J. reine angew. Math. **543** (2002), 169—186

Journal für die reine und angewandte Mathematik

Quelques classes caractéristiques en théorie des nombres

Par *Max Karoubi* à Paris et *Thierry Lambre* à Orsay

Abstract. Let A be a commutative unitary ring. We introduce a Dennis trace map mod n, from $K_1(A;\mathbb{Z}/n)$ to $\Omega^1_{\mathrm{dR}}(A)/(n)$, where $\Omega^1_{\mathrm{dR}}(A)$ is the Kähler-de Rham module of differentials in A. If A is the ring of integers in a number field, explicit elements of $K_1(A;\mathbb{Z}/n)$ are constructed and the values of their Dennis trace mod n are computed. If F is a quadratic field, we obtain in this way non trivial elements of the ideal class group of A. If F is a cyclotomic field, this trace is closely related to Kummer logarithmic derivatives.

Notations. Soient M un groupe et n un entier naturel. On définit $\times n\colon M \to M$ par $\times n(z) = nz$ si le groupe est noté additivement et par $\times n(z) = z^n$ si le groupe est noté multiplicativement. On pose $M_{(n)} = \ker(\times n)$, $M^{(n)} = \mathrm{Im}(\times n)$ et $M/(n) = M/M^{(n)}$. Tous les anneaux et algèbres sont supposés commutatifs et unitaires. Le groupe des unités d'un anneau A est noté $A^\times$.

Introduction

Soient k un anneau et A une k-algèbre. K. Dennis [9], A. Connes [7] et M. Karoubi [10] ont construit des homomorphismes "classes caractéristiques" $D_i\colon K_i(A) \to HH_i(A)$ $(i \geqq 0)$ et $\mathrm{ch}_{i,\ell}\colon K_i(A) \to HC_{i+2\ell}(A)$ ($i \geqq 0$ et $\ell \geqq 0$), de source la K-théorie de A, de but l'homologie de Hochschild de A (pour la trace de Dennis D_i) ou l'homologie cyclique (pour les caractères de Chern $\mathrm{ch}_{i,\ell}$).

Lorsque A est l'anneau des entiers d'un corps de nombres, ces classes caractéristiques sont inopérantes, car trop souvent triviales (dès que i est pair, [12]). En remplaçant la K-théorie usuelle par la K-théorie à coefficients $\mathbb{Z}/n$, nous construisons pour $i = 1$ une classe caractéristique secondaire (cf. 2.3).

Théorème. *Soit A l'anneau des entiers d'un corps de nombres F, de groupe des classes* $\mathrm{Cl}(A)$ *et soit $n \geqq 2$ un entier. Désignons par S le sous-groupe de $\Omega^1_{\mathrm{dR}}(A)$ engendré par $\{a^{-1}\,da, a \in A\} \cup n\Omega^1_{\mathrm{dR}}(A)$. Il existe une classe caractéristique secondaire*

$$d_1^{(n)}\colon \mathrm{Cl}(A)_{(n)} \to \Omega^1_{\mathrm{dR}}(A)/S$$

qui est un morphisme de groupes, non trivial en général.

Cette classe s'avère suffisamment riche pour détecter des éléments de n-torsion du groupe des classes. Des exemples sont proposés pour les corps quadratiques. Dans le cas d'un corps cyclotomique, cette classe caractéristique se trouve reliée aux dérivées logarithmiques de Kummer et aux polynômes de M. Mirimanoff.

Certaines idées de cet article ont été exposées sans démonstration il y a une dizaine d'années par le premier auteur. Elles ont été reprises dans le livre de J. Rosenberg ([17]) en tant qu'exemples d'applications de la K-théorie à la théorie des nombres. Par ailleurs, des généralisations sont possibles, notamment aux anneaux non commutatifs. Ces énoncés plus généraux ont fait l'objet d'une Note aux Comptes Rendus de l'Académie des Sciences de Paris ([11]). Le lecteur trouvera une version plus détaillée du présent texte, avec ses généralisations, dans le serveur de K-théorie (http://www.math.uiuc.edu/K-theory/).

Remerciements. Karim Belabas (Université Paris-Sud) et Thong Nguyen Quang Do (Université de Franche-Comté) ont bien volontiers accepté de lire une version préliminaire de certains passages de ce texte. Nous sommes heureux de les remercier pour leur lecture attentive. Signalons enfin que J. Berrick (National University of Singapore), a construit ([4]) des invariants voisins des nôtres au moyen de "matrices entrelacées".

