Groupe d'étude en théorie analytique des nombres

Roger Paysant-Le Roux

Unités relatives

Groupe d'étude en théorie analytique des nombres, tome 2 (1985-1986), exp. n° 13, p. 1-7
<http://www.numdam.org/item?id=TAN_1985-1986__2__A8_0>

Groupe d'étude en
THÉORIE ANALYTIQUE DES NOMBRES
3e année, 1985/86, n° 13, 7 p.

24 février 1986

UNITÉS RELATIVES

par Roger PAYSANT - LE ROUX (*)

1. Introduction.

Lorsque l'on cherche les solutions de l'équation de Pell-Fermat

$$X^2 - f^2 DY^2 = 1 , \tag{1}$$

avec D sans carré, on peut commencer par résoudre ce problème pour

$$X^2 - DY^2 = 1 , \tag{2}$$

et déterminer ensuite les solutions (x , y) de (2) telles que $f | y$.

C'est la méthode utilisée par A. SCHINZEL [1].

Une manière équivalente de formuler ce point de vue est la suivante :

Soit un anneau d'entiers A , et soit un entier Δ d'une extension du corps des quotients K de A . Si on veut connaître les unités de norme 1 de l'ordre $O_f = A[f\Delta]$, on peut déterminer les unités φ de norme 1 de l'ordre $O = A[\Delta]$, puis chercher les entiers n tels que φ^n soit une unité relative à O_f

2. Hypothèses. Notations.

Soient :

k corps

$A = \mathbb{Z}$ ou $k[X]$,

K c.d.f de A ,

Δ un élément entier algébrique sur A , séparable, de degré p ,

$\Delta^p = b_{p-1} \Delta^{p-1} + \ldots + b_0$, $b_i \in A$,

$E = K(\Delta)$,

B la fermeture intégrale de A dans E . On suppose $B = A[\Delta]$.

f un élément irréductible de A tel que $f \nmid \mathrm{Disc}_{E/K}(B)$,

G (resp. U) le groupe des unités (resp. de norme 1) de $O = A[\Delta]$

G^f (resp. U^f) le groupe des unités (resp. de norme 1) de $O^f = A + f A[\Delta]$

G_f (resp. U_f) le groupe des unités (resp. de norme 1) de $O_f = A[f\Delta]$

$f.B = \mathfrak{p}_1 \ldots \mathfrak{p}_r$ la décomposition en idéaux premiers distincts de l'idéal $f.B$ dans B .

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

Soit C un anneau, on désignera par C^* le groupe des éléments inversibles de C, et soit $s : B \longrightarrow B/fB$ l'homomorphisme canonique.

PROBLÈME. - Soit $\varphi \in G$ (resp. U) ; on cherche les entiers n tel que φ^n soit une unité (resp. unité de norme 1) relative à O_f, i. e. étude de la torsion du groupe G/G_f (resp. U/U_f).

Un ordre intermédiaire (si $p > 2$) s'introduit naturellement $O^f = A + fO$, et il permet de diviser la difficulté en deux.

3. Etude de G/G^f.

THÉORÈME 1.

(i) Soit $\varphi \in G$ ($\varphi \in G^f \iff s(\varphi) \in (A/fA)^*$).

(ii) $s(U^f)$ est contenu dans le groupe des racines p-ième de l'unité de $(A/fA)^*$.

Preuve.

(i) Dans le sens direct, soit $\varphi \in G^f$,

$$\varphi = u_0 + u_1 f\Delta + \ldots + u_{p-1} f\Delta^{p-1}, \quad u_i \in A,$$

d'où

$$s(\varphi) = s(u_0) \in A/fA.$$

Reste à montrer que $s(u_0)$ est différent de zéro. On sait que $\pi(\varphi) \in A^*$, d'où $s(\pi(\varphi)) \neq 0$, or $s(\pi(\varphi)) = s(u_0^p) = (s(u_0))^p$, on en déduit que $s(u_0) \neq 0$.

