Groupe d'étude en théorie analytique des nombres

Yves Hellegouarch

X-unités de certains corps de fonctions algébriques, II

Groupe d'étude en théorie analytique des nombres, tome 1 (1984-1985), exp. n° 19, p. 1-14

<http://www.numdam.org/item?id=TAN_1984-1985__1__A2_0>

Groupe d'étude en
THÉORIE ANALYTIQUE DES NOMBRES
1re-2e années, 1984-1985, n° 19, 14 p.

12 novembre 1984

X-UNITÉS DE CERTAINS CORPS DE FONCTIONS ALGÉBRIQUES, II

par Yves HELLEGOUARCH (*)

1. Rappel du point de départ du premier exposé.

1.1. - Dans le premier exposé on s'était donné :

$$D(X) = X^{3n} + a_{3n-1} X^{3n-1} + \ldots + a_0 \in A$$

avec $A = \mathbb{Q}[X]$, et on avait considéré la série formelle :

$$\Delta = X^n [1 + \frac{1}{X}(a_{3n-1} + \ldots + \frac{a_0}{X^{3n-1}})]^{1/3} \in \mathbb{Q}((\frac{1}{X}))$$

que nous avions appelée la "racine réelle" de $Y^3 = D(X)$.

Alors on avait introduit les objets suivants :

$$\begin{cases} K = \mathbb{Q}(X) \\ E = K(\Delta) \subset \mathbb{Q}((\frac{1}{X})) \\ B = A[\Delta] . \end{cases}$$

1.2 Généralisation. - Cette généralisation a été faite en collaboration avec D. L. Mc QUILLAN.

On se donne un corps k et un corps de fonctions algébriques E sur k (1). On se donne aussi un élément non constant X de E.

On désignera par A l'anneau $k[X]$, et par B la fermeture intégrale de A dans E.

Définition. - On appellera "ordre de E relativement à X" tout anneau $\mathcal{O}$ vérifiant les conditions :

1° $A \subset \mathcal{O} \subset B$

2° le corps des quotients de $\mathcal{O}$ est égal à E.

Le but de ce travail est une étude du groupe des unités de $\mathcal{O}$, groupe que l'on notera $\mathcal{U}(\mathcal{O})$.

Un premier procédé consiste à introduire le corps $k(X)$, que l'on désignera par K, et à utiliser la norme $\pi_{E/K}$. Nous démontrerons d'abord le résultat suivant.

THÉORÈME 1. - Soit un ordre $\mathcal{O}$ de E relativement à X. Alors $\varphi \in \mathcal{U}(\mathcal{O})$ équivaut à $\pi_{E/K}(\varphi) \in k^*$ et $\varphi \in \mathcal{O}$.

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

(1) On suppose que k est maximal en ce sens que tout élément X de $E \setminus k$ est transcendant sur k.

Remarque. - Nous dirons que la seconde condition est une "équation de Pell" généralisée.

Dans cette perspective, l'étude de $\mathcal{U}(\mathcal{O})$ est l'étude des solutions (dans $\mathcal{O}$) de l'équation de Pell.

Nous fractionnerons la démonstration du théorème 1 en un certain nombre de lemmes.

LEMME 1. - Si $\varphi \in B$, $\varphi \in \mathcal{U}(B)$ équivaut à $\pi_{E/K}(\varphi) \in k^*$.

Preuve.

1° Soit $\varphi \in \mathcal{U}(B)$, alors il existe $\psi \in B$ tel que $\varphi\psi = 1$. En prenant la norme, on en déduit que :

$$\pi_{E/K}(\varphi) \times \pi_{E/K}(\psi) = 1 .$$

Mais comme φ et $\psi \in B$, on sait que $\pi_{E/K}(\varphi)$ et $\pi_{E/K}(\psi) \in A$. Il en résulte que $\pi_{E/K}(\varphi) \in \mathcal{U}(A) = k^*$.

2° Réciproquement, soit $\varphi \in B$ tel que $\pi_{E/K}(\varphi) \in k^*$. Alors $\pi_{E/K}(\varphi) = \varphi.\rho$ où ρ est un entier sur A.

On a donc $\varphi\rho = \alpha \in k^*$, d'où $\rho = \frac{\alpha}{\varphi} \in E$, donc $\rho \in B$ et $\frac{\rho}{\alpha} \in B$. Si l'on pose $\psi = \frac{\rho}{\alpha}$, on voit donc que $\varphi\psi = 1$ avec φ et $\psi \in B$, donc φ est une unité de B.

1.3 Places à l'infini. - On appellera "place à l'infini" sur le corps $\underset{\sim}{Q}((\frac{1}{X}))$ l'application qui à

$$\sum_{n \geq -n_0} a_n (\tfrac{1}{X})^n , \quad a_{n_0} \neq 0$$

fait correspondre

$$\infty \text{ si } n_0 > 0 ,$$

$$a_0 \text{ si } n_0 = 0$$

et

$$0 \text{ si } n_0 < 0 .$$

Puisque l'on se trouvait en 1.1 devant une tour d'extensions :

$$\begin{array}{c} \underset{\sim}{Q}((\frac{1}{X})) \\ | \\ E = K(\Delta) \\ | \\ K = \underset{\sim}{Q}(X) \end{array}$$

les restrictions P_0 et $\mathfrak{p}_\infty$ de cette place à E et à K seront des places sur E et K dites "places à l'infini". En ce sens P_0 est une prolongement "canonique" de $\mathfrak{p}_\infty$ de degré 1.