1. Le groupe de K-théorie relative de l'anneau des entiers d'un corps de nombres

Soient $\mathscr{C}$ et $\mathscr{D}$ deux catégories à produit ([2], pp. 343–375) et soit φ un foncteur additif et cofinal. La catégorie $\mathrm{co}(\varphi)$ est constituée des triplets (C, α, C') où C et C' sont dans $\mathrm{Ob}(\mathscr{C})$ et où α est un isomorphisme dans la catégorie $\mathscr{D}$, de source $\varphi(C)$, de but $\varphi(C')$. Un morphisme de (C, α, C') vers (C_1, α_1, C_1') est un couple (f, f') de morphismes de $\mathscr{C}$ tels que $\alpha_1 \circ \varphi(f) = \varphi(f') \circ \alpha$. L'ensemble des classes d'isomorphismes d'objets de $\mathrm{co}(\varphi)$ est un monoïde abélien de groupe de Grothendieck $K\big(\mathrm{co}(\varphi)\big)$. Le quotient de ce groupe par le sous-groupe N engendré par les éléments de la forme

$$(C, \alpha, C') + (C', \beta, C'') - (C, \beta\alpha, C'')$$

est noté $K(\varphi)$. La classe $(C, \alpha, C') \bmod N$ est notée $[C, \alpha, C']$. La suite exacte de Bass s'écrit:

$$(\star\star) \qquad K_1(\mathscr{C}) \xrightarrow{\varphi_1} K_1(\mathscr{D}) \to K(\varphi) \to K_0(\mathscr{C}) \xrightarrow{\varphi_0} K_0(\mathscr{D}).$$

Soit A un anneau et $n \geqq 2$ un entier. Le foncteur $\bigoplus n$: **Proj**$(A) \to$ **Proj**(A) est défini par $\bigoplus n([P]) = [nP]$ où $nP = P \oplus \cdots \oplus P$ (n facteurs). Le groupe de K-théorie relative $K(\bigoplus n)$, noté $K_1(A; \mathbb{Z}/n)$, s'appelle le (premier) groupe de K-théorie à coefficients. La suite exacte $(\star\star)$ conduit à l'extension

$$(\star) \qquad 1 \to A^\times/(n) \oplus SK_1(A)/(n) \to K_1(A; \mathbb{Z}/n) \xrightarrow{\partial} \tilde{K}_0(A)_{(n)} \to 0.$$

Théorème 1.1. *Soit A l'anneau des entiers d'un corps de nombres F, de groupe des idéaux fractionnaires $I(A)$, de groupe des classes* $\mathrm{Cl}(A)$ *et soit $n \geqq 2$ un entier. Pour $x \in F$, on pose $[x] = x \bmod F^{\times(n)}$ et*

$$\mathscr{U}(A; \mathbb{Z}/n) := \{[x] \in F^\times/(n) \mid \exists I \in I(A), xA = I^n\}.$$

Alors le groupe $K_1(A;\mathbb{Z}/n)$ s'identifie au groupe $\mathscr{U}(A;\mathbb{Z}/n)$ et l'extension $(\star)$ se réduit à la suite exacte

$$(\dagger) \qquad 1 \to A^\times/(n) \to \mathscr{U}(A;\mathbb{Z}/n) \xrightarrow{\partial} \mathrm{Cl}(A)_{(n)} \to 0,$$

l'application ∂ consistant à envoyer $[x]$ sur $[I]$, où I est l'idéal tel que $I^n = xA$.

Démonstration. Introduisons les catégories **Pic**(A) et **Cart**(A) dont les objets respectifs sont les classes d'isomorphismes de A-modules projectifs de rang 1 et les classes d'isomorphismes d'idéaux fractionnaires de A. Notons $\cdot n$: **Cart**$(A) \to$ **Cart**(A) et $\bigotimes n$: **Pic**$(A) \to$ **Pic**(A) les foncteurs définis par $\cdot n([I]) = [I^n]$ et $\bigotimes n([P]) = [P^{\otimes n}]$. L'inclusion **Cart**$(A) \subset$ **Pic**(A) étant une équivalence de catégories, les groupes $K(\cdot n)$ et $K(\bigotimes n)$ sont isomorphes. Montrons que le groupe $K(\cdot n)$ est isomorphe au groupe $\mathscr{U}(A;\mathbb{Z}/n)$. Le groupe $K(\cdot n)$ est constitué des classes d'équivalence $[I,x]$ où I est un idéal fractionnaire de A tel que $I^n = xA$ avec $x \in F$. L'application γ: $K(\cdot n) \to \mathscr{U}(A;\mathbb{Z}/n)$ définie par $\gamma([I,x]) = [x]$ est un morphisme de groupes, clairement surjectif. Si $[x] \in \ker\gamma$, alors $x = y^n$ avec $y \in F^\times$ et $I^n = y^n A$. Par unicité de la décomposition en idéaux premiers dans A, on en déduit $I = yA$, c'est-à-dire $[I,x] = [yA, y^n] = 0$, ce qui montre que γ est un isomorphisme. Montrons à présent que les groupes $K(\bigotimes n)$ et $K_1(A;\mathbb{Z}/n)$ sont isomorphes. Le foncteur **dét**: **Proj**$(A) \to$ **Pic**(A) défini par **dét**$([P]) = [\Lambda^{\mathrm{rg}(P)} P]$ conduit au diagramme