Réciproquement, soit $\varphi \in G$ et $s(\varphi) = s(a)$, $a \in A$, on a donc

$$\varphi - a \in \ker s = f.B,$$

d'où

$$\varphi = a + f(v_0 + v_1 \Delta + \ldots + v_{p-1} \Delta^{p-1}), \quad v_i \in A$$

$$\varphi = a + fv_0 + fv_1 \Delta + \ldots + fv_{p-1} \Delta^{p-1}$$

et donc $\varphi \in O^f$, or $O^f \cap G = G^f$.

(ii) Soit $\varphi \in U^f$,

$$\varphi = u_0 + u_1 f\Delta + \ldots + u_{p-1} f\Delta^{p-1}, \quad u_i \in A$$

on calcule $s(\varphi_0^p)$,

$$s(\varphi_0^p) = s(u_0^p) = s(\pi(\varphi)) = s(1) = 1$$

et

$$s(\varphi) \in (A/fA)^*.$$

Applications.

(a) Corps globaux ($A = \mathbb{Z}$ ou $\mathbb{F}_q[X]$) . - On pose :

$$|f| = \begin{cases} \text{valeur absolue habituelle si } A = \mathbb{Z} \\ q^{\deg f} \quad \text{si } A = \mathbb{F}_q[x] . \end{cases} \quad \text{pour } f \in A .$$

THÉORÈME 2. - Le groupe quotient G/G^f est un groupe de torsion, dont la torsion est première avec $|f|$, et bornée par $|f|^\gamma - 1$; plus précisément, pour tout φ appartenant à G, on a $\varphi^{|f|^\gamma - 1}$ appartient à G^f, où $\gamma = \text{ppcm } \beta_i$,

$$\beta_i = [B/\mathfrak{p}_i : A/fA] .$$

Preuve. - On a l'isomorphisme

$$B/fB \simeq (B/\mathfrak{p}_1) \times \ldots \times (B/\mathfrak{p}_r)$$

et

$$|B/\mathfrak{p}_i| = |f|^{\beta_i} , \quad \forall\, i = 1 , \ldots , r .$$

Si on pose $s_i = pr_i \circ s$, où pr_i est la i-ième projection de B/fB dans $B/\mathfrak{p}_i$, on a l'égalité

$$(s_i(\varphi))^{|f|^\gamma - 1} = 1 , \quad \forall\, i = 1 , \ldots , r$$

et donc

$$(s(\varphi))^{|f|^\gamma - 1} = 1 \in (A/fA)^*$$

d'après le théorème 1, on en conclut que $\varphi^{|f|^\gamma - 1} \in G^f$.

(b) Corps de fonctions. - $A = k[X]$ où k est un corps ayant une infinité d'éléments.

THÉORÈME 3. - On suppose que le rang du groupe U est égal à un. Soit φ_0 une unité fondamentale de U . On a l'équivalence

$$U^f \text{ non trivial} \iff s_i(\varphi_0) \text{ est une racine de l'unité du corps } B/\mathfrak{p}_i .$$

De plus, si U^f est non trivial et si on pose :

$$n_0 = \text{Inf}\{n \in \mathbb{N}^* , \ s(\varphi_0^n) \in A/fA\} ,$$

alors $n_0 = [U : U^f]$.

Preuve. - Dans le sens direct, supposons U^f non trivial, alors il existe un entier non nul n tel que $\varphi_0^n \in U^f$, d'après le théorème 1,

$$(s(\varphi_0^n))^p = (s(\varphi_0))^{np} = 1 .$$

Réciproquement, si

$$\exists\, n \in \mathbb{N}^* \,,\quad (s_i(\varphi_0))^{n_i} = 1 \,,\quad \forall\, i = 1 \,, \ldots \,, r \,,$$

on en déduit

$$\exists\, n = \mathrm{ppcm}(n_i) \,,\quad (s_i(\varphi_0))^{n} = 1 \,,\quad \forall\, i = 1 \,, \ldots \,, r \,,$$

et donc

$$s(\varphi_0)^n = 1 \in A/fA$$

d'après le théorème 1, $\varphi_0^n \in G^f$.

