References

[1] N. G. De Bruijn, *On the number of positive integers $\leqslant x$ and free of prime factors $> y$*, Nederl. Akad. Wetensch. Proc. Ser. A 54 (= Indag. Math.) 13(1951), pp. 50–60.

[2] J. M. De Koninck and A. Ivić, *Topics in Arithmetical Functions*, Notas de Mathematica 72, North-Holland, Amsterdam 1980.

[3] J. M. De Koninck and J. Galambos, *Sums of reciprocals of additive functions*, Acta Arith. 25(1974), pp. 159–164.

[4] A. Ivić, *Sums of reciprocals of the largest prime factor of an integer*, Arch. Math. 36(1981), pp. 57–61.

[5] G. J. Rieger, *On two arithmetic sums*, (Abstract) Notices Amer, Math. Soc. 74T–A177.

[6] — *Zahlentheorie*, Vanderhoeck and Ruprecht, Göttingen 1976.

[7] R. L. Robinson, *An estimate for the enumerative functions of certain sets of integers*, Proc. Amer. Math. Soc. 17(1966), pp. 232–237; Correction, ibid, 17(1966), p. 1473.

DÉPARTEMENT DE MATHÉMATIQUES
UNIVERSITÉ LAVAL
Québec, G1K 7P4
Canada

DEPARTMENT OF MATHEMATICS
THE UNIVERSITY OF TOLEDO
Toledo, Ohio 43606
U.S.A.

Received on 7. 5. 1984
and in revised form on 28. 8. 1985 (1424)

ACTA ARITHMETICA
XLVIII(1987)

Unités de certains sous-anneaux des corps de fonctions algébriques

par

Y. Hellegouarch, D. L. McQuillan et
R. Paysant-Le Roux (Caen)

Introduction. Cette étude est le résultat d'un travail qui s'est développé au sein de l'équipe d'Algèbre et de Théorie des Nombres de Caen à la suite d'une visite du Professeur A. Schinzel en 1981.

Au départ, ce travail était centré sur l'algorithme des fractions continues et les méthodes utilisées s'inspiraient de celles de Schinzel [12] et d'Artin [1].

Une première étude [7] résumait les résultats obtenus, résultats plus généraux pour la partie géométrique, que pour la partie algorithmique. La partie géométrique traitait le cas des extensions $E = k(X, \sqrt[p]{D(X)})$ avec p quelconque > 0 et la partie algorithmique, qui utilisait les fractions continues, était limitée au cas $p = 2$.

Dans une seconde étape [11], Roger Paysant-Le Roux généralisait les résultats de [7] à l'aide d'une notion de meilleure approximation semblable à celle utilisée par E. Dubois et G. Rhin [6] dans le cas des corps de nombres. L'algorithme des meilleures approximations était utilisé pour remplacer celui des fractions continues. Il peut aussi être comparé aux algorithmes de J. H. Davenport [4].

Puis D. L. Mc Quillan, lors d'une visite à Caen, donnait une forme plus générale aux résultats qu'Yves Hellegouarch avait obtenus en utilisant le langage de la théorie des corps de fonctions algébriques [5].

Finalement, une étude axiomatique des notions d'approximation utilisées nous conduisait à réviser notre vocabulaire et à introduire différentes notions: commas, points extrémaux, arêtes qui sont définies de manière simple aussi bien dans les corps de nombres que dans les corps de fonctions pour lesquels on a choisi un élément X non constant [8].

Tel qu'il est composé ici, ce travail est essentiellement algébrique et se réfère aux ouvrages classiques de Deuring [5] et d'Artin [2]. Nous avons donc utilisé les notations de Deuring, qui, c'est regrettable, ne sont pas d'un usage universel. Que le lecteur habitué à d'autres notations veuille bien nous en excuser!

Ce travail reste à la lisière des applications arithmétiques qui avaient été à la base des travaux de Schmidt [13], Schinzel [12], Neubrand [9] et [10], Stender [14], etc...

Sans s'engager dans cette voie, qui exigerait de nouvelles méthodes et déborderait le cadre qu'on s'est fixé, nous mentionnerons cependant, dans le dernier paragraphe, quelques faits qui invitent à se poser des questions nouvelles.

1. Étude algébrique du cas général

1.1. Equation de Pell généralisée. 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 $\mathcal{N}_{E/K}$. 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 $\mathcal{N}_{E/K}\varphi \in k^*$ et $\varphi \in \mathcal{O}$.*

Remarque. Nous dirons que la seconde condition est une "equation 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 $\mathcal{N}_{E/K}\varphi \in k^*$.*

Preuve. 1. Soit $\varphi \in \mathcal{U}(B)$, alors il existe $\psi \in B$ tel que

$$\varphi\psi = 1.$$

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

En prenant la norme, on en déduit que:

$$\mathcal{N}_{E/K}\varphi \cdot \mathcal{N}_{E/K}\psi = 1.$$

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

2. Réciproquement, soit $\varphi \in B$ tel que $\mathcal{N}_{E/K}\varphi \in k^*$. Alors $\mathcal{N}_{E/K}\varphi = \varphi \cdot \varrho$ où ϱ est un entier sur A.

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

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

Alors on sait [5] que E ne possède qu'un nombre fini de places au-dessus de $\mathfrak{p}_\infty$, nous désignerons ces places par $P_1, \ldots, P_t$.

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 $P_1, \ldots, P_t$.*

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

$$\varphi^n + a_1\varphi^{n-1} + \ldots + a_n = 0$$

avec $a_i \in A$.

Supposons que $P(\varphi) = \infty$, alors $P(1/\varphi) = 0$. Mais on a:

$$1 + a_1(1/\varphi) + \ldots + a_n(1/\varphi)^n = 0$$

et si $P \neq P_i$, pour $i \in \{1, \ldots, t\}$, 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:

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

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 m de $A[\varphi^{-1}]$. D'après un résultat général [17] il existe un anneau de valuation (V, M) tel que $V \supset A[\varphi^{-1}]$ et $m = M \cap A[\varphi^{-1}]$.

(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 m tel que $\varphi \in m$.

D'après un résultat général [17] il existe un anneau de valuation (V, M) tel que $V \supset \mathcal{O}$ et $m = M \cap \mathcal{O}$.

(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 $P \in \{P_1, \ldots, P_t\}$.

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

1.2. Décomposition du groupe des diviseurs en somme directe. Nous désignerons par $\mathcal{D}$ le groupe des diviseurs de E, c'est:

$$\mathcal{D} = \coprod_P \mathbf{Z}P$$

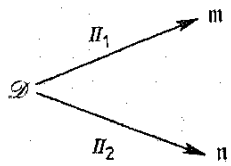
où P décrit l'ensemble des places (non équivalentes) de E. Si l'on pose:

$$\mathfrak{m} = \mathbf{Z}P_1 \oplus \ldots \oplus \mathbf{Z}P_t, \qquad \mathfrak{n} = \coprod_{\substack{P \neq P_i \\ i=1,\ldots,t}} \mathbf{Z}P.$$

Il est clair que:

$$\mathcal{D} = \mathfrak{m} \oplus \mathfrak{n}.$$

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 $\mathfrak{n}$ sur le groupe des idéaux fractionnaires de B qui envoie une place P de E sur l'idéal premier $j(P) = \{\varphi \in B \mid P(\varphi) = 0\}$.*

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. $\mathrm{Ker}(j \circ \Pi_2 \circ \mathrm{div}) = \mathcal{U}(B)$.

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

LEMME 4. *Soit $\varphi \in B \setminus \{0\}$ et P une place $\notin \{P_1, \ldots, P_t\}$. Alors pour tout $n \in \mathbf{N}$ on a l'équivalence:*

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

Preuve. Cette preuve utilise principalement le fait que la valuation associée à P est discrète [5].

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:

$$\pi = \frac{\pi_1}{u_3} \quad \text{et} \quad \varphi = \frac{u_1}{u_2}\left(\frac{\pi_1}{u_3}\right)^n$$

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:

$$[j(P)]^{n+1} \text{ divise } (\pi_1 B)^n$$

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 $P \notin \{P_1, \ldots, P_t\}$:

$$v_P(\varphi) = n$$

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 $\{P_1, \ldots, P_t\}$. Il en résulte que $\mathrm{div}(\varphi) \in \mathfrak{m}$ et $\Pi_2[\mathrm{div}(\varphi)] = 0$.

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

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

THÉORÈME 2. 1. $\mathcal{G} = \mathfrak{m}_0 \cap \mathcal{P}$.

2. *Le groupe des classes d'idéaux de B est isomorphe à $\mathfrak{n}/\Pi_2(\mathcal{P})$.*

Preuve. 1. Nous considérons l'homomorphisme:

$$L \begin{cases} \mathscr{U}(B) \to \mathfrak{m}_0 \cap \mathscr{P}, \\ \varphi \mapsto \operatorname{div}(\varphi). \end{cases}$$

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

$$\operatorname{Im} L = \mathscr{U}(B)/\operatorname{Ker} L \cong \mathscr{G}(B). \tag{1}$$

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" ssi il existe $\varphi \in B \setminus \{0\}$ telle que:

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

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. *$\mathscr{G}$ est libre et son rang est majoré par $t-1$.*

2. *Lorsqu'il existe un diviseur de degré 1 dans l'ensemble $\{P_1, \ldots, P_t\}$ le groupe des classes d'idéaux de B est isomorphe à:*

$$\mathscr{D}_0/\mathscr{P} + \mathfrak{m}_0 \cong (\mathscr{D}_0/\mathscr{P})/(\mathscr{P} + \mathfrak{m}_0/\mathscr{P})$$

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$(P_1) = 1$, alors on peut écrire que:

$$C = \Pi_2(C_1), \quad \text{avec} \quad C_1 = C - \deg(C) P_1 \in \mathfrak{m}_0,$$

$$D = \Pi_2(D_1), \quad \text{avec} \quad D_1 = D - \deg(D) P_1 \in \mathfrak{m}_0.$$

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

$$\Pi_2[D_1 - C_1 - \operatorname{div}(\varphi)] = 0$$

soit encore:

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

Le groupe des classes d'idéaux de B est donc isomorphe à:

$$\mathscr{D}_0/\mathscr{P} + \mathfrak{m}_0.$$

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

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

Corollaire 2. 1. *Soit T le sous-groupe de torsion de J, on a la relation:*

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

2. *Lorsqu'il existe un diviseur de degré 1 dans l'ensemble $\{P_1, \ldots, P_t\}$ le groupe des classes d'idéaux de B est isomorphe à J/J_∞.*

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

Alors:

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

Donc:

$$\operatorname{rang}(J_\infty/T) = t - 1 - s = t - 1 - \operatorname{rang}(\mathfrak{m}_0 \cap \mathscr{P}) = t - 1 - \operatorname{rang}(\mathscr{G}).$$

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

$$\mathscr{P} + \mathfrak{m}_0/\mathscr{P} \cong \mathfrak{m}_0/\mathfrak{m}_0 \cap \mathscr{P}.$$

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 [5] que $t = 1$ et que le degré de P_1 est égal à 1.

Ainsi $\mathfrak{m} = \mathbf{Z}P_1$, $\mathfrak{m}_0 = \{0\}$ et $J_\infty = \{0\}$.

Le corollaire montre donc que:

1. $\operatorname{rang}(\mathscr{G}) = 0$,
2. le groupe des classes d'idéaux de B est isomorphe à J.

Corollaire 3. *Lorsque k est un corps fini, $\mathscr{G}$ est un groupe abélien libre de rang $t-1$.*

Preuve. J est l'ensemble des "points rationnels" d'une variété algébrique définie sur k, donc J est fini [17].

1.3. Groupe des unités d'un ordre. Considérons maintenant un ordre $\mathscr{O}$ de E relativement à X, nous nous proposons de généraliser à $\mathscr{U}(\mathscr{O})$ le résultat du théorème 2. Nous noterons par $\mathscr{E}$ le monoïde commutatif des diviseurs des éléments de $\mathscr{O}$, soit encore:

$$\mathscr{E} = L(\mathscr{O})$$

où l'on pose comme plus haut $L(\varphi) = \operatorname{div}(\varphi)$. On peut remarquer que le symétrisé de $\mathscr{E}$ est $\mathscr{P}$.

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

Preuve. Nous allons encore démontrer que

$$L: \mathscr{U}(\mathscr{O}) \to \mathfrak{m}_0 \cap \mathscr{E}$$

est surjective.

Tout diviseur de $\mathfrak{m}_0 \cap \mathscr{E}$ est de la forme $\operatorname{div}(\varphi)$, avec $\varphi \in \mathscr{O}$.

Comme $\operatorname{div}(\varphi) \in \mathfrak{m}$, le lemme 2 entraîne que $\varphi \in \mathscr{U}(B)$.