$\mathfrak{p}_\infty$ possède une autre extension (de degré 2) à E que l'on notera P_1.

Généralisation. - Dans toute la suite de ce travail, nous désignerons par $\wp_\infty$ la place à l'infini de K, c'est-à-dire la place triviale sur k qui envoie X sur ∞.

Alors on sait [D] que E ne possède qu'un nombre fini de places au-dessus de $\wp_\infty$, nous désignerons ces places par $P_0, \ldots, P_{t-1}$.

LEMME 2. - Soit $\varphi \in E$, les conditions suivantes sont équivalentes :

(a) $\varphi \in B$,

(b) les seules places P de E telles que $P(\varphi) = \infty$ sont $P_0, \ldots, P_{t-1}$.

Preuve. - Montrons que (a) $\Longrightarrow$ (b). Puisque $\varphi \in B$, on a

$$\varphi^n + a_1 \varphi^{n-1} + \ldots + a_n = 0 \quad \text{avec} \quad a_i \in A .$$

Supposons que $P(\varphi) = \infty$, alors $P(\frac{1}{\varphi}) = 0$. Mais on a

$$1 + a_1(\frac{1}{\varphi}) + \ldots + a_n(\frac{1}{\varphi})^n = 0$$

et si $P \neq P_i$, pour $i \in \{0, \ldots, t-1\}$, on obtient $1 = 0$ en appliquant P aux deux membres de cette équation.

Montrons que (b) $\Longrightarrow$ (a).

Soit $\varphi \in E$. Si φ^{-1} est une unité de l'anneau $A[\varphi^{-1}]$, on obtient que $\varphi \in A[\varphi^{-1}]$, d'où

$$\varphi = a_0 + a_1 \varphi^{-1} + \ldots + a_r \varphi^{-r} , \quad a_i \in A ,$$

ce qui entraîne que

$$\varphi^{r+1} - a_0 \varphi^r - a_1 \varphi^{r-1} - \ldots - a_r = 0 ,$$

d'où $\varphi \in B$.

Supposons donc que φ^{-1} n'est pas une unité de $A[\varphi^{-1}]$, alors φ^{-1} appartient à un idéal maximal $\mathfrak{m}$ de $A[\varphi^{-1}]$. D'après un résultat général [B], il existe un anneau de valuation (V, M) tel que $V \supset A[\varphi^{-1}]$ et $\mathfrak{m} = M \cap A[\varphi^{-1}]$.

(V, M) détermine une place P de E qui est finie sur A et qui est telle que $P(\varphi^{-1}) = 0$.

Donc $P(\varphi) = \infty$ et, d'après la condition (b), $P \in \{P_1, \ldots, P_t\}$, donc $P(X) = \infty$!

LEMME 3. - $\mathcal{O} \cap \mathcal{U}(B) = \mathcal{U}(\mathcal{O})$.

Preuve. - Soit $\varphi \in \mathcal{O} \cap \mathcal{U}(B)$, je dis que $\varphi \in \mathcal{U}(\mathcal{O})$.

En effet, nous avons $\varphi . \psi = 1$ avec $\psi \in B$. Si $\varphi \notin \mathcal{U}(\mathcal{O})$, il existe un idéal maximal $\mathfrak{m}$ tel que $\varphi \in \mathfrak{m}$.

D'après un résultat général [B], il existe un anneau de valuation (V, M) tel que $V \supset \mathcal{O}$ et $\mathfrak{m} = M \cap \mathcal{O}$.

$(V , \mathbb{M})$ définit une place P de E qui est finie sur $\mathcal{O}$ et qui est telle que $P(\varphi) = 0$. On a donc $P(\psi) = \infty$, et comme $\psi \in B$, le lemme 2 montre que $P \in \{P_1 , \ldots , P_t\}$.

On en déduit que $P(X) = \infty$, donc P ne peut pas être finie sur A ;

Avec ce troisième lemme s'achève la démonstration du théorème 1

1.4 Est-ce que $B = A[\Delta]$?

On se donne un entier $p > 0$, un corps k dont la caractéristique ne divise pas p et un polynôme unitaire D de degré pn , avec $n > 0$.