Exemple. - On prend :

$$\begin{cases} A = \mathbb{Q}[X] \\ \Delta^2 = X^2 - h \,, \quad h \in \mathbb{Q}^* \,; \end{cases}$$

l'unité fondamentale de U est

$$\varphi_0 = \begin{cases} (X - \Delta)/\sqrt{h} & \text{si } h \text{ est un carré dans } \mathbb{Q}^* \,, \\ 1 - (2X^2/h) + (2X/h)\,\Delta \,, & \text{sinon.} \end{cases}$$

On pose $D = X^2 - h$, et comme élément irréductible de A on prend $f = X - a$, $a \in \mathbb{Q}$.

COROLLAIRE 1 (A. SCHINZEL). - U_{X-a} est non trivial si, et seulement si, $a = 0$ ou $h = 2a^2$ ou $4a^2$ ou $4/3\, a^2$.

Preuve. - Pour utiliser le théorème 3, il nous faut étudier la décomposition de l'idéal $(X - a)\,A$ dans $B = A[\Delta]$ (on a bien ici que la fermeture intégrale de A dans E est $A[\Delta]$).

Nous avons trois possibilités :

(1) Si $D(a) = a^2 - h$ est un carré dans $\mathbb{Q}^*$

$$\begin{array}{ccc} \mathfrak{p} \neq \bar{\mathfrak{p}} & & B/\mathfrak{p} \text{ et } B/\bar{\mathfrak{p}} \simeq \mathbb{Q} \\ \diagdown\ \diagup & & | \\ (X - a)\,A & & A/(X - a)\,A \simeq \mathbb{Q} \,. \end{array}$$

L'idéal $(X - a)\,B$ se décompose en deux idéaux premiers distincts, conjugués, et on n'a pas d'extension du corps des restes.

(2) Si $D(a) = a^2 - h$ n'est pas un carré dans $\mathbb{Q}^*$

$$\begin{array}{ccc} \mathfrak{p} & & B/\mathfrak{p} \simeq \mathbb{Q}(\sqrt{D(a)}) \\ | & & | \\ (X - a)\,A & & A/(X - a)\,A \simeq \mathbb{Q} \,. \end{array}$$

L'idéal $(X - a)\,B$ est premier, et on a une extension du corps des restes (extension quadratique de $\mathbb{Q}$).

(3) Si $D(a) = 0$, i. e. $h = a^2$, dans ce cas $f|D$, l'hypothèse que nous avons faite sur f ne nous permet pas de conclure, cependant, on peut montrer que U_{X-a} est trivial.

Toujours d'après le théorème 3, il faut chercher les racines de l'unité dans le corps $B/\mathfrak{p}_i$:

Si on est dans (1) ou (2) avec $D(a) > 0$, les racines de l'unité sont ± 1 .

Si on est dans (2) avec $D(a) < 0$, les racines de l'unité peuvent être : ± 1 , $\pm i$, $\pm j$, $\pm j^2$.

Finalement :

$$s(\varphi_0) = \begin{cases} j \\ \text{ou} \\ j^2 \end{cases} \Longrightarrow h = (4/3)a^2 \quad \text{ou } 4a^2 ,$$

$$s(\varphi_0) = \begin{cases} -j \\ \text{ou} \\ -j^2 \end{cases} \Longrightarrow h = 4a^2 ,$$

$$s(\varphi_0) = \begin{cases} i \\ \text{ou} \\ -i \end{cases} \Longrightarrow h = 2a^2 ,$$

$$s(\varphi_0) = \begin{cases} 1 \\ \text{ou} \\ -1 \end{cases} \Longrightarrow a = 0 .$$

4. Etude de G^f/G_f

THÉORÈME 4.

(i) Corps de nombres. Corps de fonctions sur un corps k de caractéristique $\ell \neq 0$:

G^f/G_f est un groupe de $|f|$ (resp. ℓ) torsion dont la torsion est bornée par $|f|^{p-1}$ (resp. $\ell^{\{\log(p-1)\}}$).

(ii) Corps de fonctions de caractéristique nulle :

G^f/G_f est sans torsion.

Preuve.

