif L , il n'y a qu'un nombre fini de m. a. dans une région bornée de $\underset{\sim}{Z}^3$,

3° l'ensemble des m. a. U telles que $\varphi_0(U) \leqslant 0$ (resp. $\varphi_1(U) \leqslant 0$) est totalement ordonné par le degré de U ce qui est équivalent à dire qu'il est totalement ordonné par φ_0 (resp. φ_1) . En effet, si U est une m. a. et si

$\varphi_0(U) \leqslant 0$ (resp. $\varphi_0(U) > 0$), alors $\deg U = \varphi_1(U)$ (resp. $\deg U = \varphi_0(U)$)

4. Construction des meilleures approximations.

Nous allons construire les m. a. U de 1, Δ, Δ^2 qui sont telles que $\varphi_0(U) \leqslant 0$; nous savons d'après le lemme du § 2 que dans ce cas $\varphi_1(U) = \varphi_2(U) = \deg U$. De plus, ces m. a. sont totalement ordonnées par le degré de U. Nous allons construire ces m. a. en faisant croître le degré.

(a) Les m. a. de degré 0 sont les triplets $(\lambda, 0, 0)$, $\lambda \in \underline{Q}^*$:
On remarque ensuite qu'il n'y a pas de m. a. de degré strictement compris entre zéro et n, en effet, sinon $U = (U_0, 0, 0)$, avec $0 < \deg U_0 < n$ et on aurait $\deg U = \varphi_0(U) > 0$.

(b) Les m. a. de degré n : $\Delta - E(\Delta)$ à une constante multiplicative près, où $E(\Delta)$ désigne la partie polynômiale de $\Delta = X^n + \ldots$.

Soit $U \in A^3$ avec $\deg U = n$, $U = (U_0, u_1, 0)$ où $U_0 = u_0^{(0)} X^n + \ldots + u_0^n$ et $u_1 \in \underline{Q}$. Nous cherchons à trouver un $U \in A^3$ tel que $\varphi_0(U)$ soit minimal, pour cela, on développe $\varphi(U)$ en série formelle en $(1/X)$:

$$\varphi(U) = u_0^{(0)} X^n + \ldots + u_0^{(n)} + u_1 (X^n + a_1^{(1)} X^{n-1} + \ldots + a_1^{(n)} + \ldots) .$$

Nous pouvons trouver un U qui annule les $n+1$ premiers coefficients de $\varphi(U)$.

$$\begin{cases} u_0^{(0)} + u_1 = 0 \\ u_0^{(1)} + u_1 a_1^{(1)} = 0 \\ \quad \backslash \\ u_0^{(n)} + u_1 a_1^{(n)} = 0 \end{cases}$$

Réciproquement, si nous avons un $U \in A^3$ tel que $\deg U = n$ et $\varphi_0(U) \leqslant -1$, alors

$$U = (- u_1 E(\Delta), u_1, 0) \quad \text{avec} \quad u_1 \neq 0 .$$

(c) Soit q un entier $\geqslant n$, on va construire un $U \in A^3$ tel que $U \neq 0$, $\deg U \leqslant q$ et $\varphi_0(U)$ minimum.

On montrera alors que ces conditions déterminent un U à une constante multiplicative près et que ce U est une m. a.