On pourrait aussi supposer que le coefficient du terme de plus haut degré de D est puissance p-ième d'un élément de k^* , mais cela ne change rien. On a donc

$$D(X) = X^{pn} + a_1 X^{pn-1} + \ldots \in k[X] .$$

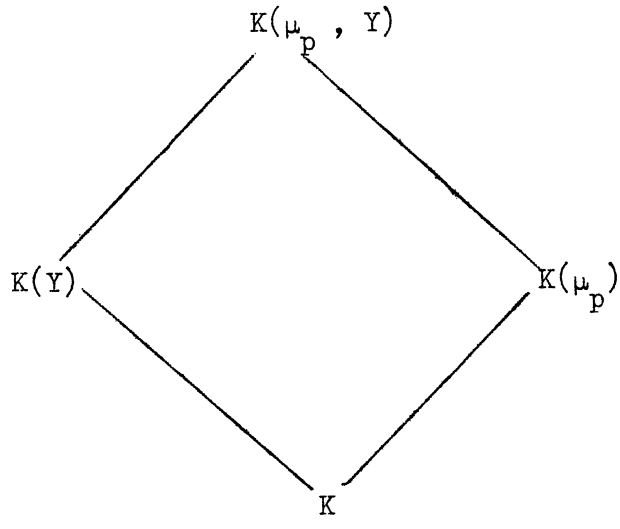
Dans toute la suite, $\bar{k}$ sera fixée, et μ_p désignera le groupe des racines p-ièmes de l'unité dans $\bar{k}$. Rappelons le résultat suivant.

On fera successivement deux hypothèses sur D :

1° Hypothèse faible : $D(X)$ n'est puissance q-ième d'un polynôme de $k(\mu_p)[X]$ pour aucun premier q divisant p et, si p est divisible par 4 , $-\frac{D}{4}$ n'est pas une puissance quatrième (ceci assure l'irréductibilité de $Y^p - D(X)$).

2° Hypothèse forte : $D(X)$ n'a pas de racine multiple dans une clôture algébrique $\bar{k}$ de k .

PROPOSITION 1. - On suppose que l'hypothèse faible est vérifiée, on pose $K = k(X)$, et on désigne par Y une racine p-ième de $D(X)$, alors on a



1° $$[K(\mu_p , Y) : K(\mu_p)] = [K(Y) : K] = p$$

$$[K(\mu_p , Y) : K(Y)] = [K(\mu_p) : K] \leqslant \varphi(p)$$

2° $\quad \mathrm{Gal}\, K(\mu_p\ ,\ Y)/K(\mu_p) \cong Z/pZ$

$\mathrm{Gal}\, K(\mu_p\ ,\ Y)/K(Y) \cong \mathrm{Gal}\, K(\mu_p)/K \cong \mathrm{Gal}\, k(\mu_p)/k \cong G \subseteq (Z/pZ)^*$.

On désigne par $k((\frac{1}{X}))$ le corps de séries formelles en $\frac{1}{X}$ du type

$$F(X) = \sum_{n \geqslant n_0} a_n X^{-n} \ , \quad a_n \in k \ .$$

Lorsque $F(X) \neq 0$, si on suppose $a_{n_0} \neq 0$, on dit que $-n_0$ est le degré de F ; lorsque $F(X) = 0$, on pose degré de F égal à $-\infty$, on le note $\deg(F)$. On désigne par t l'application

$$k((\tfrac{1}{X})) \longrightarrow k$$

$$F \longrightarrow t(F) = \begin{cases} a_{n_0} & \text{si } F \neq 0 \\ 0 & \text{si } F = 0 \ . \end{cases}$$

On dira que $F(X)$ est <u>unitaire</u> lorsque $t(F) = 1$

PROPOSITION 2. - <u>L'équation</u> $Y^p = D(X)$ <u>admet une solution unitaire</u> Δ <u>dans</u> $k((\frac{1}{X}))$.

<u>Preuve</u>. - $D(X) = X^{pn}[1 + \frac{1}{X} R(\frac{1}{X})]$, où $R(\frac{1}{X})$ est un polynôme en $\frac{1}{X}$ de degré $pn - 2$. La formule du binôme de Newton nous permet de définir $D^{1/p}$ parce que la caractéristique de k ne divise pas p , nous avons

$$\Delta(X) = X^n[\textstyle\sum_{i=0}^{\infty} C^i_{1/p} X^{-i} R^i(\frac{1}{X})] \ .$$

D'après la proposition 1, $\Delta(X)$ est un élément algébrique de degré p sur $k(X)$, et on a degré $\Delta(X) = n$ (en tant que série formelle).

THÉORÈME 2. - <u>On suppose l'hypothèse faible vérifiée. On met</u> D <u>sous la forme</u> $Q_1^{\alpha_1} \ldots Q_s^{\alpha_s} . F$, où Q_1 ; ... , Q_s <u>sont des polynômes irréductibles distincts sur</u> $k(X)$ **avec** $\alpha_\ell \geqslant 2$ pour $1 \leqslant \ell \leqslant s$ et $(Q_\ell , F) = 1$ pour $1 \leqslant \ell \leqslant s$.

<u>On suppose, de plus,</u> F <u>sans racine multiple dans</u> $\bar{k}$ <u>et les</u> α_ℓ <u>premiers avec</u> p pour $1 \leqslant \ell \leqslant s$.