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

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

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

Remarque. Dans certains cas $\operatorname{rang} \mathscr{G}(\mathscr{O}) < \operatorname{rang} \mathscr{G}(B)$, donc

$$\operatorname{rang}(J_\infty(\mathscr{O})/T) > \operatorname{rang} J_\infty/T.$$

1.4. Commas, points extrémaux et arêtes. Dans ce paragraphe E désignera soit un corps de fonctions algébriques d'une variable, soit un corps de nombres algébriques.

Dans le premier cas on se donnera $X \in E \setminus k$ et on désignera par S l'ensemble des places à l'infini $P_1, \ldots, P_t$, dans le second cas S sera l'ensemble des valeurs absolues archimédiennes de E.

Dans les deux cas, on sait que la formule du produit [2] est valable dans E et que l'anneau des entiers de E (ou des X-entiers de E) est:

$$B = \{x \in E \mid |x|_P \leqslant 1, \ \forall P \notin S\}.$$

On posera:

$$k^* = \{x \in E \mid |x|_P = 1, \ \forall P\}.$$

C'est le groupe multiplicatif des constantes de E (dans le premier cas) ou le groupe des racines de l'unité.

DÉFINITION. On dira que $\varphi \in B \setminus \{0\}$ est un *comma* de E (relativement à X si E est un corps de fonctions algébriques) resp. un *point extrémal* de E, une *arête* de E si les conditions:

$$(\varphi' \in B \setminus \{0\}, \ |\varphi'|_P \leqslant |\varphi|_P, \text{ pour tout } P \in S)$$

entraînent:

$$\exists \lambda \in k^*, \quad \varphi' = \lambda \varphi$$

resp. $|\varphi'|_P = |\varphi|_P$ pour tout $P \in S$, il existe $P \in S$ tel que $|\varphi'|_P = |\varphi|_P$. Voir [8].

On désignera par $\mathscr{U}$ le groupe des unités de B, $\mathscr{C}$ l'ensemble des commas de E, $\mathscr{E}$ l'ensemble des points extrémaux et $\mathscr{A}$ l'ensemble des arêtes. Il est clair que:

$$\mathscr{C} \subset \mathscr{E} \subset \mathscr{A}.$$

PROPOSITION 2. *Toute unité est un comma.*

Preuve. Soit $\varphi \in \mathscr{U}$ et $\varphi' \in B \setminus \{0\}$, on suppose que pour tout $P \in S$, on a:

$$|\varphi'|_P \leqslant |\varphi|_P$$

et on veut en déduire que pour toute place P:

$$|\varphi'|_P = |\varphi|_P.$$

Puisque $\varphi \in \mathscr{U}$, on a $|\varphi|_P = 1$ pour tout $P \notin S$.

La formule du produit (appliquée à φ) entraîne donc que:

$$\prod_{P \in S} |\varphi'|_P \leqslant \prod_{P \in S} |\varphi|_P = 1.$$

Mais puisque $\varphi' \in B \setminus \{0\}$, la formule du produit (appliquée à φ') entraîne que:

$$\prod_{P \in S} |\varphi'|_P \geqslant 1.$$

On en déduit que:

$$\prod_{P \in S} |\varphi'|_P = 1$$

donc que $|\varphi'|_P = |\varphi|_P$ pour $P \in S$.

Maintenant si $P \notin S$, on a $|\varphi'|_P = 1 = |\varphi|_P$ car

$$\prod_{P \notin S} |\varphi'|_P = 1.$$

PROPOSITION 3. *Si $u \in \mathscr{U}$ et $\varphi \in \mathscr{C}$ (resp. $\varphi \in \mathscr{E}$, $\varphi \in \mathscr{A}$) alors $u\varphi \in \mathscr{C}$ (resp. $u\varphi \in \mathscr{E}$, $u\varphi \in \mathscr{A}$).*

Preuve. Les conditions $|\varphi'|_P \leqslant |u\varphi|_P$ et $|u^{-1}\varphi'|_P \leqslant |\varphi|_P$ sont équivalentes. Il en résulte que $\mathscr{U}$ opère sur $\mathscr{C}$ (resp. $\mathscr{E}$, $\mathscr{A}$) et, en particulier, $\mathscr{U}$ est l'orbite de 1. On désignera par

$$[\mathscr{C}: \mathscr{U}] \quad (\text{resp. } [\mathscr{E}: \mathscr{U}], \ [\mathscr{A}: \mathscr{U}])$$

le nombre d'orbites de $\mathscr{C}$ (res. $\mathscr{E}$, $\mathscr{A}$) modulo $\mathscr{U}$. Notre but est d'établir un rapport entre $\mathscr{E}: \mathscr{U}$ et le rang du groupe $\mathscr{U}$, mais avant d'en arriver là nous allons démontrer un certain nombre de propriétés générales.

PROPOSITION 4. *On suppose que E est un corps de fonctions algébriques de genre g et on pose*:

$$h = \inf\{\deg P, \ P \in S\}, \qquad e = \sum_{P \in S} \deg P.$$

1. *Si $\varphi \in \mathscr{C}$, on a*:

$$0 \leqslant \deg[\Pi_2(\operatorname{div}\varphi)] \leqslant g \quad \text{et} \quad 0 \geqslant \deg[\Pi_1(\operatorname{div}\varphi)] \geqslant -g.$$

2. *Si* $\varphi\in\mathscr{E}$, *on a*:

$$0\leqslant \deg[\Pi_2(\operatorname{div}\varphi)]\leqslant g+h-1 \quad \textit{et} \quad 0\geqslant \deg|\Pi_1(\operatorname{div}\varphi)]\geqslant -g-h+1.$$

3. *Si* $\varphi\in\mathscr{A}$, *on a*:

$$0\leqslant \deg[\Pi_2(\operatorname{div}\varphi)]\leqslant g+e-1 \quad \textit{et} \quad 0\geqslant \deg[\Pi_1(\operatorname{div}\varphi)]\geqslant -g-e+1.$$

Preuve. La démonstration est basée sur le théorème de Riemann [2], mais nous nous bornerons au cas où $\varphi\in\mathscr{C}$.

La définition d'un comma revient à dire que si $D\in\mathfrak{m}$ est égal à $\Pi_1[\operatorname{div}\varphi]$, alors $l(D)=1$. D'après le théorème de Riemann, on a immédiatement:

$$l(D)+\deg D\geqslant 1-g$$

d'où $\deg D\geqslant -g$.

Comme $\deg D\leqslant 0$, d'après le lemme 2, nous avons démontré le premier point.

Proposition 5. *Si* S *possède une valeur absolue réelle ou de degré* 1, *on a*: $\mathscr{C}=\mathscr{E}$.

Preuve. 1. Le cas des corps de nombres est immédiat, car:

$$(P \text{ réelle et } |\varphi'|_P=|\varphi|_P)\Rightarrow \varphi'=\pm\varphi.$$

2. Supposons que E soit un corps de fonctions algébriques et que P_1 soit de degré 1. Soit $\varphi\in\mathscr{E}$ et $\varphi'\in B\setminus\{0\}$ telle que $|\varphi'|_P\leqslant|\varphi|_P$, pour tout $P\in S$. On en déduit que $|\varphi'|_P=|\varphi|_P$ pour tout $P\in S$ et qu'en particulier on a: $|\varphi'|_{P_1}=|\varphi|_{P_1}$. Puisque P_1 est de degré 1 il existe $\lambda\in k^*$ telle que: $|\varphi'-\lambda\varphi|_{P_1}<|\varphi|_{P_1}$. Posons $\varphi'-\lambda\varphi=\varphi''$; $\varphi''\in B$. Pour tout $P\in S$, on a $|\varphi''|_P\leqslant|\varphi|_P$, donc $\varphi''=0$.

Remarques. 1. Lorsque E est un corps de nombres algébriques $\mathscr{E}=\mathscr{A}$.

En effet, soit $\varphi\in\mathscr{A}$ et $\varphi'\in B\setminus\{0\}$ tel que $|\varphi'|_P\leqslant|\varphi|_P$ pour tout $P\in S$. Alors il existe $P_1\in S$ tel que $|\varphi'|_{P_1}=|\varphi|_{P_1}$.

Soient $\sigma_1,\ldots,\sigma_t$ les différents plongements de E dans $\boldsymbol{C}$ à conjugaison près, alors $|\varphi|_{P_1}=|\sigma_i(\varphi)|$ ou $|\varphi|_{P_1}=|\sigma_i(\varphi)|^2$ suivant que P_1 est réelle ou complexe.

Si P_1 est réelle $|\sigma_i(\varphi')|=|\sigma_i(\varphi)|$ entraîne $\varphi'=\pm\varphi$.

Si P_1 est complexe $|\sigma_i(\varphi')|^2=|\sigma_i(\varphi)|^2$ entraîne que

$$\sigma_i(\varphi')\cdot\overline{\sigma_i(\varphi')}=\sigma_i(\varphi)\cdot\overline{\sigma_i(\varphi)},$$

donc:

$$[\text{Norme } \sigma_i(\varphi')][\text{Norme } \overline{\sigma_i(\varphi')}]=[\text{Norme } \sigma_i(\varphi)][\text{Norme } \overline{\sigma_i(\varphi)}]$$

et

$$|\text{Norme } \varphi'|=|\text{Norme } \varphi|.$$

On en déduit que $|\varphi'|_P=|\varphi|_P$ pour tout $P\in S$.

2. Lorsque E est un corps de fonctions algébriques $\mathscr{E}$ n'est pas nécessairement égal à $\mathscr{A}$.

Exemple. $E=k(X)(\sqrt{X^2+1})$, $\varphi=1+X+2X^2-(2X+1)\sqrt{X^2+1}$. On constate que $\varphi\in\mathscr{A}\setminus\mathscr{E}$.

Lemme 5. *On pose* $K=k(X)$ *ou* $\boldsymbol{Q}$ *suivant le cas. Si* k *est fini, il n'existe qu'un nombre fini de* $\varphi\in B$, *non associés, tels que* $\mathscr{N}_{E/K}\varphi$ *soit donné, à un élément de* k^* *près.*

Preuve. Supposons qu'il existe $a\in A$, avec $A=k[X]$ ou $\boldsymbol{Z}$, et $\varphi,\varphi'\in B$, tels que:

$$\mathscr{N}\varphi'=\alpha.\mathscr{N}\varphi=\alpha a, \quad \alpha\in k^*.$$

Nous allons montrer que si, de plus

$$\varphi'\equiv\lambda\varphi \pmod{aB}$$

avec $\lambda\in\mathscr{U}$, alors $\varphi'=u\varphi$, avec $u\in\mathscr{U}$.

En effet nous avons:

$$\varphi'=\lambda\varphi+\mathscr{N}(\varphi)b, \quad \text{avec } b\in B$$

donc:

$$\frac{\varphi'}{\varphi}=\lambda+\frac{\mathscr{N}(\varphi)}{\varphi}b.$$

Comme $\dfrac{\mathscr{N}(\varphi)}{\varphi}b$ est entier sur A et que B est intégralement fermé, on voit que $(\varphi'/\varphi)\in B$.

On aurait de même $(\varphi/\varphi')\in B$, donc $\varphi'=u\varphi$, $u\in\mathscr{U}_S$. Le lemme résulte alors du fait que le cardinal de B/aB est fini.

Définition. Si pour tout $P_i\in S$, on se donne $c_i\in\boldsymbol{R}_+$, on pose:

$$c=(c_1,\ldots,c_t) \quad \text{où} \quad t=|S|,$$

$$\Pi_c=\{x\in E^*;\ |x|_{P_i}<c_i\}$$

et on dira que Π_c est le parallèlotope associé à c.

Le volume du parallélotope Π_c sera, par définition, le nombre $c_1\ldots c_t$ et on écrira:

$$v(\Pi_c)=c_1\ldots c_t.$$

Lemme 6 (de Minkowski). *Il existe une constante effectivement calculable* M *telle que* $v(\Pi_c)>M$ *entraîne que* $\Pi_c\cap B\neq\emptyset$ *quel que soit* c.

Preuve. 1. Lorsque E est un corps de nombres algébriques, c'est le lemme de Minkowski proprement dit et on peut prendre $M=(2/\pi)^t\sqrt{|D|}$.

