

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
(Secrétariat mathématique, Paris), 1984-1985, tous droits réservés.

L'accès aux archives de la collection « Groupe d'étude en théorie analytique des nombres » 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/>

X-UNITÉS DE CERTAINS CORPS DE FONCTIONS ALGÈBRIQUES, II

par Yves HELLEGOUARCH (*)

1. Rappel du point de départ du premier exposé.

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

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

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

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

que nous avons 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.

THÉOREME 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 $\varphi \in B$, $\varphi \in \mathcal{U}(B)$ équivalent 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 $\pi_{E/K}(\varphi) = \varphi \cdot \rho$ 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 $\mathbb{Q}((\frac{1}{X}))$ l'application qui à

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

fait correspondre

$$\begin{aligned} \infty & \text{ si } n_0 > 0, \\ a_0 & \text{ si } n_0 = 0 \end{aligned}$$

et

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

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

$$\begin{array}{c} \mathbb{Q}((\frac{1}{X})) \\ \downarrow \\ E = K(\Delta) \\ \downarrow \\ K = \mathbb{Q}(X) \end{array}$$

les restrictions P_0 et p_∞ 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 p_∞ de degré 1.

p_∞ 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 p_∞ 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 p_∞ , nous désignerons ces places par $P_0, \dots, P_{t-1}$.

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 $P_0, \dots, P_{t-1}$.

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

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

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

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

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

Montrons que (b) $\Rightarrow$ (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

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

ce qui entraîne que

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

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 $\mathfrak{n}$ 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 $\mathfrak{n} = M \cap A[\varphi^{-1}]$.

(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), $P \in \{P_1, \dots, P_t\}$, 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 $\varphi \cdot \psi = 1$ avec $\psi \in B$. Si $\varphi \notin \mathcal{U}(\mathcal{O})$, il existe un idéal maximal $\mathfrak{n}$ tel que $\varphi \in \mathfrak{n}$.

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

(V, 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 $P \in \{P_1, \dots, P_t\}$.

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

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

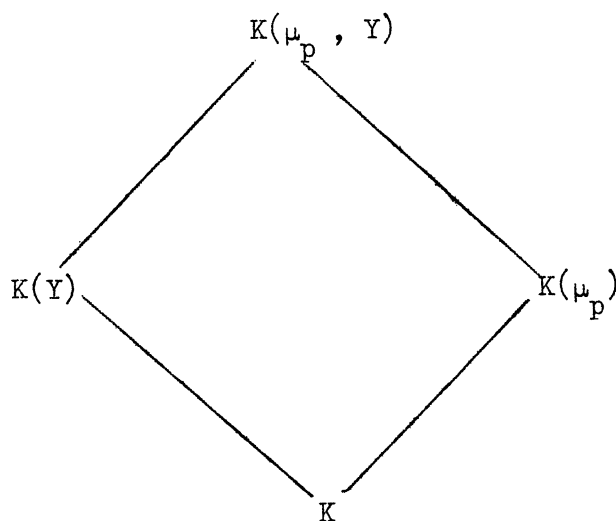
Dans toute la suite, $\bar{k}$ sera fixée, et μ_p désignera le groupe des racines p -ièmes de l'unité dans $\bar{k}$. Rappelons le résultat suivant.

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°

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

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

$$2^{\circ} \quad \text{Gal } K(\mu_p, Y)/K(\mu_p) \cong \mathbb{Z}/p\mathbb{Z}$$

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

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

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

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

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

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

On dira que $F(X)$ est unitaire lorsque $t(F) = 1$

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

Preuve. - $D(X) = X^{pn} [1 + \frac{1}{X} R(\frac{1}{X})]$, 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

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

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).

THÉOREME 2. - On suppose l'hypothèse faible vérifiée. On met D sous la forme $Q_1^{\alpha_1} \dots Q_s^{\alpha_s} F$, où $Q_1, \dots, Q_s$ sont des polynômes irréductibles distincts sur $k(X)$ avec $\alpha_j \geq 2$ pour $1 \leq j \leq s$ et $(Q_j, F) = 1$ pour $1 \leq j \leq s$.

On suppose, de plus, F sans racine multiple dans $\bar{k}$ et les α_j premiers avec p pour $1 \leq j \leq s$.

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

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

où les polynômes U_i appartiennent à A et vérifient la condition

$$\forall i, \forall j, Q_j^{\alpha_j - j} \mid U_i \quad \text{où } j = [\frac{ip}{\alpha_j}].$$

On a, toujours d'après le lemme 2,

$$f \in B \iff v_{q_\lambda}(\varphi) \geq \beta_\lambda \text{ pour } 1 \leq \lambda \leq s,$$

où q_λ est le diviseur premier de $k(X, Y)$ au-dessus de Q_λ et v_{q_λ} la valuation associée à q_λ et telle que $v_{q_\lambda}(Q_\lambda) = 1$, on a alors $v_{q_\lambda}(q_\lambda) = \frac{\lambda_1}{p}$ car on a supposé $(\alpha_\lambda, p) = 1$ pour $1 \leq \lambda \leq s$.