<u>Sous ces hypothèses, la clôture intégrale</u> B <u>de</u> A <u>dans</u> E <u>est l'ordre formé des fonctions</u> f <u>de la forme</u>

$$f = \frac{U_0 + U_1 Y + \ldots + U_{p-1} Y^{p-1}}{Q_1^{\alpha_1} \ldots Q_s^{\alpha_s}} \ ,$$

<u>où les polynômes</u> U_i <u>appartiennent à</u> A <u>et vérifient la condition</u>

$$\forall\, i\ ,\ \forall\, \ell\ ,\quad Q_\ell^{\alpha_\ell - j} \mid U_i \quad \text{où} \quad j = [\tfrac{ip}{\alpha_\ell}] \ .$$

COROLLAIRE 5. - Si on suppose l'hypothèse forte vérifiée, la clôture intégrale B de A dans E est $k[X , Y]$.

COROLLAIRE 6. - Si $p = 3$, et si D est de la forme $Q^2.F$, avec Q sans facteur carré, F sans racine multiple dans $\bar{k}$, $(Q , F) = 1$. Si on pose $\bar{D} = QF^2$, on a

$$B = A + AY + A\bar{Y} \quad \text{où} \quad \bar{Y}^3 = \bar{D} \quad \text{avec} \quad (\bar{Y} = \frac{Y^2}{Q}) .$$

Preuve. - Soit $f \in B$, alors

$$f = \frac{U_0 + U_1 Y + \ldots + U_{p-1} Y^{p-1}}{Q} ,$$

avec $U_i \in A$ pour $0 \leqslant i \leqslant p - 1$, $Q \in A$ non nul.

On peut supposer $(Q , U_0 , U_1 , \ldots , U_{p-1}) = 1$ et $Q \notin k$ (en effet, si $Q \in k^*$, $f \in B$).

Soit P un polynôme irréductible divisant Q , $(P^\beta | \ | Q)$ nous allons montrer qu'alors P ne peut être qu'un Q_i .

Soit $\mathfrak{p}$ un diviseur premier de $k(\mu_p , X , Y)$ au-dessus de P , et soit φ la fonction $U_0 + U_1 Y + \ldots + U_{p-1} Y^{p-1}$ on a, d'après le lemme 2,

$$f \in B \Longrightarrow v_{\mathfrak{p}}(\varphi) \geqslant v_{\mathfrak{p}}(Q) \geqslant \beta\alpha \geqslant 1 \quad \text{si} \quad v_{\mathfrak{p}}(P) = \beta\alpha$$

et, pour des raisons galoisiennes, σ désignant un générateur du groupe de Galois,

$$v_{\mathfrak{p}}(\sigma^i(\varphi)) = v_{\mathfrak{p}}(\varphi) , \quad \forall\, i , \quad 0 \leqslant i \leqslant p - 1 ,$$

on en déduit que

$$v_{\mathfrak{p}}(p U_i Y^i) = v_{\mathfrak{p}}(\textstyle\sum_{j=0}^{p-1} \xi^i \sigma^j(\varphi)) \geqslant \beta\alpha , \ \forall\, i , \ 0 \leqslant i \leqslant p - 1$$

et, a fortiori, $v_{\mathfrak{p}}(U_i Y^{p-1}) \geqslant \beta\alpha$.

Mais comme $(P , U_0 , \ldots , U_{p-1}) = 1$, il existe des polynômes $V_0, V_1, \ldots, V_{p-1} \in A$ tels que $(P , \sum_{i=0}^{p-1} U_i V_i) = 1$.

On en déduit que

$$v_{\mathfrak{p}}(Y^{p-1}) = v_{\mathfrak{p}}((\textstyle\sum U_i V_i) Y^{p-1}) \geqslant \beta\alpha ,$$

d'où

$$v_{\mathfrak{p}}(D) = v_{\mathfrak{p}}(Y^p) > \beta\alpha \geqslant v_{\mathfrak{p}}(P) .$$

Ainsi P^2 divise D , ce qui montre bien que P ne peut être qu'un Q_i .

Cherchons maintenant à quelle condition la fonction

$$f = \frac{U_0 + U_1 Y + \ldots + U_{p-1} Y^{p-1}}{Q_1^{\beta_1} \ldots Q_s^{\beta_s}}$$

est un entier sur A .

On a, toujours d'après le lemme 2,

$$f \in B \iff v_{q_\ell}(\varphi) \geqslant \beta_\ell \quad \text{pour} \quad 1 \leqslant \ell \leqslant s ,$$

où q_ℓ est le diviseur premier de $k(X , Y)$ au-dessus de Q_ℓ et v_{q_ℓ} la valuation associée à q_ℓ et telle que $v_{q_\ell}(Q_\ell) = 1$, on a alors $v_{q_\ell}(q_\ell) = \frac{1}{p}$ car on a supposé $(\alpha_\ell , p) = 1$ pour $1 \leqslant \ell \leqslant s$.