2. Supposons maintenant que E est un corps de fonctions algébriques et donnons-nous $c=(c_1,\ldots,c_t)$.

Posons, pour $P\in S$: $|\varphi|_P=\gamma^{-\deg P\cdot v_P(\varphi)}$ où $\gamma>1$ comme dans [2],

$$e_P=\left[\frac{-\log c_i}{\deg P\log\gamma}\right] \quad \text{et} \quad D_c=\sum_{P\in S} e_P P.$$

On a:

$$\deg D_c=\sum_{P\in S} e_P\deg P$$

donc $l(D_c+\sum_{P\in S}P)\geqslant 1$ lorsque $v(\Pi_c)$ est assez grand $(v(\Pi_c)>\gamma^{e+g})$ puisque, d'après le théorème de Riemann:

$$l(D_c+\sum_{P\in S}P)+\deg(D_c+\sum_{P\in S}P)\geqslant 1-g$$

alors si $\varphi\in L(D_c+\sum_{P\in S}P)$, $\varphi\neq 0$, $\varphi\in\Pi_c\cap B$.

Lemme 7. *Soit $\varphi\in\Pi_c\cap B$, alors:*

$$|\mathcal{N}_{E/K}\varphi|\leqslant C^{te}$$

où on pose $|Q|=\gamma^{-\deg Q}$ lorsque Q est un polynôme appartenant à A, la constante ne dépendant que du volume de Π_c.

Preuve. 1. Si E est un corps de nombres algébriques, c'est un résultat classique.

2. Si E est un corps de fonctions algébriques, on a [5]:

$$\deg_K[\mathcal{N}_{E/K}\Pi_2(\operatorname{div}\varphi)]=\deg_E[\Pi_2(\operatorname{div}\varphi)]$$

or $\varphi\in\Pi_c\cap B$ entraîne (lemme 2) que:

$$0\geqslant\deg_E[\Pi_1(\operatorname{div}\varphi)]\geqslant C^{te},$$

$$0\leqslant\deg_E[\Pi_2(\operatorname{div}\varphi)]\leqslant C^{te}$$

donc la norme de φ, qui est dans $A=k[X]$, est un polynôme de degré borné.

Remarque. Si $\varphi\in\mathcal{O}$, la proposition 4 montre que: $|\mathcal{N}_{E/K}\varphi|\leqslant|X|^g$.

Théorème 4. $|k^*|<\infty\Rightarrow[\mathcal{A}:\mathcal{U}]<\infty$.

Preuve. 1. L'idée de la démonstration consiste à montrer que $|\mathcal{N}_{E/K}\varphi|$ est bornée, d'après le lemme 5, il n'y aura donc qu'un nombre fini de φ possibles.

2. Soit $\varphi\in\mathcal{A}$, on veut montrer que $|\mathcal{N}_{E/K}\varphi|$ est borné. Posons $c_P=|\varphi|_P$ pour tout $P\in S$, nous allons montrer par l'absurde que $c_{P_1}\ldots c_{P_t}\leqslant M$, où M désigne la constante du lemme 6.

Sinon ce lemme entraîne que $\Pi_c\cap B\neq\{0\}$ donc qu'il existe $\varphi'\in B\setminus\{0\}$ tel que:

$$|\varphi'|_P<|\varphi|_P \quad \text{pour tout } P\in S$$

ce qui est absurde.

Finalement le lemme 7 et le lemme 5 donnent le résultat.

Corollaire. *Si $|k^*|<\infty$, alors $[\mathcal{E}:\mathcal{U}]$ et $[\mathcal{O}:\mathcal{U}]$ sont finis.*

Définition. Soient $|\ |_{P_1},\ldots,|\ |_{P_t}$ les différentes valeurs absolues de S, on dira que (φ_h) est une suite de commas (resp. points extrémaux, arêtes) dans la direction P_i si:

1. $\varphi_0=1$,
2. φ_h est un comma (resp. point extrémal, arête) et:

$$|\varphi_h|_{P_i} \text{ croît avec } h, \quad |\varphi_h|_{P_j} \text{ décroît avec } h \text{ pour tout } j\neq i.$$

Lemme 8. *Si $P_i\in S$ et $|S|\geqslant 2$, E possède une suite de points extrémaux dans la direction P_i.*

Preuve. Par récurrence sur h, on construit l'ensemble

$$\mathcal{O}_{h+1}=\{\varphi\in B-\{0\};\ |\varphi|_{P_i}<|\varphi_h|_{P_i},\ i\neq 1\}.$$

D'après le lemme 6, il n'est pas vide.

Soit

$$c_1=\inf\{|\varphi|_{P_1};\ \varphi\in\mathcal{O}_{h+1}\}.$$

Cette borne inférieure existe et est atteinte:

— dans le cas où E est un corps de nombres, grâce au lemme de Minkowski,

— dans le cas où E est un corps de fonctions, on a $|\varphi_h|_{P_i}\leqslant 1$, $\forall i\neq 1$ par hypothèse de récurrence. Si $\varphi\in\mathcal{O}_{h+1}$, la formule du produit donne:

$$|\varphi|_{P_1}\prod_{P\neq P_1}|\varphi|_P=1.$$

Comme $|\varphi|_P\leqslant 1$, $\forall P\neq P_1$, on obtient $|\varphi|_{P_1}\geqslant 1$ et comme la valeur absolue $|\ |_{P_1}$ est discrète, on en déduit le résultat.

Soit $D_1=\{\varphi\in\mathcal{O}_{h+1};\ |\varphi|_{P_1}=c_1^{(h+1)}\}$. On considère P_2 et on pose

$$c_2=\inf\{|\varphi|_{P_2};\ \varphi\in D_1\}.$$

Cette borne inférieure existe et est atteinte, pour les mêmes raisons que ci-dessus.

Soit $D_2=\{\varphi\in D_1;\ |\varphi|_{P_2}=c_2\}$. On considère ensuite P_3, etc... Aucun des ensembles que l'on construit n'est vide. Finalement on choisit $\varphi_{h+1}\in D_t$.

Montrons que φ_{h+1} est un point extrémal. En effet, si $\varphi'\in B-\{0\}$ et

$|\varphi'|_P \leqslant |\varphi_{h+1}|_P$ pour tout $P \in S$, on voit que $\varphi' \in \mathscr{C}_{h+1}$ et que, successivement, φ' est dans tous les D_j donc, pour tout $P \in S$, on a:

$$|\varphi'|_P = |\varphi_{h+1}|_P.$$

THÉORÈME 5. *On suppose que* $[\mathscr{C}:\mathscr{U}] < \infty$, *alors* E *possède une famille d'unités* (ε_i), *avec* $1 \leqslant i \leqslant t$, *telle que*:

$$|\varepsilon_i|_{P_i} > 1 \text{ et } |\varepsilon_i|_P < 1, \quad \forall P \neq P_i,\ P \in S.$$

Pour tout $m < t$, *toute sous-famille de cardinal* m *est libre.*

Remarque. Cela fournit une deuxième démonstration du corollaire 3.

Preuve. 1. Puisqu'il n'y a qu'un nombre fini de classes de points extrémaux, si l'on se fixe une direction P_i, une classe au moins contient deux points extrémaux distincts dans la direction P_i, soient φ_{n_1} et φ_{n_2} deux points extrémaux, avec $n_1 < n_2$.

On peut alors poser:

$$\varepsilon_i = \varphi_{n_2}/\varphi_{n_1}.$$

2. Montrons par exemple que la famille $\varepsilon_1, \ldots, \varepsilon_{t-1}$ est libre. On a en effet, pour $i = 1, \ldots, t-1$:

$$\sum_{j=1}^{t} \log |\varepsilon_i|_{P_j} = 0$$

donc:

$$\sum_{j=1}^{t-1} \log |\varepsilon_i|_{P_j} = -\log |\varepsilon_i|_{P_t} > 0$$

finalement

$$\log |\varepsilon_i|_{P_i} > \sum_{\substack{j=1 \\ j \neq i}}^{t-1} |\log |\varepsilon_i|_{P_j}|$$

donc le déterminant:

$$\begin{vmatrix} \log |\varepsilon_1|_{P_1} & \ldots & \log |\varepsilon_1|_{P_{t-1}} \\ \log |\varepsilon_{t-1}|_{P_1} & \ldots & \log |\varepsilon_{t-1}|_{P_{t-1}} \end{vmatrix}$$

est non nul.

DÉFINITION. 1. Soient φ et ψ deux éléments de E^*, on dit que φ est *équivalent* à ψ s'il existe λ appartenant à k^* tel que $\varphi = \lambda\psi$, on note $\varphi \sim \psi$.

2. On dit que la suite des commas (φ_h) dans la direction P_i est *purement pseudo-périodique* si la suite $\alpha_h \sim \varphi_{h+1}/\varphi_h$ est telle qu'il existe $\pi_1 \geqslant 1$, $\alpha_{q\pi_1+r} \sim \alpha_r$, $\forall q \geqslant 0$, $0 \leqslant r \leqslant \pi_1 - 1$.

π_1 est appelé la *longueur* de la pseudo-période si π_1 est minimal.

THÉORÈME 6. *Soit* E *un corps de fonctions algébriques. Soient* $\mathscr{C}$ *(resp.* $\mathscr{U}$*) les commas (resp. les unités) de* E *relativement à* X. *On suppose que* $|S| = 2$.

Les propriétés suivantes sont équivalentes:

(1) $\operatorname{rg}(\mathscr{U}/k^*) = 1$.

(2) $[\mathscr{C}:\mathscr{U}] < \infty$.

(3) *La suite des commas est pseudo-périodique dans la direction* P_i, *pour* $i = 1$ *et* 2.

Preuve. On remarque que sous l'hypothèse $|S| = 2$, l'ensemble des commas de E est la réunion des commas dans la direction P_1 et dans la direction P_2 et on peut ordonner totalement les commas par leurs valeurs absolues en P_1 ou P_2 (modulo k^*) car deux commas non équivalents ont des valeurs absolues distincts en P_1 et P_2.

(1) $\Rightarrow$ (2). Soient u_0 l'unité fondamentale de $\mathscr{U}$ dans la direction P_1 et $\varphi_0 = 1$, $\varphi_1, \ldots, \varphi_{\pi_1-1}, \varphi_{\pi_1} \sim u_0$ les π_1 commas dans la direction P_1 compris entre 1 et u_0.

Soit φ un comma de E dans la direction P_1 alors d'après la proposition 3 il existe un entier q positif ou nul unique tel que

$$\varphi/u_0^q \text{ soit un comma dans la direction } P_1$$

et

$$\varphi/u_0^{q+1} \text{ soit un comma dans la direction } P_2.$$

Par suite, il existe un entier r: $0 \leqslant r \leqslant \pi_1 - 1$ tel que $(\varphi/u_0^q) \sim \varphi_r$.

(2) $\Rightarrow$ (3). Soit u_0 la première unité n'appartenant pas à k^*, qui apparait dans la suite des commas dans la direction P_1 et soit $(\varphi_h)_{h \geqslant 0}$ la suite des commas dans la direction P_1.

Il existe donc un unique entier $\pi_1 \geqslant 1$ tel que

$$u_0 \sim \varphi_{\pi_1}$$

et en précisant la démonstration précédente si $h = q\pi_1 + r$, avec $0 \leqslant r < \pi_1$, on a

$$\varphi_h \sim u_0^q \varphi_r$$

d'où

$$\alpha_{q\pi_1+r} = \frac{\varphi_{q\pi_1+r+1}}{\varphi_{q\pi_1+r}} \sim \frac{u_0^q \varphi_{r+1}}{u_0^q \varphi_r} = \alpha_r$$

si $0 \leqslant r \leqslant \pi_1 - 2$, si $r = \pi_1 - 1$, on a

$$\alpha_{q\pi_1+\pi_1-1} = \frac{\varphi_{(q+1)\pi_1}}{\varphi_{q\pi_1+\pi_1-1}} \sim \frac{u_0^q \varphi_{\pi_1}}{u_0^q \varphi_{\pi_1-1}} = \alpha_{\pi_1-1}.$$

(3) $\Rightarrow$ (1). Supposons la suite des commas purement pseudo-périodique

$$\alpha_{q\pi_1+r} \sim \alpha_r, \quad q \geqslant 0,\ 0 \leqslant r \leqslant \pi_1 - 1.$$

Posons $u_0 = \alpha_0 \ldots \alpha_{\pi_1-1}$, alors $u_0 \notin k^*$ et on a:

$$\varphi_{q\pi_1} = \frac{\varphi_{q\pi_1}}{\varphi_{q\pi_1-1}} \cdot \frac{\varphi_{q\pi_1-1}}{\varphi_{q\pi_1-2}} \cdots \frac{\varphi_1}{\varphi_0},$$

$$\varphi_{q\pi_1} = \alpha_{q\pi_1-1} \cdot \alpha_{q\pi_1-2} \ldots \alpha_0 \sim \underbrace{\alpha_{\pi_1-1} \cdot \alpha_{\pi_1-2} \ldots \alpha_0}_{u_0} \ldots \underbrace{\alpha_{\pi_1-1}\, \alpha_{\pi_1-2} \cdot \alpha_0}_{u_0},$$

$$\varphi_{q\pi_1} = u_0^q.$$

D'autre part, on a si φ est un comma, d'après la proposition 4

$$\deg_K(\mathcal{N}_{E/K} \operatorname{div}_2 \varphi) \leqslant g \quad \text{(on a posé } \operatorname{div}_2 \varphi = \Pi_2(\operatorname{div} \varphi)\text{)}$$

d'où

$$0 \leqslant \deg_K(\mathcal{N}_{E/K} \operatorname{div}_2(\varphi_{q\pi_1})) = \deg_K(\mathcal{N}_{E/K} \operatorname{div}_2(u_0^q))$$
$$= q \deg_K(\mathcal{N}_{E/K} \operatorname{div}_2(u_0)) \leqslant g, \quad \forall q \geqslant 0$$

ce qui entraîne que $\deg_K \mathcal{N}_{E/K} \operatorname{div}_2(u_0) = 0$.