$$\begin{array}{ccccccccc}
A^\times \oplus SK_1(A) & \longrightarrow & A^\times \oplus SK_1(A) & \longrightarrow & K_1(A;\mathbb{Z}/n) & \longrightarrow & \tilde{K}_0(A) & \longrightarrow & \tilde{K}_0(A) \\
\downarrow{\scriptstyle \text{dét}_1} & & \downarrow{\scriptstyle \text{dét}_1} & & \downarrow{\scriptstyle \text{dét}_1^{(n)}} & & \downarrow{\scriptstyle \text{dét}_0} & & \downarrow{\scriptstyle \text{dét}_0} \\
A^\times & \longrightarrow & A^\times & \longrightarrow & K(\bigotimes n) & \longrightarrow & \mathrm{Pic}(A) & \longrightarrow & \mathrm{Pic}(A).
\end{array}$$

L'application dét_0 est un isomorphisme. D'après le théorème de Bass-Milnor et Serre ([3]), on a $SK_1(A) = 0$, ce qui montre que dét_1 est un isomorphisme et par suite $\text{dét}_1^{(n)}$ est également un isomorphisme, cqfd.

Notons $\mathrm{Spec}(A)$ le spectre premier de A. Pour $\mathfrak{p} \in \mathrm{Spec}(A)$, $\hat{A}_\mathfrak{p}$ est le complété $\mathfrak{p}$-adique de l'anneau de valuation discrète $A_\mathfrak{p}$. Notons $\hat{A}$ l'anneau $\prod_{\mathfrak{p} \in \mathrm{Spec}(A)} \hat{A}_\mathfrak{p}$, appelé anneau des adèles restreints de A et notons $\hat{F}$ la somme amalgamée $\hat{A} \otimes_A F$. Rappelons le résultat suivant.

Proposition 1.2. *Soit A l'anneau des entiers d'un corps de nombres F et soit $n \geqq 2$ un entier. Alors le groupe $\mathscr{U}(A;\mathbb{Z}/n)$ s'identifie au sous-groupe $\hat{A}^\times/(n) \cap F^\times/(n)$ de $\hat{F}^\times/(n)$.*

Démonstration. Dans le diagramme

$$\begin{array}{ccc}
\mathscr{U}(A;\mathbb{Z}/n) & \xrightarrow{j} & F^\times/(n) \\
{\scriptstyle \imath}\downarrow & & \downarrow{\scriptstyle \bar{\imath}} \\
\hat{A}^\times/(n) & \xrightarrow[\bar{j}]{} & \hat{F}^\times/(n)
\end{array}$$

les applications $\imath$, j et $\bar{j}$ sont trivialement injectives. Dans l'anneau $\hat{A}$, on s'est restreint aux

places archimédiennes. D'après [1], Chap. X.I, dans cette situation, l'application $\bar{\imath}$ est également injective. Le produit fibré $\hat{A}^\times/(n) \oplus_{\hat{F}^\times/(n)} F^\times/(n)$ est donc égal à $\hat{A}^\times/(n) \cap F^\times/(n)$. Soit $x \in F^\times/(n)$; l'élément $[x] = x \bmod F^{\times(n)}$ de $F^\times/(n)$ appartient à $\hat{A}^\times/(n)$ si et seulement si $n \mid v_\mathfrak{p}(x_\mathfrak{p})$ pour tout $\mathfrak{p} \in \mathrm{Spec}(A)$, c'est-à-dire qu'on a $xA = I^n$ avec I idéal fractionnaire.

Remarque 1.3. Avec les notations de 1.2, l'application induite par $A \to \hat{A}$ en K-théorie à coefficients est l'inclusion $\hat{A}^\times/(n) \cap F^\times/(n) \to \hat{A}^\times/(n)$.