Désignons par q un q_ℓ , α un α_ℓ , β un β_ℓ , on a

$$v_q(U_i Y^i) = v_q(U_i) + \frac{i\alpha}{p} , \quad 0 \leqslant i \leqslant p - 1 ,$$

comme d'autre part $(\alpha , p) = 1$, on a

$$v_q(U_i Y^i) \neq v_q(U_j Y^j) \quad \forall\, i , j , \ i \neq j ,$$

et donc

$$v_q(\varphi) \geqslant \beta \iff Q^\beta | U_i , \ 0 \leqslant i < \frac{P}{\alpha} , \ Q^{\beta-1} | U_i , \ \frac{P}{\alpha} \leqslant i < \frac{2P}{\alpha} , \ \ldots$$

en remarquant que si $\beta > \alpha$, alors $Q | U_0 , \ldots , U_{p-1}$, on peut donc supposer $\beta \leqslant \alpha$ et en multipliant le numérateur et le dénominateur par $Q^{\alpha-\beta}$, mettre tout élément f de B sous la forme

$$f = \frac{U_0 + U_1 Y + \ldots + U_{p-1} Y^{p-1}}{Q_1^{\alpha_1} \ldots Q_s^{\alpha_s}}$$

et la condition du théorème est celle trouvée en tenant compte de cette transformation.

2. Décomposition du groupe des diviseurs en somme directe.

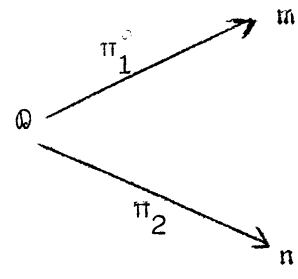
Nous désignerons par $\mathfrak{D}$ le groupe des diviseurs de E , c'est $\mathfrak{D} = \coprod_P Z\,P$, où P décrit l'ensemble des places (non équivalentes) de E . Si l'on pose

$$\mathfrak{m} = Z\,P_0 \oplus \ldots \oplus Z\,P_{t-1} ,$$

$$\mathfrak{n} = \coprod_{P \neq P_i} Z\,P , \quad i = 0 , \ldots , t - 1 .$$

Il est clair que $\mathfrak{D} = \mathfrak{m} \oplus \mathfrak{n}$.

Nous désignerons par π_1 et π_2 les projecteurs associés à cette décomposition en somme directe



PROPOSITION 1.

1° Il existe un isomorphisme j, et un seul, de n sur le groupe des idéaux fractionnaires de B qui envoie une place P de E sur l'idéal premier

$$j(P) = \{\varphi \in B \; ; \; P(\varphi) = 0\} .$$

2° Si $\varphi \in E \setminus \{0\}$, alors $j \circ \pi_2[\mathrm{div}(\varphi)]$ est l'idéal fractionnaire de B engendré par φ.

3° $\mathrm{Ker}(j \circ \pi_2 \circ \mathrm{div}) = \mathfrak{U}(B)$.

Comme plus haut, nous démontrerons d'abord un lemme.

LEMME 4. - Soit $\varphi \in B \setminus \{0\}$ et P une place $\notin \{P_0 , \dots , P_{t-1}\}$. Alors, pour tout $n \in \mathbb{N}$, on a l'équivalence

$$v_P(\varphi) = n \iff \varphi \in [j(P)]^n \setminus [j(P)]^{n+1} .$$

Preuve. - Cette preuve utilise principalement le fait que la valuation associée à P est discrète [D].

Soit (V , M) l'anneau de valuation de P, et soit π un générateur de M, on a donc

$$\varphi = u\pi^n , \quad u \text{ unité de } V .$$

Puisque E est le corps des quotients de B, on peut écrire

$$\varphi = \frac{u_1}{u_2} \left(\frac{\pi_1}{u_3}\right)^n ,$$

où $u_1 , u_2 , u_3 \in B \setminus j(P)$ et $\pi_1 \in j(P)$. On en déduit que

$$\varphi \, u_2 \, u_3^n = u_1 (\pi_1)^n \in [j(P)]^n$$

et, comme $u_2 \, u_3^n \notin j(P)$, on voit que $\varphi \in [j(P)]^n$.

Mais si $\varphi \in [j(P)]^{n+1}$, on a $\pi_1^n \in [j(P)]^{n+1}$, donc $[j(P)]^{n+1}$ divise $(\pi_1 \, B)^n$, ce qui entraîne que $[j(P)]^2$ divise $(\pi_1 \, B)$, et $v_P(\pi_1) \geqslant 2$, ce qui est absurde.

Démonstration de la proposition 1. - La première partie résulte de la propriété universelle des groupes abéliens libres.

Pour la deuxième partie, on utilise le lemme 4 qui entraîne que, si $P \notin \{P_0 , \dots , P_{t-1}\}$, $v_p(\varphi) = n$ equivaut à dire que $[j(P)]^n$ divise exactement $\varphi \, B$.

La troisième partie résulte du lemme 2.

Si $\varphi \in \mathfrak{U}(B)$, alors $\varphi^{-1} \in B$, et les zéros et pôles de φ appartiennent à $\{P_0 , \dots , P_{t-1}\}$. Il en résulte que $\mathrm{div}(\varphi) \in \mathfrak{m}$ et $\pi_2[\mathrm{div}(\varphi)] = 0$.

Dans toute la suite, nous désignerons par $\mathfrak{D}_0$, $\mathfrak{m}_0$, $\mathfrak{n}_0$ les sous-groupes de $\mathfrak{D}$, $\mathfrak{m}$, $\mathfrak{n}$ constitués par les diviseurs de degré zéro, et nous désignerons par $\mathfrak{P}$ le sous-groupe des diviseurs principaux de $\mathfrak{D}$.