Ceci montre que u_0 est une unité non triviale de $\mathcal{U}$, comme on sait que $\operatorname{rg}(\mathcal{U}/k^*) \leqslant 1$ on a $\operatorname{rg}(\mathcal{U}/k^*) = 1$.

Remarque. Si dans le théorème 6, on remplace $|S| = 2$ par $|S| = t > 2$, on peut montrer que (2) $\Rightarrow$ (3) $\Rightarrow$ (1), mais on ne sait pas si (1) $\Rightarrow$ (2) ou si (3) $\Rightarrow$ (2).

On revient au cas $|S| = 2$. Les commas, comme les unités, sont définis à une constante multiplicative près, pour avoir l'unicité à une racine n-ième de l'unité appartenant à k près, on choisit un système de représentant $\mathcal{S}$ de k^*/k^{*n} où $k^{*n} = \{\alpha^n \mid \alpha \in k^*\}$, tel que $1 \in \mathcal{S}$ $(n = [E:K])$.

Définition. φ sera un *comma simplifié* si φ est un comma et si $\mathcal{N}_{E/K}\varphi = \gamma_l X^l + \ldots$ on a $\gamma_l \in \mathcal{S}$. On voit alors que deux commas simplifiés équivalents diffèrent d'une racine n-ième de l'unité appartenant à k, en effet, soient φ et ψ deux commas simplifiés

$$\mathcal{N}\varphi = \gamma_l X^l + \ldots,$$
$$\mathcal{N}\psi = \delta_l X^l + \ldots$$

et on a $\psi = \zeta\varphi$ pour un certain $\zeta \in k^*$ d'où $\delta_l = \zeta^n \gamma_l$ et donc $\zeta^n = 1$.

Dans le cas $k = \mathbf{Q}$, on pourra choisir le système de représentants $\mathcal{S}$ tel que $s \in \mathcal{S}$ si et seulement si s est un entier ne possédant pas de puissance n-ième dans sa décomposition en facteurs premiers et $s > 0$ si n est impair. Ceci permet d'avoir, dans ce cas, l'unicité du comma simplifié.

Définition. On dit que la suite des commas simplifiés (φ_h) dans la direction P_i est purement périodique si la suite $\alpha_h = \varphi_{h+1}/\varphi_h$ est telle qu'il existe $\pi_2 \geqslant 1$, $\alpha_{q\pi_2+r} = \zeta\alpha_r$, $\forall q \geqslant 0$, $0 \leqslant r \leqslant \pi_2$ où ζ est une racine n-ième de l'unité de k. π_2 sera appelé la longueur de la période.

Ceci permet de préciser le théorème 6.

Proposition. (a) *Si u est une unité de norme λ alors u^n/λ est une unité de norme 1.*

(b) *La suite des commas dans la direction P_i est purement pseudo-périodique si et seulement si elle est purement périodique, et $\pi_1 \neq \pi_2$ si et seulement si il existe une unité qui est un comma simplifié de norme différente de l'unité et dans ce cas $\pi_2 | n\pi_1$.*

Preuve. Le (a) est clair, montrons le (b). Supposons la suite des commas simplifiés purement pseudo-périodique dans la direction P_1 de longueur π_1 et posons

$$\mathcal{N}(\varphi_{\pi_1}) = \lambda$$

on a, $\forall q \geqslant 0$, $\forall r$, $0 \leqslant r \leqslant n-1$, $\forall s$, $0 \leqslant s \leqslant \pi_1 - 1$.

$$\mathcal{N}\left(\frac{\varphi_{qn\pi_1}}{\lambda^q} \cdot \varphi_{r\pi_1+s}\right) = \mathcal{N}(\varphi_{r\pi_1+s})$$

de plus on montre que $\dfrac{\varphi_{qn\pi_1}}{\lambda^q} \cdot \varphi_{r\pi_1+s}$ est le comma dans la direction P_i d'indice $qn\pi_1 + r\pi_1 + s$ et c'est un comma simplifié d'après l'égalité des normes et du fait que $\varphi_{r\pi_1+s}$ est un comma simplifié, on en déduit l'égalité:

$$\varphi_{qn\pi_1+r\pi_1+s} = \zeta \cdot \frac{\varphi_{qn\pi_1}}{\lambda^q} \cdot \varphi_{r\pi_1+s}$$

où ζ est une racine n-ième de l'unité de k.

En passant au quotient, on a $\forall q \geqslant 0$, $\forall r$, $0 \leqslant r \leqslant n-1$, $\forall s$, $0 \leqslant s \leqslant \pi_1 - 1$

$$\alpha_{qn\pi_1+r\pi_1+s} = \zeta' \alpha_{r\pi_1+s}$$

où ζ' est une racine n-ième de l'unité de k, et ceci montre que la période divise $n\pi_1$.

2. Étude analytique d'un cas particulier

2.1. Généralités. 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:

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

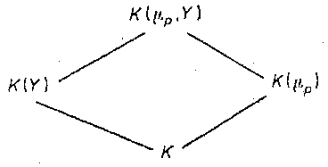
Dans toute la suite $\bar{k}$ sera fixée et μ_p désignera le groupe des racines p-ièmes de l'unité dans $\bar{k}$.

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, $-D/4$ 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 la clôture algébrique $\bar{k}$ de k.

PROPOSITION 6. *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) $\mathrm{Gal}\, K(\mu_p, Y)/K(\mu_p) \cong \boldsymbol{Z}/p\boldsymbol{Z}$,
$\mathrm{Gal}\, K(\mu_p, Y)/K(Y) \cong \mathrm{Gal}\, K(\mu_p)/K \cong \mathrm{Gal}\, k(\mu_p)/k \cong G \subseteqq (\boldsymbol{Z}/p\boldsymbol{Z})^*$.

On désigne par $k((1/X))$ le corps de séries formelles en $1/X$ du type:

$$F(X) = \sum_{m \geqslant m_0} a_m X^{-m}, \qquad a_m \in k.$$

Lorsque $F(X) \neq 0$, si on suppose $a_{m_0} \neq 0$ on dit que $-m_0$ est le degré de F; lorsque $F(X) = 0$, on pose degré de F égal $-\infty$, on le note $\deg F$. On désigne par t l'application:

$$k((1/X)) \to k,$$

$$F \to t(F) = \begin{cases} a_{m_0} & \text{si} \quad F \neq 0, \\ 0 & \text{si} \quad F = 0. \end{cases}$$

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

PROPOSITION 7. *L'équation* $Y^p = D(X)$ *admet une solution unitaire* Δ *dans* $k((1/X))$.

Preuve. $D(X) = X^{pn}[1 + (1/X)R(1/X)]$, où $R(1/X)$ est un polynôme en $1/X$ de degré $pn-1$. 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:

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

D'après la proposition 6, $\Delta(X)$ est un élément algébrique de degré p sur $k(X)$ et on a degré $\Delta(X) = n$ (en tant que série formelle).

Soit $\zeta \in k$ une racine primitive p-ième de l'unité, alors les autres racines de l'équation sont $\zeta^i \Delta$, $1 \leqslant i \leqslant p-1$.

On pose

$$U = (U_0, U_1, \ldots, U_{p-1}) \in A^p \quad \text{avec } A = k[X],$$

$$\varphi(U) = U_0 + U_1 \Delta + \ldots + U_{p-1} \Delta^{p-1},$$

$$\mathscr{C}(U) = \frac{\mathscr{N}(\varphi(U))}{\varphi(U)}$$

où $\mathscr{N}$ désigne la norme de l'extension algébrique

$$k(X) \to k(X)(\Delta),$$

$$\mathscr{N}(\varphi(U)) = \varphi_0 \cdot \sigma(\varphi) \ldots \sigma^{p-1}(\varphi) \in A,$$

où

$$\sigma^i(\Delta) = \zeta^i \Delta, \qquad 1 \leqslant i \leqslant p-1.$$

On pose:

$$\Phi(U) = \deg \varphi(U),$$

$$C(U) = \deg \mathscr{C}(U),$$

$$N(U) = \deg \mathscr{N}\varphi(U),$$

$$\deg U = \max(\deg U_0, \deg U_1 \Delta, \ldots, \deg U_{p-1} \Delta^{p-1}).$$

Remarquons que l'on a soit $N(U) \geqslant 0$, soit $N(U) = -\infty$ et que dans ce dernier cas $U = 0$, en effet $N(U) = -\infty$ si et seulement si il existe i, $0 \leqslant i \leqslant p-1$ tel que $\sigma^i \varphi(U) = 0$ et comme l'extension $K(\zeta, \Delta)/K(\zeta)$ est de degré p, on a $U = 0$.

On pose:

$$\varphi_i = \sigma^i \varphi, \qquad 0 \leqslant i \leqslant p-1, \qquad \varphi_p = \varphi_0.$$

Nous désignerons par G le groupe de Galois de $k(\zeta)/k$, c'est aussi celui de $K(\zeta)/K$ et il est isomorphe à un sous-groupe de $(\boldsymbol{Z}/p\boldsymbol{Z})^*$.

Son action sur $\mu_p = \{\zeta^0, \zeta^1, \ldots, \zeta^{p-1}\}$ sera représentée (abus de langage) de la manière suivante:

$$\tau(\zeta^i) = \zeta^{\tau(i)}, \qquad \tau \in G, \qquad i \in \boldsymbol{Z}/p\boldsymbol{Z}.$$

Naturellement on aura aussi:

$$\tau(\varphi_i) = \varphi_{\tau(i)}.$$

G opère donc sur Z/pZ et on désignera par ω_h les orbites de Z/pZ pour l'action de G:

$$Z/pZ = \bigcup_{0 \leqslant h \leqslant d(k)} \omega_h$$

on conviendra de poser $\omega_0 = \{0\}$.

Le nombre d'orbites est donc $d(k)+1$.

Si l'on pose $\Omega = \{\varphi_0, \varphi_1, \ldots, \varphi_{p-1}\}$, les orbites de Ω pour l'action de G sont naturellement les ensembles

$$\{\varphi_i \mid i \in \omega_h\}.$$

On pose:

$$\Phi_n(U) = \sum_{i \in \omega_h} \deg \varphi_i(U).$$

Remarque. Si $G \cong (Z/pZ)^*$, on a:

$$|\omega_h| = \varphi(p/d) \quad \text{où} \quad d = (h, p),$$

$$d(k) = \sum_{\substack{d \mid p \\ 1 \leqslant d < p}} 1.$$

2.2. Etude de la clôture intégrale B.

THÉORÈME 7. *On suppose l'hypothèse faible vérifiée.*

On met D sous la forme $Q_1^{\alpha_1} \ldots Q_s^{\alpha_s} \cdot F$ où $Q_1, \ldots, Q_s$ sont des polynômes irréductibles distincts de $k[X]$ tels que $\alpha_l \geqslant 2$ pour $1 \leqslant l \leqslant s$ et $(Q_l, F) = 1$ pour $1 \leqslant l \leqslant s$.

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

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

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

où les polynômes U_i appartiennent à A et vérifient la condition:

$$\forall i, \ \forall l, \quad Q_l^{\alpha_l - j} \mid U_i \quad \text{où} \quad j = [ip/\alpha_l].$$

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 $Q^2 \cdot F$ avec Q sans facteur carré, F sans racine multiple dans $\bar{k}$, $(Q, F) = 1$ et si on pose $\bar{D} = QF^2$ on a:*

$$B = A + AY + A\bar{Y} \quad \text{où} \quad \bar{Y}^3 = \bar{D}.$$

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,

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

et pour des raisons galoisiennes ($\mathfrak{p}$ étant arbitraire):

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

on en déduit que:

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

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:

$$\Big(P, \sum_{i=0}^{p-1} U_i V_i\Big) = 1.$$

On en déduit que:

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

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

$$f \in B \Leftrightarrow v_{q_l}(\varphi) \geqslant \beta_l \quad \text{pour} \quad 1 \leqslant l \leqslant s$$

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 telle que $v_{q_l}(Q_l) = 1$, on a alors $v_{q_l}(q_l) = 1/p$ car on a supposé $(\alpha_l, p) = 1$ pour $1 \leqslant l \leqslant s$.