Désignons par q un q_λ , α un α_λ , β un β_λ , on a

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

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

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

et donc

$$v_q(\varphi) \geq \beta \iff Q^\beta | U_i, \quad 0 \leq i < \frac{p}{\alpha}, \quad Q^{\beta-1} | U_i, \quad \frac{p}{\alpha} \leq i < \frac{2p}{\alpha}, \dots$$

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

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

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

2. Décomposition du groupe des diviseurs en somme directe.

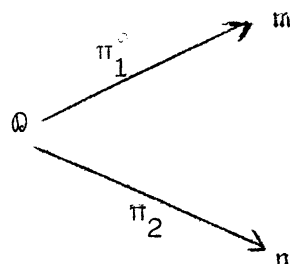
Nous désignerons par $\mathcal{O}$ le groupe des diviseurs de E , c'est $\mathcal{O} = \coprod_P \mathbb{Z} P$, où P décrit l'ensemble des places (non équivalentes) de E . Si l'on pose

$$m = \mathbb{Z} P_0 \oplus \dots \oplus \mathbb{Z} P_{t-1},$$

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

Il est clair que $\mathcal{O} = m \oplus n$.

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 $j \circ \pi_2[\text{div}(\varphi)]$ est l'idéal fractionnaire de B engendré par φ .

$$3^\circ \text{Ker}(j \circ \pi_2 \circ \text{div}) = \mathcal{U}(B) .$$

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 $v_P(\pi_1) \geq 2$, 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 $\varphi \notin \{P_0, \dots, P_{t-1}\}$, $v_P(\varphi) = n$ équivaut à dire que $[j(P)]^n$ divise exactement φB .

La troisième partie résulte du lemme 2.

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

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

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

THÉOREME 3.

$$1^\circ \quad \mathfrak{S} \cong \mathfrak{m}_0 \cap \mathcal{P}.$$

$$2^\circ \quad \text{Le groupe des classes d'idéaux de } B \text{ est isomorphe à } \pi/\pi_2(\mathcal{P}).$$

Preuve.

1° Nous considérons l'homomorphisme :

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

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

$$(1) \quad \text{Im } L \cong \mathcal{U}(B)/\text{Ker } L \cong \mathfrak{S}(B) .$$

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

$$(2) \quad J = I \cdot (\varphi B) .$$

D'après la proposition 1, il existe des diviseurs C et D dans n tels que

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

et la relation (2) équivaut à

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

COROLLAIRE 1.

$$1^\circ \quad \mathfrak{S} \text{ est libre et son rang est majoré par } t - 1 .$$

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

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

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

Preuve.

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

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

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

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

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

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

soit encore

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

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

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

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

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

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

Donc

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

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 $\mathfrak{m} = \mathbb{Z} P_0$, $\mathfrak{m}_0 = \{0\}$ et $J_\infty = \{0\}$.

Le corollaire montre donc que :

1° $\text{rang}(\mathcal{G}) = 0$.

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

COROLLAIRE 3. - Lorsque k est un corps fini, $\mathfrak{g}$ 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

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

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

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

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

et posons

$$D_1 = [v_P(\varphi) - v_P(\varphi')] P - \text{div}(\varphi) .$$

Alors $\varphi' \in L(-D_1)$, mais comme $\deg(D_1) < 0$, le théorème de Riemann-Roch entraîne que $L(-D_1) = 0$, 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

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

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

$$D_2(\varphi) = \text{div}_2(\varphi) - \deg[\text{div}_2(\varphi)] P \in \mathcal{O}_0$$

et son "fantôme"

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

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 .

THÉOREME 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 $D_1 = \text{div}_1(\varphi)$, 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

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

alors nous avons

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

donc

$$\deg D_2 \leq g .$$

3° Mais, d'après [D] (page 110),

$$\deg_K(\pi_{E/K} D_2) = \deg_E(D_2)$$

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 $P_0, \dots, P_{t-1}$ les valeurs absolues "archimédiennes" 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

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

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 $x \in \mathcal{U}(B)$, on sait que, pour toute valeur absolue non-archimédienne 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

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

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

$$|y|_P \leq 1 .$$

Donc la formule du produit entraîne que l'on a $|y|_P = |x|_P$ pour toute valeur absolue P .

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

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

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

PROBLÈME. - Est-ce que les conmas de $E = K(\Delta)$ se spécialisent en conmas de $\mathbb{Q}(\sqrt[t]{D(x_0)})$ lorsque l'on spécialise X en x_0 ?

4. Rang du groupe $\mathcal{G}(\mathcal{O})$.

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, $L(\varphi) = \text{div}(\varphi)$. On peut remarquer que le synétrisé de $\mathcal{E}$ est $\mathcal{P}$.

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

Preuve. - Nous allons encore démontrer que

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

est surjective.

Tout diviseur de $\mathcal{P}_0 \cap \mathcal{E}$ est de la forme $\text{div}(\varphi)$, avec $\varphi \in \mathcal{O}$. Comme $\text{div}(\varphi) \in \mathcal{M}$, 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. - Soit $T(\mathcal{O})$ le sous-groupe de torsion de $J_\infty(\mathcal{O}) := \mathcal{P}_0 / \mathcal{P}_0 \cap \mathcal{E}$ on a la relation

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

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

⁽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 instructional conference [1965. Brighton].* - London and New York, Academic Press, 1967.
 - [D] DEURING (H.). - *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).
-