Dans ce travail, nous nous intéresserons principalement au groupe quotient $\mathcal{S} = \mathcal{U}(B)/k^*$, c'est-à-dire au groupe des solutions de l'équation de Pell (dans B) définies à une constante multiplication près.

THÉORÈME 3.

1° $\mathcal{S} \cong \mathfrak{m}_0 \cap \mathcal{P}$.

2° Le groupe des classes d'idéaux de B est isomorphe à $\mathfrak{n}/\pi_2(\mathcal{P})$.

Preuve.

1° Nous considérons l'homorphisme :

$$L \begin{cases} \mathcal{U}(B) \longrightarrow \mathfrak{m}_0 \cap \mathcal{P} \\ \varphi \longmapsto \operatorname{div}(\varphi) . \end{cases}$$

Il est clair que L est surjective, et comme $\operatorname{Ker} L = k^*$, on obtient

$$\operatorname{Im} L \cong \mathcal{U}(B)/\operatorname{Ker} L \cong \mathcal{S}(B) . \tag{1}$$

2° Une manière de décrire le groupe des classes d'idéaux de B est la suivante : Deux idéaux fractionnaires I et J de B sont dits "équivalents", si, et seulement s'il existe $\varphi \in B \setminus \{0\}$ telle que

$$J = I.(\varphi B) . \tag{2}$$

D'après la proposition 1, il existe des diviseurs C et D dans $\mathfrak{n}$ tels que

$$I = j(C) \quad \text{et} \quad J = j(D) ,$$

et la relation (2) équivaut à

$$D = C + \pi_2[\operatorname{div}(\varphi)].$$

COROLLAIRE 1.

1° $\mathcal{S}$ est libre et son rang est majoré par $t - 1$.

2° Lorsqu'il existe un diviseur de degré 1 dans l'ensemble $\{P_0 , \dots , P_{t-1}\}$, le groupe des classes d'idéaux de B est isomorphe à

$$\mathbb{O}_0/\mathcal{P} + \mathfrak{m}_0 \cong (\mathbb{O}_0/\mathcal{P})/(\mathcal{P} + \mathfrak{m}_0/\mathcal{P}) ,$$

c'est donc un quotient de la jacobienne de E.

Preuve.

1° En effet $\mathfrak{m}_0$ est libre, de rang $t - 1$.

2° Supposons que degré $(P_0) = 1$, alors on peut écrire que

$$C = \pi_2(C_1) , \text{ avec } C_1 = C - \deg(C)\, P_0 \in \mathfrak{m}_0$$

$$D = \pi_2(D_1) , \text{ avec } D_1 = D - \deg(D)\, P_0 \in \mathfrak{m}_0 .$$

Par suite, l'équivalence de C et de D s'écrit

$$\pi_2[D_1 - C_1 - \mathrm{div}(\varphi)] = 0 ,$$

soit encore

$$D_1 \equiv C_1 + \mathrm{div}(\varphi) \ \mathrm{mod}(\mathfrak{m}_0) .$$

Le groupe des classes d'idéaux de B est donc isomorphe à $\mathfrak{O}_0/\mathcal{P} + \mathfrak{m}_0$.

Nous appellerons "partie à l'infini" de la jacobienne J de E le groupe quotient

$$J_\infty = \mathfrak{m}_0/\mathfrak{m}_0 \cap \mathcal{P} .$$

COROLLAIRE 2.

1° Soit T le sous-groupe de torsion de J , on a la relation

$$\mathrm{rang}(J_\infty/T) + \mathrm{rang}(\mathcal{G}) = t - 1 .$$

2° Lorsqu'il existe un diviseur de degré 1 dans l'ensemble $\{P_0 , \dots , P_{t-1}\}$, le groupe des classes d'idéaux de B est isomorphe à J/J_∞ .

Preuve.

1° On sait qu'il existe une base $u_1 , \dots , u_{t-1}$ de $\mathfrak{m}_0$ et des entiers non nuls $d_1 , \dots , d_s$, avec $d_1 | d_2 | \dots | d_s$ tels que $d_1 u_1 , \dots , d_s u_s$ soit une base de $\mathfrak{m}_0 \cap \mathcal{P}$.

alors

$$\mathfrak{m}_0/\mathfrak{m}_0 \cap \mathcal{P} \cong Z/d_1 \oplus \dots \oplus Z/d_s Z \oplus Z^{t-1-s} .$$

Donc

$$\begin{aligned} \mathrm{rang}(J_\infty/T) &= t - 1 - s \\ &= t - 1 - \mathrm{rang}(\mathfrak{m}_0 \cap \mathcal{P}) \\ &= t - 1 - \mathrm{rang}(\mathcal{G}) . \end{aligned}$$

2° Il suffit de transcrire la seconde partie du corollaire 1 en tenant compte de l'isomorphisme

$$(\mathcal{P} + \mathfrak{m}_0)/\mathcal{P} \cong \mathfrak{m}_0(\mathfrak{m}_0 \cap \mathcal{P}) .$$

Exemple. - On suppose que $E = K(Y)$ avec $Y^p = D(X) \in A$, où $D(X)$ est un polynôme dont le degré est premier avec p .