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

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

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

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

et donc:

$$v_q(\varphi) \geqslant \beta \Leftrightarrow Q^\beta | U_i, \quad 0 \leqslant i < p/\alpha, \quad Q^{\beta-1} | U_i, \quad p/\alpha \leqslant i < 2p/\alpha, \ldots$$

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.

2.3. Rang du groupe $\mathscr{G}(\mathscr{O})$. D'après le théorème 1 l'étude de $\mathscr{G}(\mathscr{O})$ revient à celle de l'équation de Pell:

$$(E_p) \qquad \mathscr{N}[\varphi(U)] \in k^*.$$

On remarque que les éléments de k^* sont solutions de (E_p), on les appellera les "solutions triviales" de (E_p).

On rappelle que $\mathscr{G}(\mathscr{O}) = \{\varphi(U) \text{ tels que } \mathscr{N}[\varphi(U)] \in k^*\}/\sim$ où $\sim$ désigne la relation d'équivalence

$$\varphi_1 \sim \varphi_2 \quad \text{ssi il existe } \lambda \in k^* \text{ tel que } \varphi_1 = \lambda \varphi_2.$$

Le théorème 3 nous donne le résultat suivant:

THÉORÈME 3'. *$\mathscr{G}(\mathscr{O})$ est un groupe abélien de rang inférieur ou égal à $d(k)$, où $d(k)+1$ désigne le nombre d'orbites de μ_p pour l'action de G.*

Nous expliquerons plus loin pourquoi le nombre t des places rationnelles à l'infini est égal à $d(k)+1$.

Mais pour des raisons de commodité (le lemme suivant sera utilisé ultérieurement) nous allons donner une preuve "analytique" directe du théorème 3'.

LEMME 9. *On suppose $U \neq 0$.*

(a) *$\forall U \in A^p$, $\forall h \in \{0, \ldots, d(k)\}$ et $\forall i \in \omega_h$, on a:*

$$\deg \varphi_i(U) = \text{constante} := n_h,$$

$$\Phi_i(U) = |\omega_h| \, n_h.$$

(b) *Si $\Phi_h(U) < |\omega_h| \deg U$ pour tout $h \in \{0, \ldots, d(k)\}$ sauf pour un h_0, alors:*

$$\Phi_{h_0}(U) = |\omega_{h_0}| \deg U.$$

Preuve du lemme 9. (a) Posons

$$\varphi_i(U) = \sum_{m \geqslant -\deg U} a_m^{(i)} X^{-m}, \quad 0 \leqslant i \leqslant p-1, \quad a_m^{(i)} \in k(\zeta),$$

$$U_j \Delta^j = \sum_{m \geqslant -\deg U} b_m^{(j)} X^{-m}, \quad 0 \leqslant j \leqslant p-1, \quad b_m^{(j)} \in k$$

on a

$$a_m^{(i)} = \sum_{j=0}^{p-1} \zeta^{ij} b_m^{(j)}, \quad \forall m \geqslant -\deg U, \quad 0 \leqslant i \leqslant p-1.$$

Montrons que $\deg \varphi_i(U) = \deg \varphi_j(U)$ si i et $j \in \omega_h$

$$i \text{ et } j \in \omega_h \Rightarrow \exists \tau \in G \quad \text{t.q.} \quad \varphi_i = \tau \varphi_j$$

d'où

$$a_m^{(i)} = \tau(a_m^{(j)}) \quad \forall m \geqslant -\deg U$$

en particulier:

$$a_{n_h}^{(i)} = \tau(a_{n_h}^{(j)}) \neq 0$$

ceci montre que $\deg \varphi_i(U) = n_h$, $\forall i \in \omega_h$.

(b) Clairement, on a:

$$\Phi_{h_0}(U) \leqslant |\omega_{h_0}| \deg U.$$

Supposons que l'inégalité soit stricte, alors nous avons:

$$\Phi_h < |\omega_h| \deg U, \quad \text{pour tout } h.$$

D'après (a), ceci implique:

$$\deg \varphi_i(U) < \deg U, \quad \text{pour tout } i$$

d'où:

$$0 = a_{-\deg U}^{(i)} = \sum_{j=0}^{p-1} \zeta^{ij} b_{-\deg U}^{(j)}, \quad \text{pour tout } i$$

et en résolvant ce système de Vandermonde:

$$b^{(j)}_{-\deg U} = 0, \quad 0 \leqslant j \leqslant p-1$$

ce qui contredit la définition de $\deg U$.

Preuve du théorème. Considérons l'homomorphisme

$$\mathscr{G}(\mathscr{O}) \xrightarrow{L} Z^p,$$

$$\varphi(U) \mapsto (\deg \varphi_0(U), \deg \varphi_1(U), \ldots, \deg \varphi_{p-1}(U)).$$

1. L est injectif. Supposons $\varphi(U) \notin k^*$, alors on a $\deg U > 0$. Donc $\deg \varphi_i(U) = 0$, $\forall i$, entraîne:

$$\Phi_h(U) < |\omega_h| \deg U$$

pour $h \in \{1, \ldots, d(k)\}$.

D'après la partie (b) du lemme 9, on a donc:

$$\varphi_0(U) = \Phi_0(U) = \deg U$$

et comme $\varphi_0(U) = 0$, $\deg U = 0$, ce qui est absurde.

2. Il est clair que l'image de L est contenue dans la variété linéaire d'équations:

$$X_0 + X_1 + \ldots + X_{p-1} = 0,$$

$$X_i = X_{i_0}, \quad \forall h \in \{0, \ldots, d(k)\} \text{ et } \forall i \in \omega_h,\ i_0 \in \omega_h \text{ fixe}, \quad i \neq i_0$$

la première équation provient de $\mathscr{N}\varphi(U) = Cte \neq 0$ et les autres du lemme 9 (a).

Ces équations étant indépendantes, le rang est au plus $p-r$, où r est le nombre d'équations.

On a

$$r = 1 + \sum_{h=0}^{d(k)} (|\omega_h| - 1) = p - d(k).$$

Corollaire 7. *Si $d(k) = 1$, $\mathscr{G}(\mathscr{O})$ est soit trivial, soit cyclique infini.*

Définition. Si l'équation de Pell $\mathscr{N}\varphi(U) = Cte \neq 0$ admet une solution non triviale, on dira que l'équation de Pell est *résoluble*.

2.4. Interprétation géométrique.

2.4.1. La courbe Γ et sa jacobienne. On considère la courbe Γ d'équation:

$$Y^p = D(X)$$

et on désigne par L le corps des fonctions de Γ sur k: $L = k(X, Y)$, $\bar{L}$ le corps des fonctions de Γ sur $\bar{k}$: $\bar{L} = \bar{k}(X, Y)$.

Les extensions $L/k(X)$ et $\bar{L}/\bar{k}(X)$ sont de degré p, et la seconde est galoisienne de groupe de Galois $H \cong \boldsymbol{Z}/p\boldsymbol{Z}$.

La première n'est pas nécessairement galoisienne comme l'on voit en prenant $k = \boldsymbol{Q}$.

On désignera par σ un générateur de H, il sera déterminé par:

$$\sigma(X) = X,$$

$$\sigma(Y) = \zeta Y$$

où ζ est une certaine racine primitive p-ième de 1. Il est clair que H est un groupe d'automorphismes de la courbe Γ.

Une place $\mathfrak{p}$ de $\bar{k}(X)$ se prolonge en général en p place $P_1, P_2, P_3, \ldots$ de $\bar{K}$, sauf lorsque $D(X)$ est annulé par $\mathfrak{p}$ (on écrira $D(X) \in \mathfrak{p}$). Les prolongements des places à distance finie de $\bar{k}(X)$ seront appelées les "points à distance finie" de Γ.

Pour prolonger la place à l'infini ($(1/X) \in \mathfrak{p}$), on considère la transformation birationnelle:

$$X \mapsto X' = 1/X,$$

$$Y \mapsto Y' = Y/X^n$$

qui transforme Γ en Γ^* d'équation:

$$Y'^p = D^*(X')$$

où D^* désigne le polynôme réciproque de D. Puisque D est unitaire, $D^*(0) = 1$, donc la place à l'infini se prolonge en p places de $\bar{K}$, que l'on notera ∞_0 (lorsque $Y \mapsto 1$), ∞_1 (lorsque $Y \mapsto \zeta$), ..., ∞_{p-1} (lorsque $Y \mapsto \zeta^{p-1}$) (voir [7]).

Le groupe abélien libre $\mathscr{A}$ engendré par les places de $\bar{K}$ est appelé le *groupe des diviseurs* de Γ. Les éléments de $\mathscr{A}$ qui sont invariants par $\mathrm{Gal}(\bar{k}/k)$ sont appelés les *diviseurs rationnels* de Γ lorsque k est de caractéristique zéro (2).

La *jacobienne* J de Γ est le groupe quotient du groupe $\mathscr{A}_0$ des diviseurs de degré zéro par le sous-groupe des diviseurs des éléments de $\bar{L}$. Un point de J est *rationnel* lorsqu'il est l'image d'un diviseur rationnel par la projection canonique: $\mathscr{A}_0 \to J$.

2.4.2. Module des diviseurs rationnels à l'infini de degré 0. On désigne par k' le corps $k(\zeta)$ et par G le groupe de Galois de k'/k. Lorsque $\tau \in G$, on prolonge τ à $k'(X, Y)$ en posant $\tau(X) = X$ et $\tau(Y) = \zeta Y$.

(2) Dans le cas général, il faut tenir compte des questions de séparabilité.

Soit $\mathscr{M} = \mathbf{Z}\infty_0 + \mathbf{Z}\infty_1 + \ldots + \mathbf{Z}\infty_{p-1}$ le $\mathbf{Z}$-module des "diviseurs à l'infini" de Γ, alors G agit sur $\mathscr{M}$ de la manière suivante:

$$\tau(v_0\infty_0 + \ldots + v_{p-1}\infty_{p-1}) = v_0\infty_0 + v_1\infty_{\tau(1)} + v_2\infty_{\tau(2)} + \ldots + v_{p-1}\infty_{\tau(p-1)}$$

$v_0, \ldots, v_{p-1}$ représentants des entiers quelconques.

Posons $D = v_0\infty_0 + \ldots + v_{p-1}\infty_{p-1} \in \mathscr{M}$.

Définition. Nous dirons que D est *rationnel sur* k ssi, pour tout $\tau \in G$, on a $\tau(D) = D$.

Proposition 8. *L'ensemble des diviseurs de* $\mathscr{M}$ *rationnels sur* k *admet pour base l'ensemble des diviseurs* $P_h = \sum_{i\in\omega_h} \infty_i$, *avec* $0 \leqslant h < d(k)$.

Ce module est donc isomorphe à $\mathbf{Z}^{d(k)+1}$.

Preuve. Puisque $\mathscr{M}$ est un $\mathbf{Z}$-module libre de base $\infty_0, \ldots, \infty_{p-1}$, la condition pour que D soit rationnel sur k s'écrit:

$$v_i = v_{\tau(i)}$$

pour tout $\tau \in G$.

Ceci prouve que v_i ne dépend que de la classe ω_h de i dans $\mathbf{Z}/p\mathbf{Z}$ modulo l'action G. Comme dans le lemme 9, on a donc:

$$v_j = v_i \quad \text{si} \quad i, j \in \omega_h$$

et l'on voit que le diviseur D s'écrit d'une manière et d'une seule:

$$D = \sum_{0\leqslant h\leqslant d(k)} v_h\Big(\sum_{i\in\omega_h} \infty_i\Big).$$

Posons $P_h = \sum_{i\in\omega_h} \infty_i$, alors D s'écrit d'une manière et d'une seule:

$$D = \sum_{0\leqslant h\leqslant d(k)} v_h P_h.$$

Comme les diviseurs P_h sont au nombre de $d(k)+1$ on en déduit que le module des diviseurs rationnels à l'infini est isomorphe à $\mathbf{Z}^{d(k)+1}$.