On pose

$$U_0 = u_0^{(0)} X^q + u_0^{(1)} X^{q-1} + \ldots + u_0^{(q)}$$

$$U_1 = u_1^{(0)} X^{q-n} + u_1^{(1)} X^{q-n-1} + \ldots + u_1^{(q-n)}$$

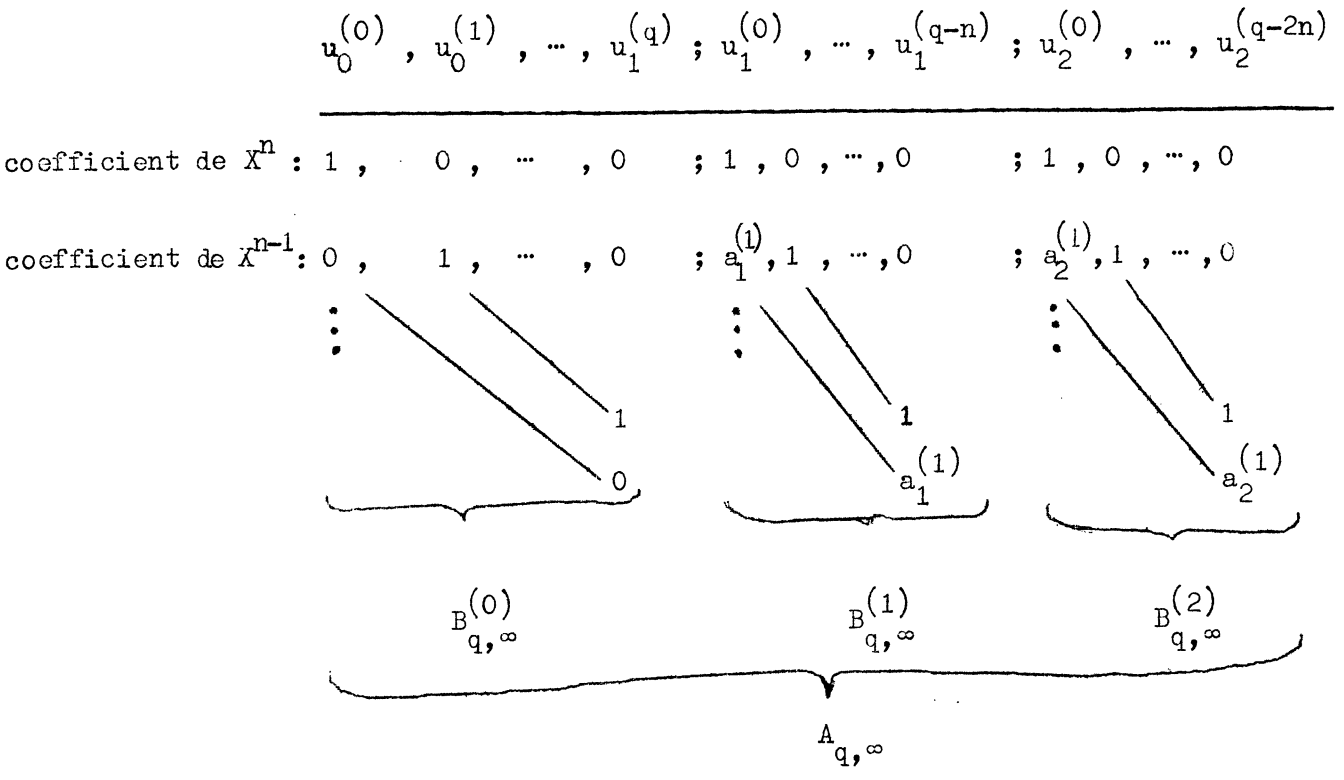
$$U_2 = u_2^{(0)} X^{q-2n} + u_2^{(0)} X^{q-2n-1} + \ldots + u_2^{(q-2n)}$$

$$\Delta = X^n + a_1^{(1)} X^{n-1} + \ldots$$

$$\Delta^2 = X^{2n} + a_2^{(1)} X^{2n-1} + \ldots$$

Si on développe $\varphi(U)$ un $\frac{1}{X}$, ses coefficients sont des combinaisons linéaires des coefficients des polynômes U_0, U_1, U_2.

Appelons $A_{q,\infty}$ la matrice de ces coefficients



Soit ℓ_q le nombre de colonnes de la matrice $A_{q,\infty}$. On considère la matrice tronquée $A_{q,m}$ formée des m premières lignes de $A_{q,\infty}$, alors on peut énoncer :

Trouver $U \neq 0$ avec $\deg U \leq q$ et $\Phi_0(U)$ minimum équivaut à trouver un entier m_q qui vérifie

$$\exists\, \tilde{U} \in \underset{\sim}{Q}^{\ell_q}\,,\ \tilde{U} \neq 0\,,\ A_{q,m_q-1}\,\tilde{U} = 0$$

$$\forall\, \tilde{U} \in \underset{\sim}{Q}^{\ell_q}\,,\ A_{q,m_q}\,\tilde{U} = 0 \Longrightarrow \tilde{U} = 0\,.$$

On remarque alors que le système $A_{q,\ell_q-1}\,\tilde{U} = 0$ a une solution non triviale et que par suite

$$\ell_q \leq m_q\,.$$

On montre alors que

$$\Phi_0(U) \leq -m_q + q + 1 \leq -\ell_q + q + 1$$

et que

$$N(U) = (\Phi_0 + \Phi_1 + \Phi_2)(U) \leq 3n - 2 \quad \text{si} \quad \left[\frac{q}{n}\right] \geq 2\,.$$

Ce nombre $3n - 2$ est le genre de la courbe dans le cas particulier où D n'a que des racines simples. Ceci n'est pas un hasard car on peut introduire les m. a. à l'aide du théorème de Riemann-Roch.

Pour construire la suite des m. a., on fait varier q de 1 à l'infini.

$$U^{(0)} = (1\ ,\ 0\ ,\ 0)\ ,\quad U^{(1)} \sim E(\Delta) - \Delta\ ,\quad E^{(2)}\ ,\ \ldots\ ,\ U^{(i)}\ ,\ \ldots$$

$$\deg U^{(0)} = 0 < \deg U^{(1)} = n < \deg U^{(2)} < \ldots < \deg U^{(i)} < \ldots$$

$$\Phi_0\, U^{(0)} = 0 > \Phi_0(U^{(1)}) > \Phi_0(U^{(2)}) > \ldots > \Phi_0(U^{(i)}) > \ldots$$

i est appelé le rang de la m. a.