On voit facilement que P_∞ se ramifie dans E , et que son indice de ramification est égal à p .

Il en résulte que $t = 1$ et que le degré de P_0 est égal à 1 . Ainsi $\mathfrak{m} = Z P_0$, $\mathfrak{m}_0 = \{0\}$ et $J_\infty = \{0\}$.

Le corollaire montre donc que :

1° $\mathrm{rang}(\mathcal{G}) = 0$.

2° Le groupe des classes d'idéaux de B est isomorphe à J .

COROLLAIRE 3. - Lorsque k est un corps fini, $\mathcal{S}$ est un groupe abélien libre de rang $t - 1$.

Preuve. - J est l'ensemble des "points rationnels" d'une variété algébrique définie sur k [L]. Donc J est fini.

3. Connas (de E relativement à X , dans les corps de nombres algébriques).

On dira que $\varphi \in B \setminus \{0\}$ est un "conna de E relativement à X " ou une "meilleure approximation dans B ", si φ vérifie

$$(\forall\, \varphi' \in B \setminus \{0\}\ ,\ v_{p_i}(\varphi') \geq v_{p_i}(\varphi) \quad \text{pour} \quad i = 0\ ,\ \dots\ ,\ t-1)$$

$$\Longrightarrow (\exists\, \lambda \in k^*\ ,\ \varphi' = \lambda\varphi)\ .$$

PROPRIÉTÉ. - Toute unité de B est un conna de E relativement à X .

Preuve. - Soit $\varphi \in \mathcal{U}(B)$, si φ n'est pas un conna de E , il existe $\varphi' \in B \setminus \{0\}$ et il existe une place P tels que

$$\begin{cases} v_{p_i}(\varphi') \geq v_{p_i}(\varphi)\ , \text{ pour } i = 0\ ,\ \cdots\ ,\ T-1 \\ v_p(\varphi') > v_p(\varphi) \end{cases}$$

et posons

$$D_1 = [v_p(\varphi) - v_p(\varphi')]\, P - \operatorname{div}(\varphi)\ .$$

Alors $\varphi' \in L(-D_1)$, mais comme $\deg(D_1) < 0$, le théorème de Riemann-Roch entraîne que $\ell(-D_1) = 0$, donc $\varphi' = 0$, ce qui est absurde.

Mais on doit noter qu'en général un conna φ n'est pas dans $\mathcal{U}(B)$. On considère alors les applications

$$\varphi \in B \longmapsto \operatorname{div}(\varphi) \begin{cases} \xrightarrow{\pi_1} \operatorname{div}_1(\varphi) \in \mathfrak{n} \\ \xrightarrow{\pi_2} \operatorname{div}_2(\varphi) \in \mathfrak{n}\ . \end{cases}$$

Si $\varphi \in B \setminus \mathcal{U}(B)$, $\operatorname{div}_1(\varphi) \notin \mathfrak{n}_0$ et $\operatorname{div}_2(\varphi) > 0$. Lorsqu'il existe un diviseur premier P à l'infini de degré 1 , on peut considérer :

$$D_2(\varphi) = \operatorname{div}_2(\varphi) - \deg[\operatorname{div}_2(\varphi)]\, P \in \mathfrak{D}_0$$

et son "fantôme"

$$D_1(\varphi) = \operatorname{div}_1(\varphi) + \deg[\operatorname{div}_2(\varphi)]\, P \in \mathfrak{n}_0\ .$$

Lorsque $t = 2$, on voit que l'existence d'unités non triviales dans B équivaut à dire que $D_2(\varphi)$ (ou son "fantôme") sont d'ordre fini sur J .

THÉORÈME 4. - Si φ est un comma de E relativement à X, le degré du polynôme $\pi(\varphi) \in A$ est inférieur ou égal au genre de E.

Preuve.

1° Si nous posons $D_1 = \mathrm{div}_1(\varphi)$, la condition pour que φ soit un comma s'écrit

$$\ell(D_1) = 1 .$$

Mais le théorème de Riemann [D] nous donne

$$\ell(D_1) + d(D_1) \geq 1 - g ,$$

donc

$$d(D_1) \geq - g .$$

2° Si nous posons maintenant

$$D_2 = \mathrm{div}_2(\varphi) ,$$

alors nous avons

$$\deg(D_1) + \deg(D_2) = 0$$

donc

$$\deg D_2 \leq g .$$

3° Mais, d'après [D] (page 110),

$$\deg_K(\mathfrak{N}_{E/K} D_2) = \deg_E(D_2)$$

ce qui, dans nos notations, donne

$$\deg_K[\pi(\varphi)] = \deg D_2 ,$$

et finalement

$$\deg_K[\pi(\varphi)] \leq g .$$

Commas dans les corps de nombres.

Soit un corps de nombres algébriques E. On désigne par B l'anneau des entiers de E et par $P_0 , \ldots , P_{t-1}$ les valeurs absolues "archinédiennes" de E [C].