Corollaire 8. 1. *Si l'on désigne par* $\mathscr{M}_0$ *le module des diviseurs rationnels à l'infini de degré zéro, on a:*

$$\mathscr{M}_0 = \Big\{\sum_h v_h P_h \Big| \sum_h v_h|\omega_h| = 0\Big\}.$$

2. $\mathscr{M}_0$ *est isomorphe au sous-module de* $\mathbf{Z}^p$ *défini par les équations*

$$X_0 + X_1 + \ldots + X_{p-1} = 0,$$

$$X_i = X_{i_0}, \quad \forall h \in \{0, \ldots, d(k)\},\ \forall i \in \omega_h,\ i_0 \in \omega_h \text{ fixé},\ i \neq i_0.$$

3. $\mathscr{M}_0$ *est isomorphe à* $\mathbf{Z}^{d(k)}$.

Remarques. 1. $\varphi_i = \sigma^i\varphi$, donc l'opposé de son degré est la même chose que sa valuation au point ∞_0, donc que la valuation de φ au point $\sigma^{-1}(\infty_0) = \infty_{-i}$, ainsi:

$$\deg \varphi_i(U) = -v_{-i}(\varphi).$$

2. Comme nous l'avions annoncé dans le paragraphe 2.3, la proposition 3 entraîne que le nombre des places à l'infini, rationnelles sur k, est égal à $d(k)+1$.

Nous conclurons ce paragraphe en regroupant les derniers corollaires du paragraphe 1.2 sous forme de "théorème de dualité".

Théorème 8. 1. *Soit* $\mathscr{E}$ *le monoïde des diviseurs des éléments de* $\mathscr{C}$, *alors* $\mathscr{G}(\mathscr{C}) \cong \mathscr{M}_0 \cap \mathscr{E}$.

2. *Si l'on pose* $J_\infty(\mathscr{C}) = \mathscr{M}_0/\mathscr{M}_0 \cap \mathscr{E}$ *et si l'on désigne par* $T(\mathscr{C})$ *le sous-groupe de torsion de* $J_\infty(\mathscr{C})$, *nous avons:*

$$\operatorname{rang}\big(J_\infty(\mathscr{C})/T(\mathscr{C})\big) + \operatorname{rang}\mathscr{G}(\mathscr{C}) = d(k).$$

3. *Sous l'hypothèse forte* $J_\infty(\mathscr{C})$ *est la "partie à l'infini" de la jacobienne* J *de* Γ.

Corollaire 9. *Lorsque l'hypothèse forte est vérifiée, les assertions suivantes sont équivalentes:*

(i) *le rang de* $\mathscr{G}$ *est égal à* $d(k)$,

(ii) *les éléments de* $\mathscr{M}_0$ *sont d'ordre fini sur la jacobienne* J *de* Γ.

2.5. Construction des commas dans le cas particulier $|S| = 2$. Commençons par redonner la définition d'un comma de $\mathscr{C}$ dans le cas particulier où l'ordre est:

$$\mathscr{O} = A + A\Delta + \ldots + A\Delta^{p-1}.$$

Définition. On dit que $U \in A^p$ est un *comma de* $\mathscr{O}$ si $U \neq 0$ et vérifie la propriété:

$$\big(\forall U' \in A^p,\ U' \neq 0,\ \forall h,\ 0 \leqslant h \leqslant d(k),\ \Phi_h(U') \leqslant \Phi_h(U)\big) \Rightarrow (\exists \lambda \in k^*,\ U' = \lambda U).$$

D'après le corollaire 5, nous savons que $\mathscr{O} = B$ si l'hypothèse forte est vérifiée, et $\mathscr{O} \subset B$, avec l'inclusion stricte possible, dans le cas de l'hypothèse faible.

Dans le cas particulier que l'on considère $Y^p = X^{p^n} + \ldots$ on caractérise le fait que $|S| = 2$ par

Proposition 9. *Le nombre de places au-dessus de* $\mathscr{P}_\infty$ *est égal à deux si et seulement si* p *est premier et* $[k(\mu_p):k] = p-1$.

Preuve. Nous avons vu, que pour calculer le nombre d'éléments de S, il fallait compter le nombre d'orbites de $\mathbf{Z}/p\mathbf{Z}$ pour l'action de G (on utilise les notations de la proposition 8).

Or, on a $G \subset (\mathbf{Z}/p\mathbf{Z})^*$ donc

$$[(\mathbf{Z}/p\mathbf{Z}):(\mathbf{Z}/p\mathbf{Z})^*] \leqslant [\mathbf{Z}/p\mathbf{Z}:G]$$

et comme:

$$[(\mathbf{Z}/p\mathbf{Z}):(\mathbf{Z}/p\mathbf{Z})^*] = \sum_{\substack{d|p \\ 1 \leqslant d < p}} 1$$

on en déduit le résultat.

On désignera par P_0 et P_1 les deux places au-dessus de $\mathscr{P}_\infty$ associées à Φ_0 et Φ_1. La place P_0 est de degré 1, la place P_1 est de degré $p-1$.

Dans le cas particulier où $|S| = 2$, l'ensemble des commas de $\mathcal{C}$ est la réunion de l'ensemble des commas dans la direction P_0 et de l'ensemble des commas dans la direction P_1 on a:

Proposition 10. *Les propriétés suivantes sont équivalentes:*

(1) *U est un comma de $\mathcal{C}$ dans la direction P_1.*

(2) *U est un comma de $\mathcal{C}$ et $\Phi_0(U) \leqslant 0$.*

(3) $(\forall\, U' \neq \lambda U,\ \lambda \in k^*,\ \Phi_0(U') \leqslant \Phi_0(U) \leqslant 0) \Rightarrow \deg U' > \deg U$.

Preuve. Elle résulte des définitions et de l'égalité $\Phi_1(U) = (p-1)\deg U$.

Dans toute la suite, on va supposer p premier et $[k(\mu_p):k] = p-1$.

Construction des commas U dans la direction P_1. Si on veut construire un $U \in A^p$ tel que $\Phi_0(U)$ soit le plus petit possible, on voudra annuler le plus grand nombre de coefficients dans le développement en série formelle de $\varphi(U)$. On va donc chercher à résoudre un système linéaire homogène où les inconnues sont les coefficients des polynômes U_0, $U_1, \ldots, U_{p-1}$.

Si on pose:

$$U_i = u_i^{(0)} X^{q-in} + u_i^{(1)} X^{q-in-1} + \ldots + u_i^{(q-in)}, \quad 0 \leqslant i \leqslant p-1,$$

$$A^i = X^{in} + a_i^{(1)} X^{in-1} + a_i^{(2)} X^{in-2} + \ldots, \quad 1 \leqslant i \leqslant p-1.$$

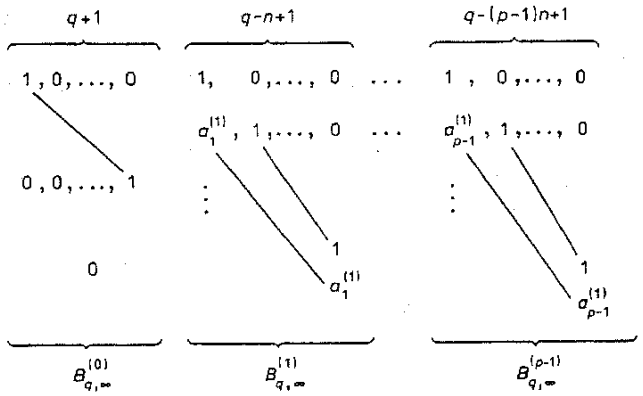
Le premier coefficient de $\varphi(U)$ éventuellement nul est:

$$u_0^{(0)} + u_1^{(0)} + \ldots + u_{p-1}^{(0)}.$$

Le deuxième coefficient est:

$$u_0^{(1)} + \underbrace{u_1^{(0)} a_1^{(1)} + u_1^{(1)}} + \ldots + \underbrace{u_{p-1}^{(0)} a_{p-1}^{(1)} + u_{p-1}^{(1)}}.$$

Nous sommes amené à considérer la matrice $A_{q,\infty}$ formée des blocs $B_{q,\infty}^{(0)}$, $B_{q,\infty}^{(1)}, \ldots, B_{q,\infty}^{(p-1)}$



Cette matrice $A_{q,\infty}$ a l_q colonnes:

$$l_q = \sum_{i=0}^{p-1} b_q^{(i)} \quad \text{où} \quad b_q^{(i)} = \begin{cases} q-in+1 & \text{si} \quad q-in+1 \geqslant 0, \\ 0 & \text{sinon} \end{cases}$$

ce qui donne:

$$(1) \qquad l_q = \begin{cases} (i+1)(q+1) - \dfrac{i(i+1)}{2} n, & \text{si} \quad \left[\dfrac{q}{n}\right] \leqslant p-2 \text{ avec } i = \left[\dfrac{q}{n}\right], \\ p(q+1) - \dfrac{p(p-1)}{2} n, & \text{si} \quad \left[\dfrac{q}{n}\right] \geqslant p-1. \end{cases}$$

a) Si $[q/n] \leqslant p-2$.

Trouver $U \neq 0$ avec $\deg U \leqslant q$ et $\Phi_0(U) \leqslant -m+q+1$ équivaut à trouver

$$\tilde{U} = (u_0^{(0)}, \ldots, u_0^{(q)}, \ldots, u_{p-1}^{(0)}, \ldots, u_{p-1}^{(q-in)}) \in k^{l_q}, \quad \tilde{U} \neq 0,$$

tel que $\tilde{U}$ soit solution du système $A_{q,m-1}\,\tilde{U} = 0$, où $A_{q,m-1}$ est la matrice tronquée ayant comme $m-1$ lignes les $m-1$ premières lignes de $A_{q,\infty}$.

b) De même si $[q/n] \geqslant p-1$.

Trouver $U \neq 0$ avec $\deg U \leqslant q$ et $\Phi_0(U) \leqslant -m+q+1$ équivaut à trouver

$$\tilde{U} = (u_0^{(0)}, \ldots, u_0^{(q)}, \ldots, u_{p-1}^{(0)}, \ldots, u_{p-1}^{q-(p-1)n}) \in k^{l_q}, \quad \tilde{U} \neq 0,$$

tel que $\tilde{U}$ soit solution du système $A_{q,m-1}\,\tilde{U} = 0$, où $A_{q,m-1}$ désigne la même matrice que précédemment.

Dans les deux cas:

Trouver $U \neq 0$ avec $\deg U \leqslant q$ et $\Phi_0(U)$ minimum équivaut à trouver un entier m_q maximum tel qu'il existe $\tilde{U} \in k^{l_q}$, $\tilde{U} \neq 0$ tel que: $A_{q,m_q-1}\,\tilde{U} = 0$, ce qui équivaut à trouver un entier $m_q \geqslant 1$ tel que:

$$(2) \qquad \exists\, \tilde{U} \in k^{l_q},\ \tilde{U} \neq 0, \quad A_{q,m_q-1}\,\tilde{U} = 0,$$

$$(3) \qquad \forall\, \tilde{U} \in k^{l_q}, \quad A_{q,m_q}\,\tilde{U} = 0 \Rightarrow \tilde{U} = 0.$$

La deuxième condition étant là pour assurer la maximalité de m.

Le nombre d'inconnues du système $A_{q,m_q-1}\tilde{U}=0$ étant l_q, on en déduit que le système $A_{q,l_q-1}\tilde{U}=0$ a une solution non triviale et par suite:

$$m_q \geqslant l_q.$$

Montrons maintenant que m_q est fini.

Pour cela, nous allons montrer qu'il existe un entier $m \geqslant 1$ suffisamment grand tel que:

$$\forall \tilde{U}\in k^{l_q}, \quad A_{q,m}\tilde{U}=0 \Rightarrow \tilde{U}=0.$$

Supposons le contraire:

$$\forall m \geqslant 1,\ \exists Y_m \neq 0 \quad Y\in k^{l_q}, \quad A_{q,m}Y=0.$$

Cette solution $Y_m \neq 0$ détermine un p-uple $(U_0, U_1, \ldots, U_{p-1}) \neq 0$ tel que:

$$\varphi(U)=U_0+U_1\Delta+\ldots+U_{p-1}\Delta^{p-1}.$$

Supposons de plus $\varphi(U)\neq 0$ alors $\mathcal{N}\varphi(U)\neq 0$ et donc $N(U)\geqslant 0$.

D'autre part, on a:

$$N(U)=\Phi_0(U)+\Phi_1(U)\leqslant -m+q+1+(p-1)q$$

et donc si nous prenons m assez grand

$$N(U)<0$$

par suite $\varphi(U)=0$ avec $U\neq 0$ ce qui contredit le fait que Δ soit un nombre algébrique de degré p sur $k(X)$.