Les m. a. $U^{(i)}$ sont définies à une constante multiplicative près, un moyen d'obtenir l'unicité est de choisir un système de représentants $\mathbb{S}$ de $\mathbb{Q}^*/\mathbb{Q}^{*3}$. Un élément de $\mathbb{Q}^*$ appartiendra à $\mathbb{S}$ s'il ne contient pas de puissance 3e dans sa décomposition en facteurs premiers et s'il est strictement positif :

Définition. - U est "la" m. a. de rang i si

1° $U \sim U^{(i)}$

2° $s \in \mathbb{S}$ où s est le coefficient du terme de plus haut degré du polynôme $\pi\varphi(U)$, la m. a. U définie de cette façon est unique.

En effet, soient U et V deux m. a. de rang i. Elles diffèrent donc d'une constante $U = \lambda V$, $\lambda \in \mathbb{Q}^*$. On a alors

$$\pi\varphi(U) = \lambda^3\, \pi\varphi(V)\ .$$

Si on pose

$$\pi\varphi(U) = s\, X^m + \ldots$$

$$\pi\varphi(V) = t\, X^m + \ldots$$

on en déduit l'égalité $s = \lambda^3 t$ et comme s et $t \in \mathbb{S}$, on a $\lambda^3 = 1$ et donc $\lambda = 1$.

5. Périodicité des m. a. et solution à l'équation de Pell.

On pose

$$\alpha_i = \frac{\varphi(U^{(i+1)})}{\varphi(U^{(i)})}\ ,\quad i \geqslant 0\ .$$

Définition. - On dit que la suite des m. a. est purement pseudo-périodique (resp. purement périodique) si la suite $(\alpha_i)_{i\geqslant 0}$ est telle que

$$\exists\, \pi_1 \geqslant 1\ ,\quad \forall\, q \geqslant 0\ ,\quad \forall\, r\ ,\quad 0 \leqslant r \leqslant \pi_1 - 1\ ,\quad \alpha_{q\pi_1 + r} \sim \alpha_1$$

$$(\text{resp. } \exists\, \pi_2 \geqslant 1\ ,\quad \forall\, q \geqslant 0\ ,\quad \forall\, r\ ,\quad 0 \leqslant r \leqslant \pi_2 - 1\ ,\quad \alpha_{q\pi_2 + r} = \alpha_r)\ .$$

THÉORÈME 2. - L'équation de Pell (1) a une solution non triviale si, et seulement si, la suite des m. a. est purement pseudo-périodique (i. e. purement périodique).

Ce théorème généralise le théorème : L'équation de Pell $U_0 - U_1 D = Cte \neq 0$ admet une solution non triviale si, et seulement si, le développement en fraction continue de $\sqrt{D}$ est périodique (voir [5])

6. Le cas particulier $n = 1$.

Soit $D(X) = X^3 + aX + b$, $(a , b) \neq 0$.

Grâce à un calcul fait sur Mac-syma, P. TOFFIN et B. VALLÉE ont trouvé les n. a. de rang 2,3,...,6. Nous avons pu alors dresser la liste de couples (a , b) , tels que l'équation de Pell admet une solution non triviale.

On remarque que si le couple (a , b) est tel que l'équation de Pell admet une solution non triviale c'est encore le cas pour le couple $(\lambda^2 a , \lambda^3 b)$ avec $\lambda \in \mathbb{Q}^*$. Nous résumons les résultats obtenus à l'aide du tableau

a	b	Solution fondamentale	π	i	π_1	π_2
0	$\neq 0$	$- X + \Delta$	$b = \begin{cases} \text{cube} \\ \neq \text{cube} \end{cases}$	1	1	$\begin{cases} 1 \\ 3 \end{cases}$
$\neq 0$	0	$1 + \frac{3X}{a}\Delta - \frac{3}{a}\Delta^2$	1	2	2	2
-6	6	$- X^2 - 2X + 4 + 2\Delta + \Delta^2$	4	2	2	6
-9	9	$\frac{X^3}{3} - 3X + 4 + (-\frac{X^2}{3} - X + 2)\Delta + \Delta^2$	1	3	3	3

RÉFÉRENCES

[1] ARTIN (E.). - Quadratische Körper in Gebiet der höheren Kongruenzen I, II, Math. Z., t. 19, 1924, p. 153-246.

[2] DEURING (M.). - Lectures on the theory of algebraic functions of one variable. - Berlin, Heidelberg, New York, Springer-Verlag, 1973 (Lecture Notes in Mathematics, 314).

[3] HELLEGOUARCH (Y.) et LOZACH (M.). - Equation de Pell et points d'ordre fini, "Théorie analytique et élémentaire des nombres", 30 mai - 3 juin 1983, Marseille (à paraître).

[4] NEUBRAND (M.). - Einheiten in algebraischen Funktionen und Zahlkörpern, J. für reine und angew. Math., t. 303/304, 1978, p. 170-204.

[5] SCHINZEL (A.). - On some problems of the arithmetical theory of continued fractions, Acta Arithm., Warszawa, t. 6, 1960/61, p. 393-413 ; t. 7, 1961/62, p. 287-298.