Définition. - Soit $x \in B \setminus \{0\}$. On dira que x est un comma de E si, et seulement si, quel que soit $y \in B \setminus \{0\}$, les conditions

$$|y|_{p_i} \leq |x|_{p_i} \quad \text{pour} \quad i = 0 , \ldots , t - 1$$

entraînent que $y = \zeta x$, où ζ est une racine de l'unité dans E.

PROPRIÉTÉ. - Toute unité de B est un comma de E.

Preuve. - On utilisera la formule du produit [C]. Puisque $x \in \mathfrak{U}(B)$, on sait que, pour toute valeur absolue non-archinédienne P,

$$|x|_p = 1$$

Donc la formule du produit entraîne que

$$\prod_{i=0}^{t-1} |x|_{p_i} = 1 .$$

D'après nos conditions, nous avons

$$\prod_{i=0}^{t-1} |y|_{p_i} \leqslant 1 .$$

Mais puisque $y \in B$, nous avons, pour toute valeur absolue non-archimédienne P :

$$|y|_p \leqslant 1 .$$

Donc la formule du produit entraîne que l'on a $|y|_p = |x|_p$ pour <u>toute</u> valeur absolue P .

Donc si l'on pose $\zeta = \frac{y}{x}$, on a

$$\zeta \in \mathcal{U}(B) \quad \text{et} \quad |\zeta|_{p_i} = 1 , \quad i = 0 , \ldots , t - 1 .$$

Il en résulte que ζ est une racine de l'unité [C] ([1]).

PROBLÈME. - <u>Est-ce que les corps de</u> $E = K(\Delta)$ <u>se spécialisent en corps de</u> $\mathbb{Q}(\sqrt[3]{D(x_0)})$ <u>lorsque l'on spécialise</u> X <u>en</u> x_0 ?

4. <u>Rang du groupe</u> $\mathcal{S}(\mathcal{O})$.

Considérons maintenant un ordre $\mathcal{O}$ de E relativement à X , nous nous proposons de généraliser à $\mathcal{U}(\mathcal{O})$ le résultat du théorème 2. Nous noterons par $\mathcal{E}$ le monoïde commutatif des diviseurs des éléments de $\mathcal{O}$, soit encore $\mathcal{E} = L(\mathcal{O})$ où l'on pose, comme plus haut, $L(\varphi) = \mathrm{div}(\varphi)$. On peut remarquer que le symétrisé de $\mathcal{E}$ est $\mathcal{P}$.

THÉORÈME 3. - $\mathcal{S}(\mathcal{O}) := \mathcal{U}(\mathcal{O})/k^*$ <u>est un sous-groupe de</u> $\mathcal{S}$ <u>qui est isomorphe à</u> $\mathfrak{m}_0 \cap \mathcal{E}$. <u>Son rang est encore majoré par</u> $t - 1$.

<u>Preuve</u>. - Nous allons encore démontrer que

$$L : \mathcal{U}(\mathcal{O}) \longrightarrow \mathfrak{m}_0 \cap \mathcal{E}$$

est surjective.

Tout diviseur de $\mathfrak{m}_0 \cap \mathcal{E}$ est de la forme $\mathrm{div}(\varphi)$, avec $\varphi \in \mathcal{O}$. Comme $\mathrm{div}(\varphi) \in \mathfrak{m}$, le lemme 4 entraîne que $\varphi \in \mathcal{U}(B)$.

Il en résulte que $\varphi \in \mathcal{O} \cap \mathcal{U}(B) = \mathcal{U}(\mathcal{O})$ d'après le lemme 3.

COROLLAIRE 4. - <u>Soit</u> $T(\mathcal{O})$ <u>le sous-groupe de torsion de</u> $J_\infty(\mathcal{O}) := \mathfrak{m}_0/\mathfrak{m}_0 \cap \mathcal{E}$ <u>on a la relation</u>

$$\mathrm{rang}(J_\infty(\mathcal{O})/T) + \mathrm{rang}\ \mathcal{S}(\mathcal{O}) = t - 1 .$$

<u>Remarque.</u> - Dans certains cas $\mathrm{rang}\ \mathcal{S}(\mathcal{O}) < \mathrm{rang}\ \mathcal{S}(B)$, donc $\mathrm{rang}(J_\infty(\mathcal{O})/T) > \mathrm{rang}\ J_\infty/T$.

([1]) Cette démonstration s'applique également aux corps de fonctions algébriques puisque la formule du produit est valable.

RÉFÉRENCES

[B] BOURBAKI (N.). - Eléments de mathématiques. Algèbre commutative. Ch. 6 : Valuations. - Paris, Hermann, 1964 (Actualités scientifiques et industrielles 1308 ; Bourbaki 30).

[C] CASSELS (J. W. S.) [Ed.]. - Algebraic number theory. Proceedings of an instructural conference [1965. Brighton]. - London and New York, Academic Press, 1967.

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

[L] LANG (S.). - Abelian varieties. - New York, London, Interscience Publishers, 1959 (Interscience Tracts in pure and applied Mathematics, 7).