Soit $\tilde{U}\in k^{l_q}$ une solution de (2), alors elle détermine un p-uple $U=(U_0, U_1, \ldots, U_{p-1})$ vérifiant:

$$(4)\quad \begin{cases} \begin{cases}\Phi_0(U)\leqslant -m_q+q+1\leqslant -l_q+q+1,\\ \Phi_1(U)=(p-1)\deg U\leqslant (p-1)q,\end{cases} \\ N(U)\leqslant \begin{cases}(p-1-i)q+\dfrac{i(i+1)}{2}n-i, & \text{si} \quad i=\left[\dfrac{q}{n}\right]\leqslant p-2,\\ \dfrac{p(p-1)}{2}n-p+1=g, & \text{si} \quad \left[\dfrac{q}{n}\right]\geqslant p-1.\end{cases}(3)\end{cases}$$

(a) Montrons que $\tilde{U}$ *est unique* à une constante multiplicative près.

Soient $\tilde{U}$ et $\tilde{V}\in k^{l_q}$, $\tilde{U}$ et $\tilde{V}\neq 0$, deux solutions de (2), on a d'après (2) et (3):

(3) g est le genre de la courbe $Y^p=D(X)$ quand $D(X)$ n'a pas de racine multiple.

$$A_{q,m_q}\tilde{U}=\begin{bmatrix}0\\ \vdots\\ 0\\ \alpha\end{bmatrix}, \quad \alpha\neq 0, \qquad A_{q,m_q}\tilde{V}=\begin{bmatrix}0\\ \vdots\\ 0\\ \beta\end{bmatrix}, \quad \beta\neq 0$$

d'où:

$$A_{q,m_q}(\beta\tilde{U}-\alpha\tilde{V})=0$$

et donc d'après (3) $\beta\tilde{U}-\alpha\tilde{V}=0$.

(b) Montrons maintenant qu'une telle solution est un comma.

Soit $U'\neq 0$ tel que $\Phi_0(U')\leqslant\Phi_0(U)\leqslant 0$ et supposons $\deg U'\leqslant\deg U\leqslant q$ comme $\Phi_0(U')\leqslant\Phi_0(U)$, on a $A_{q,m_q-1}\tilde{U}'=0$ et donc d'après le (a) $U'=\lambda\cdot U$ avec $\lambda\in k^*$.

(c) Réciproquement un comma U de degré strictement positif et tel que $\Phi_0(U)\leqslant 0$ est construit de cette façon.

Posons $\deg U=q>0$, et soit U' le comma construit comme précédemment avec l'entier q.

On a d'après la construction de U',

$$\deg U'\leqslant q=\deg U,$$

$$\Phi_0(U')\leqslant\Phi_0(U)\leqslant 0.$$

Comme U est un comma on a:

$$\exists\lambda\in k^*, \quad U'=\lambda U.$$

Finalement, nous avons montré le résultat:

THÉORÈME 9. *Avec les notations définies ci-dessus*

– *"La" solution, définie à une constante multiplicative près, du système* $A_{q,m_q-1}\tilde{U}=0$ *est un comma de degré inférieur ou égale à* q.

– *Réciproquement, tout comma* U *dans la direction* P_1 *est construit de cette façon.*

En faisant varier q de 1 à l'infini, on obtient la suite des commas $(U^{(i)})_{i\geqslant 1}$ non deux à deux équivalents tels que la suite $(\deg U^{(i)})_{i\geqslant 1}$ soit strictement croissante. On dira que $U^{(i)}$ est un comma de rang i.

2.6. Propriétés des commas.

PROPOSITION 11. (1) *Si* U *est un comma, le* $\operatorname{pgcd}(U_0, U_1, \ldots, U_{p-1})=1$.

(2) *Deux commas successifs sont linéairement indépendants sur* A.

(3) $\varphi(U^{(1)})\sim E(\Delta)-\Delta$, *où* $E(\Delta)$ *désigne la partie polynomiale de* Δ.

(4) *Si* $p\geqslant 3$, *on a les inégalités*

$$\forall i\geqslant 1, \quad 1\leqslant\deg U^{(i+1)}-\deg U^{(i)}\leqslant[pn/2] \quad \text{si} \quad n\leqslant p-1,$$

$$1\leqslant\deg U^{(i+1)}-\deg U^{(i)}\leqslant(p+1)n/2 \quad \text{si} \quad n>p-1.$$

(4') *Si* $p=2$ *et si* $U^{(i)}$ *n'est pas solution de l'équation de Pell, on a:*

$$\forall i \geqslant 1, \quad 1 \leqslant \deg U^{(i+1)} - \deg U^{(i)} \leqslant n-1.$$

(5) *Toute solution non triviale* U *de l'équation de Pell*

$$\varphi(U) = Cte \neq 0$$

avec $\Phi_0(U) \leqslant 0$ *est un comma dans la direction* P_1.

Preuve. (1) Soit $P \in A$, $\deg P \geqslant 1$ et $P | U_l$ $(0 \leqslant l \leqslant p-1)$ alors il est clair que U/P est un comma et donc si U est le comma de rang i, il existe un entier j, $0 \leqslant j \leqslant i$, tel que

$$U^{(j)} = U^{(i)}/P \quad \text{d'où} \quad \Phi_0(U^{(i)}) = \Phi_0(P) + \Phi_0(U^{(j)}) > \Phi_0(U^{(j)}),$$

ce qui est impossible.

(2) Soient $U^{(i)}$, $U^{(i+1)}$ deux commas successifs. Supposons qu'il existe P, $Q \in A$:

$$PU^{(i)} + QU^{(i+1)} = 0$$

alors $Q | PU_l^{(i)}$ $(0 \leqslant l \leqslant p-1)$ et d'après (1) $Q | P$, de même on montre que $P | Q$ d'où P et Q sont des constantes

$$\lambda U^{(i)} + \mu U^{(i+1)} = 0, \quad \lambda, \mu \in k$$

et comme

$$\deg U^{(i)} < \deg U^{(i+1)}, \quad \text{on a } \lambda = \mu = 0.$$

(3) Supposons $\deg U^{(1)} < n$ alors $U^{(1)} = (P, 0, \ldots, 0)$ avec $\deg P > 0$, or il est clair que $(P, 0, \ldots, 0)$ avec $\deg P > 0$ n'est pas un comma.

Maintenant prenons $q = n$, alors le comma U construit vérifie:

$$\Phi_0(U) \leqslant -1$$

en effet $A_{n;\alpha}$ a $n+2$ colonnes $(l_n = n+2)$ et d'après (4) $\Phi_0(U) \leqslant -l_n + n + 1 = -1$ et donc $U \neq U^{(0)}$.

Ce comma construit est de la forme

$$U = (U_0, U_1, 0, \ldots, 0) \quad \text{avec} \quad U_1 = Cte \neq 0$$

et comme il n'y a pas de comma de degré $< n$ à part $U^{(0)}$, U est celui de rang 1.

D'autre part, on remarque que $\varphi(U) = E(\Delta) - \Delta$ vérifie

$$\Phi_0(U) \leqslant -1, \quad \deg U = n.$$

C'est donc le comma de rang 1 à une équivalence près.

(4) $p \geqslant 3$. L'idée de la démonstration est: étant donné un comma U de rang i de construire un comma de rang strictement plus grand que i en prenant un entier q suffisamment grand.

Cet entier q sera

$$\deg U + [pn/2] \quad \text{si} \quad n \leqslant p-1,$$

$$\deg U + (p+1)n/2 \quad \text{si} \quad n > p-1.$$

Lemme 10. *On pose* $\deg U^{(i)} = u_i$. *Soit* U *le comma construit avec l'entier* q. *Pour montrer que ce comma est de rang strictement supérieur à* i *il suffit de montrer que:*

$$l_q - (q+1) > (p-1)u_i.$$

Preuve. D'après (4) on a:

$$\Phi_0(U) \leqslant -l_q + q + 1$$

donc:

$$\Phi_0(U) < -(p-1)u_i.$$

Puisque:

$$N(U^{(i)}) \geqslant 0,$$

$$\Phi_1(U^{(i)}) = (p-1)u_i.$$

On en déduit que:

$$\Phi_0(U^{(i)}) \geqslant -(p-1)u_i > \Phi_0(U).$$

Lemme 11. *On pose* $\deg U^{(i)} = u_i$ *et on suppose seulement* p *premier* $\geqslant 2$. *Si* $u_i \geqslant (p-1)n - [pn/2]$, *alors on a:*

$$\deg U^{(i+1)} - \deg U^{(i)} \leqslant [pn/2].$$

Preuve. Prenons $q = u_i + [pn/2]$, il suffit alors de montrer que le comma construit avec l'entier q est de rang strictement supérieur à i.

En utilisant le lemme 10 on est conduit à montrer que:

$$l_q - (q+1) > (p-1)u_i.$$

Or d'après (1):

$$l_q = p(q+1) - p(p-1)n/2.$$

On a donc:

$$l_q - (q+1) = (p-1)\left(q + 1 - \frac{pn}{2}\right)$$

$$= (p-1)\left(u_i + \left[\frac{pn}{2}\right] + 1 - \frac{pn}{2}\right) > (p-1)u_i.$$

(a) $p \geqslant n+1$. Si $u_i \geqslant (p-1)n-[pn/2]$ le lemme 11 nous donne l'inégalité cherchée.

Supposons donc $u_i < (p-1)n-[pn/2]$, alors le lemme 10 nous montre qu'il suffit de prouver qu'on a:

$$l_q-(q+1) > (p-1)u_i.$$

Divisons q et u_i par n nous avons:

$$q = jn+r, \quad 0 \leqslant r < n,$$

$$u_i = j_1 n+r_1, \quad 0 \leqslant r_1 < n.$$

Comme nous savons que:

$$q = u_i+[pn/2] < (p-1)n$$

il est clair que:

$$[q/n] = j \leqslant p-2$$

donc

$$l_q = (j+1)(q+1)-j(j+1)n/2$$

et l'inégalité à prouver s'écrit:

$$j(jn+r+1)-j(j+1)n/2 > (p-1)u_i. \tag{5}$$

Nous allons maintenant exprimer j et r en fonction de j_1 et r_1 et nous poserons $p = 2p'+1$.

Nous utiliserons la relation:

$$q = u_i+p'n+[n/2] = (j_1+p')n+r_1+[n/2].$$

Nous avons donc:

$$\begin{aligned} j &= j_1+p'+\varepsilon \\ r &= r_1+[n/2]-\varepsilon n \end{aligned} \quad \text{avec} \quad \varepsilon \in \{0, 1\}.$$

Après cette transformation l'équation (5) devient:

$$\tfrac{1}{2}nj_1^2+(r_1+\theta-p'n)j_1+(p'+\varepsilon)[\tfrac{1}{2}n(p'+\varepsilon)+\theta-\varepsilon n]+r_1(\varepsilon-p') > 0 \tag{6}$$

où l'on pose $\theta = 1+[n/2]-n/2 \in \{1/2, 1\}$.

Il est clair que l'inégalité (6) est entraînée par l'inégalité plus forte obtenue en prenant $\theta = 1/2$:

$$\tfrac{1}{2}nj_1^2+(r_1+\tfrac{1}{2}-p'n)j_1[\tfrac{1}{2}n(p'-\varepsilon)+\tfrac{1}{2}] \tag{7}$$
$$+(p'+\varepsilon)[\tfrac{1}{2}n(p'+\varepsilon)+\tfrac{1}{2}-\varepsilon n]+r_1(\varepsilon-p') > 0.$$

Pour établir l'inégalité (7) nous montrerons que le discriminant Δ' de ce trinôme en j_1 est négatif.

Ce discriminant est:

$$\Delta' = r_1^2+r_1(1-2n\varepsilon)+\tfrac{1}{4}-n(2p'+\varepsilon)+\varepsilon n^2.$$

Premier cas: $\varepsilon = 0$. Cela signifie que $r_1 < n/2$.

On a alors:

$$\frac{\Delta'}{n^2} = \frac{r_1^2}{n^2}+\frac{r_1}{n^2}+\frac{1}{4n^2}-\frac{2p'}{n} < \frac{1}{4}+\frac{1}{2n}+\frac{1}{4n^2}-\frac{2p'}{n} \leqslant \frac{1}{4}+\frac{1}{2n}+\frac{1}{4n^2}-1$$

puisque $p-1 \geqslant n$. On voit donc que $\Delta' < 0$.

Deuxième cas $\varepsilon = 1$. Cela signifie que $r_1 \geqslant n/2$.

On a alors:

$$\frac{\Delta'}{n^2} = \frac{r_1^2}{n^2}+(1-2n)\frac{r_1}{n^2}+\frac{1}{4n^2}-\frac{2p'+1}{n}+1$$

$$< 2+\frac{1-2n}{2n}+\frac{1}{4n^2}-\frac{p}{n} \leqslant 1+\frac{1}{2n}+\frac{1}{4n^2}-\frac{p}{n} \leqslant -\frac{1}{2n}+\frac{1}{4n^2}$$

puisque $p \geqslant n+1$. On voit donc que $\Delta' < 0$.