(i) Ceci résulte de la formule du binôme. Dans le cas des corps de nombres, soit $\varphi \in G^f$,

$$\varphi = u_0 + u_1 f\Delta + \ldots + u_{p-1} f\Delta^{p-1} ,$$

on calcule φ^f

$$\varphi^f = u_0^f + u_1^f f^f \Delta^f + \ldots + u_{p-1}^f f^f \Delta^{f(p-1)}$$

$$+ \sum_{(i_0,\ldots,i_{p-1})\in I} \frac{f!}{i_0! \ldots i_{p-1}!} u_0^{i_0} \ldots u_{p-1}^{i_{p-1}} f^{\sum_{k=1}^{p-1} i_k} \Delta^{\sum_{k=1}^{p-1} k i}$$

où $I = \{(i_0, \ldots, i_{p-1}) \in \mathbb{N}^p$, $\sum_{k=0}^{p-1} i_k = f$ et $i_k \neq f$, $\forall k\}$, on voit que φ^f peut s'écrire :

$$\varphi^f = v_0 + v_1 f^2 \Delta + \ldots + v_{p-1} f^2 \Delta^{p-1} ,$$

et on itère le procédé.

(ii) Idée de la démonstration : On se place dans le cas particulier $\Delta^3 = D$.

Soit $\varphi = u_0 + u_1 \Delta + u_2 \Delta^2 \in G^f$. On suppose qu'il existe un entier q supérieur ou égal à 2 tel que

$$\varphi^q = v_0 + v_1 \Delta + v_2 \Delta^2 \in G_f ,$$

ce qui permet d'écrire

$$v_2 = u_0^{q-1} u_2 + \sum_I \frac{q!}{i_0!\, i_1!\, i_2!} u_0^{i_0} u_1^{i_1} u_2^{i_2} D^{\alpha(i_0,i_1,i_2)}$$

où

$$I = \{(i_0 , i_1 , i_2) \in \mathbb{N}^3 , \ i_0 + i_1 + i_2 = q , \ i_1 + 2i_2 \equiv 2 \pmod 3 , \ i_0 \leqslant q - 2\}$$

$$\alpha(i_0 , i_1 , i_2) = \frac{i_1 + 2i_2 - 2}{3} .$$

Or, on a

$$f^2 | u_0^{i_0} u_1^{i_1} u_2^{i_2} , \quad \forall (i_0 , i_1 , i_2) \in I$$

et $f^2 | v_2$ par hypothèse.

On en déduit que $f^2 | u_0^{q-1} u_2$ et donc, puisque $f \nmid u_0$, que $f^2 | u_2$.

C. Q. F. D.

COROLLAIRE 2. - Soit D un polynôme de la forme $X^3 + aX + b$, avec a et $b \in \mathbb{Q}$.

Soit Δ appartenant à $\mathbb{Q}((1/X))$ vérifiant $\Delta^3 = D$. Pour tout rationnel α , le groupe des unités de l'ordre $O_{X-\alpha}$ est trivial.

Preuve. - Il n'est pas difficile de montrer que si D a une racine double, le

groupe des unités de O est trivial. On suppose donc D sans racine double. Dans ce cas, $B = A[\Delta]$, et on connait les couples (a , b) [1] pour lesquels le groupe U des unités de norme 1 de O est non trivial, et pour un tel couple on connait une unité fondamentale φ_n de U. On continue alors comme dans le corollaire 1.

BIBLIOGRAPHIE

[1] HELIEGOUARCH (Y.), Mc QUILLAN (D. L.) et PAYSANT - LE ROUX (Roger). - Unités de certains sous-anneaux des corps de fonctions algébriques, Acta Arithm., Warszawa (à paraître).

[2] LOZAC'H (M.) et PAYSANT - LE ROUX (Roger). - Unités relatives, Prépublication de l'Université de Caen n° 30.

[3] SCHINZEL (A.). - On some problems of the arithmetical theory of continued fractions, I-II, Acta Arithm., Warszawa, t. 6, 1961, p. 393-413 et t. 7, 1962, p. 287-298.