(b) $p < n+1$. Avec les mêmes notations que dans le (a) on prend:

$$q = u_i+(p+1)n/2$$

et on a:

$$\begin{aligned} j &= j_1+(p+1)/2, \\ r &= r_1. \end{aligned}$$

Il suffit alors de démontrer l'inégalité (5), on montre que celle-ci s'écrit:

$$\frac{n}{2}j_1^2+\left(n+r_1+1-\frac{np}{2}\right)j_1+\frac{p+1}{2}\left(\frac{n(p-1)}{4}+1\right)+r_1\left(\frac{3-p}{2}\right) > 0.$$

Le calcul du discriminant donne:

$$\frac{\Delta'}{n^2} = \left(\frac{r_1}{n}\right)^2+(2-n)\frac{r_1}{n^2}+\frac{5}{4}-p+\frac{1-2p}{n}+\frac{1}{n^2} < 1+\frac{5}{4}-p+\frac{2-2p}{n} < \frac{9}{4}-p < 0$$

puisque $p \geqslant 3$.

Remarque. Dans le cas $p = 3$, l'inégalité

$$\deg U^{(i+1)}-\deg U^{(i)} \leqslant [pn/2]$$

est valable quel que soit $n \geqslant 1$, en effet le lemme 11 s'applique quel que soit $i \geqslant 1$, compte tenu que $u_1 = n$.

(4') On utilise le lemme 11 en remarquant que l'inégalité peut être améliorée car $N(U^{(i)}) \geqslant 1$ puisque $U^{(i)}$ n'est pas solution de l'équation de Pell.

THÉORÈME 10. *On suppose l'hypothèse forte vérifiée.*

A. *L'équation de Pell admet une solution non triviale si et seulement si* $(p-1)P_0-P_1$ *est un élément d'ordre fini l de la jacobienne J, où* $P_0=\infty_0$ *et* $P_1=\infty_1+\ldots+\infty_{p-1}$.

B. *De plus, on a:*

(1) $l=\deg U^{(\pi)}$, *où* $U^{(\pi)}$ *est le comma de rang* π, π *étant la pseudo-période de la suite des commas de* $\mathcal{O}$.

(2) (a) *Si* $p=2$, $\pi+n-1\leqslant l\leqslant 1+\pi(n-1)$,

(b) *Si* $p\geqslant 3$, $\pi+n-1\leqslant l\leqslant n+[pn/2](\pi-1)$ *si* $n\leqslant p-1$,

$\pi+n-1\leqslant l\leqslant n+\big((p+1)n/2\big)(\pi-1)$ *si* $n>p-1$.

Preuve. A. Soit $\varphi(U)\in\mathscr{G}$ tel que $\Phi_0(U)<0$ (ce que l'on peut toujours supposer): on a:

$$\operatorname{div}\varphi=(p-1)\deg U\cdot P_0-\deg U\cdot P_1=\deg U\big((p-1)P_0-P_1\big), \tag{8}$$

et

$$(p-1)P_0-P_1\in\mathscr{M}_0.$$

La réciproque résulte du corallaire 9.

B. (1) En effet si $U^{(\pi)}$ est le comma de rang π, $\varphi(U^{(\pi)})$ est la solution fondamentale telle que $\Phi_0(U^{(\pi)})<0$ et donc d'après (8), $l|\deg U^{(\pi)}$.

Réciproquement soit $\varphi(U)\in\mathscr{G}$ tel que

$$\operatorname{div}\varphi(U)=l\big((p-1)P_0-P_1\big)$$

d'aprés la remarque 1, page 35, on a:

$$v_0(\varphi)=-\deg\varphi=l(p-1)>0,$$

$$v_i(\varphi)=-\deg\varphi_i=-l,\quad i\neq 0,\quad i\in\mathbf{Z}/p\mathbf{Z}$$

on en déduit que $\Phi_0(U)=\deg\varphi<0$ et donc d'après le lemme 9 (b), on a:

$$\Phi_1(U)=(p-1)\deg U=\sum_{i\in\omega_1}\deg\varphi_i=(p-1)l\quad\text{d'où}\quad l=\deg U$$

et comme $\varphi(U^{(\pi)})$ est la solution fondamentale telle que $\Phi_0(U^{(\pi)})<0$, on a:

$$\varphi(U)\sim\big(\varphi(U^{(\pi)})\big)^i,\quad i\geqslant 1$$

et donc

$$\deg U^{(\pi)}|\deg U=l.$$

(2) Pour montrer les inégalités on utilise la proposition 11.

COROLLAIRE 10. *Si* $p=2$ *et* $n=2$, $l=\pi+1$.

Si $p=3$ *et* $n=1$, $l=\pi$.

2.7. Résolution de l'équation de Pell dans le cas: $p=3$, $n=1$, $k=Q$. On pose:

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

et où D est sans racine multiple.

On se propose de donner une réponse au problème suivant:

Trouver tous les triplets (U_0, U_1, U_2), $U_i\in Q[X]$, tels que

$$U_0^3+U_1^3D+U_2^3D^2-3U_0U_1U_2D=Cte\neq 0.$$

Pour cela, nous devons considérer la cubique

$$(\Gamma)\qquad Y^3=X^3+aX+b,\quad (a,b)\neq(0,0)$$

et nous poser la question: le point $2P_0-P_1$ est-il un point d'ordre fini de la courbe Γ?

La cubique (Γ) mise sous forme de Weierstrass est de la forme $Y^2=X^3-D$ où $D\in Q^*$, et d'après G. Bergman [15] cette cubique a comme groupe de torsion sur Q, $\{0\}$ ou $Z/2Z$ ou $Z/3Z$ ou $Z/6Z$.

Nous avons donc trouver les couples (a, b) tels que les commas de rang 1, 2, 3, 6 sont des unités.

P. Toffin et B. Vallée, grâce à un calcul fait sur Mac Syma, ont trouvé les commas de rang 2, 3, 6; en calculant la norme de ces commas, on a pu trouver tous les couples $(a, b)\in Q^2$ tels que l'équation de Pell admet une solution non triviale.

On obtient comme trois premièrs commas:

$$U^{(0)}=(1,0,0),\quad \mathscr{N}\varphi(U^{(0)})=1,$$

$$U^{(1)}=(-X,1,0),\quad \mathscr{N}\varphi(U^{(1)})=aX+b,$$

$$U^{(2)}\sim\big(-9b^2X^2-3ba^2X+a^4,(18b^2+3a^3)X+3ba^2,-9b^2-3a^3\big),$$

$$\mathscr{N}\varphi(U^{(2)})=(-9a^{10}b-135a^7b^3-729a^4b^5-1458ab^7)X+a^{12}-135a^6b^4-729a^3b^6-729b^8.$$

On peut alors chercher les couples (a, b) tels que le coefficient de X dans l'expression $\mathscr{N}\varphi(U^{(i)})=(i=1,2,3,6)$ s'annule.

Nous aurons besoin par la suite de la définition suivante:

Soient (Γ) (resp. (Γ')) la courbe d'équation:

$$Y^3=X^3+aX+b,\quad (a,b)\neq(0,0)$$

resp.

$$Y'^3=X'^3+a'X'+b',\quad (a',b')\neq(0,0).$$

DÉFINITION. On dit que (Γ) et (Γ') sont *équivalentes* si il existe $\lambda \in \boldsymbol{Q}^*$ tel que si $(X, Y) \in \Gamma$ alors $(\lambda X, \lambda Y) \in \Gamma'$, i.e.

$$a' = \lambda^2 \cdot a \quad \text{et} \quad b' = \lambda^3 \cdot b.$$

Explicitons les calculs dans le cas $i = 1$ et $i = 2$.

$i = 1$, les couples (a, b), $(a, b) \neq (0, 0)$, tels que l'équation de Pell admet une solution fondamentale au rang $i = 1$ sont les couples $(0, b)$, $b \in \boldsymbol{Q}^*$; dans ce cas, ou bien b est un cube et alors la longueur de la pseudo-période est égale à la longueur de la période, qui est égale à 1, ou bien b n'est pas un cube et alors la longueur de la pseudo-période est égale à 1.

$i = 2$, les couples (a, b), $(a, b) \neq (0, 0)$ tels que l'équation de Pell admet une solution fondamentale au rang $i = 2$ sont les couples

$$\begin{cases} (a, 0), \ a \in \boldsymbol{Q}^*, \\ (a, b), \ a \text{ et } b \neq 0 \text{ qui satisfont l'équation} \\ \qquad a^9 + 15a^6 b^2 + 8a^3 b^4 + 162 b^6 = 0. \end{cases}$$

Si on pose $t = a^3/b^2$, t doit vérifier l'équation

$$t^3 + 15t^2 + 81t + 162 = 0$$

et comme on a:

$$t^3 + 15t^2 + 81t + 162 = (t+6)(t^2 + 9t + 27)$$

on trouve comme valeurs de (a, b), a et $b \neq 0$,

$$a = -6c^{2\alpha}, \quad b = 6c^{3\alpha}, \quad c \in \boldsymbol{Z}^*, \quad \alpha \in \boldsymbol{N}.$$

Cependant, cette infinité de solutions est à une équivalence près la solution $a = -6$, $b = 6$.

Dans le cas $i = 3$, on trouve les solutions

$$a = -9c^{2\alpha}, \quad b = 9c^{3\alpha}, \quad c \in \boldsymbol{Z}^*, \quad \alpha \in \boldsymbol{N}$$

et donc à une équivalence près, la solution $a = -9$, $b = 9$.

On résume les résultats obtenus dans le tableau suivant:

a	b	solution fondamentale	C^{ic}	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	$\frac{X^3}{3} - 3X + 4 + \left(\frac{-X^2}{3} - X + 2\right)\Delta + \Delta^2$	1	3	3	3

π_1 = longueur de la pseudo-période
π_2 = longueur de la période

Références

[1] E. Artin, *Quadratischer Körper im Gebiet der höheren Kongruenzen I, II*, Math. Zeitschr. 19(1924), p. 153–246.

[2] – *Algebraic Numbers and Algebraic Functions*, Gordon and Breach, 1967.

[3] Z. I. Borevich, I. R. Shafarevich, *Théorie des Nombres*, Gauthier-Villars, 1967.

[4] J. H. Davenport, *On the integration of algebraic functions*, Lecture Notes in Computer Science, N° 102, 1981.

[5] M. Deuring, *Lectures on the theory of algebraic functions of one variable*, Lecture Notes in Math, N° 314, 1973.

[6] E. Dubois et G. Rhin, *Meilleures approximations d'une forme linéaire cubique*, Acta Arith. 40(1982), p. 197–208.

[7] Y. Hellegouarch et M. Lozach, *Equation de Pell et points d'ordre fini*. Colloque "Théorie analytique et élémentaire des nombres", 30 mai–3 juin 83 (à paraître).

[8] Y. Hellegouarch et R. Paysant-Le Roux, *Commas, points extrémaux et arêtes des corps possédant une formule du produit*, C. R. Math. Ac. Sc. Canada 7 (5) (1985).

[9] M. Neubrand, *Einheiten in algebraischen Funktionen und Zahlkörpen*, J. Reine Angew, Math. 303/304 (1978), p. 170–204.

[10] – *Scharen quadratischer Zahlkörper mit gleichgebauten Einheiten*, Acta Arith. 39(1981), pp. 125–132.

[11] R. Paysant-Le Roux, D. L. Mc Quillan, Y. Hellegouarch, *Unités de certains sous-anneaux de corps de fonctions algébriques*, C. R. Math. Ac. Sc. Canada, 7(2) (1985).

[12] A. Schinzel, *On some problems of the arithmetical theory of continued fractions*, Acta Arith. 6(1961), pp. 393–413; 7(1982), pp. 287–298.

[13] H. Schmidt, *Über einheitliche Kettenbruchentwicklungen für die Quadratwurzel aus einem Polynom in einer ganzzahligen Variablen*, Manuskript 1975.

[14] H. J. Stender, *Über die Grundeinheit für spezielle unendliche Klassen reiner kubischer Zahlkörpen*, Abh. Math. Seminar Univ. Hamburg 33(1969), p. 203–215.

[15] G. Bergman, *On the exceptional points of cubic curves*, Arkiv för Matematik 2 (1954), p. 489–535.

[16] N. Bourbaki, *Algèbre commutative*, Chap. 6, Hermann, 1964.

[17] S. Lang, *Abelian Varieties*, Interscience, 1959.

UNIVERSITÉ DE CAEN
DEPARTEMENT DE MATHEMATIQUES ET DE MECANIQUE
14032 Caen Cedex, France

Reçu le 15. 2. 1985
et dans la forme modifiée le 7. 3. 1985 (1494)