En effet, calculons $K_1(\hat{A}; \mathbb{Z}/n)$. Rappelons pour cela que si $(A_i)_{i\in I}$ est une famille d'anneaux commutatifs de rang stable $d \geqq 2$ au sens de [2], p. 231, on a $K_1\Big(\prod_{i\in I} A_i\Big) \cong \prod_{i\in I} K_1(A_i)$ et $\tilde{K}_0\Big(\prod_{i\in I} A_i\Big) \cong \prod_{i\in I} \tilde{K}_0(A_i)$. Les anneaux de la famille $(\hat{A}_\mathfrak{p})_{\mathfrak{p}\in \mathrm{Spec}(A)}$ sont tous de rang stable $d = 2$. De $\tilde{K}_0(\hat{A}_\mathfrak{p})_{(n)} = 0$ et $K_1(\hat{A}_\mathfrak{p}) = \hat{A}_\mathfrak{p}^\times$, on tire $K_1(\hat{A}) = \hat{A}^\times$. L'extension $(\star)$ nous mène à $K_1(\hat{A}; \mathbb{Z}/p) = \hat{A}^\times/(n)$, cqfd.

Le lemme (N-N_1) ci-après permet de construire des éléments du groupe $\mathscr{U}(A; \mathbb{Z}/n)$.

Soit L/F une extension de corps de nombres de degré ℓ. On pose $A = \mathcal{O}_F$ et on note B la fermeture intégrale de A dans L.

Pour $z \in L$, désignons par $\mu_z : L \to L$ la multiplication par z. Les quantités $N_j(z) \in L$ sont définies par $\det(X\,\mathrm{id}_L - \mu_z) = \sum_{j=0}^{\ell} (-1)^{\ell-j} N_j(z) X^j$. En particulier, $N_\ell(z) = 1$, $N_{\ell-1}(z) = \mathrm{tr}_{L/F}(z)$, $N_0(z) = N_{L/F}(z) = N(z)$.

Proposition 1.4. *Soit $z \in L$ (resp. B) et $h \in F$ (resp. A). Alors on a*

$$N(z+h) = N(z) + N_1(z)h + h^2\varepsilon(z,h) \quad \textit{avec } \varepsilon(z,h) \in F \textit{ (resp. } A).$$

Remarquons qu'on a la formule commode $N_1(z) = \left(\left(\frac{d}{dh}\right)_{h\in F} N(z+h)\right)_{h=0}$.

Lemme (N-N_1) 1.5. *Soient L/F une extension de corps de nombres, A l'anneau des entiers de F et B la fermeture intégrale de A dans L et n un entier $\geqq 2$. Considérons un élément u de B tel que $N(u) = ea^n$ avec $e \in A^\times$, $a \in A$ et $\big(N(u), N_1(u)\big) = A$. En désignant par $[u]$ la classe de u dans $L^\times/(n)$, on a alors $[u] \in \mathscr{U}(B; \mathbb{Z}/n)$.*

Démonstration. L'hypothèse $\big(N(u), N_1(u)\big) = A$ signifie que u est premier à tous ses conjugués. En effet, si $\sigma : L \to \mathbb{C}$ désigne un F-plongement de L (c'est-à-dire $\sigma|_F = \mathrm{id}$), on a $N(u) = \prod_\sigma \sigma(u)$, $N_1(u) = \Big(\prod_\sigma \sigma(u)\Big)\Big(\sum_\sigma \sigma(u)^{-1}\Big)$ et $P_u(X) = \prod_\sigma \big(X - \sigma(u)\big)$. Soit $\mathfrak{p}$ un idéal premier de A. On a $\mathfrak{p} \mid \big(N(u), N_1(u)\big)$ si et seulement si $P_u(X) \equiv X^2 Q(X) \bmod \mathfrak{p}$. Ceci signifie qu'il existe deux plongements σ_1 et σ_2 tels que $\big(\sigma_1(u), \sigma_2(u)\big) \subset \mathfrak{p}$. En posant $\tau = \sigma_1^{-1}\sigma_2$ et $\mathfrak{q} = \sigma_1^{-1}(\mathfrak{p})$, on en déduit $\big(u, \tau(u)\big) \subset \mathfrak{q}$.

Pour montrer que $[u]$ appartient à $K_1(A; \mathbb{Z}/n)$, on remarque que la puissance n-ième de l'idéal fractionnaire $I = (u, a)$ de B est principale. En effet

$$I^n = \big(u^n, N(u)\big) = \Big(u^n, u \prod_{\sigma \neq \mathrm{id}} \sigma(u)\Big);$$

et puisque $\big(u, \sigma(u)\big) = B$, on en déduit $I^n = uB$. Ceci montre $[u] \in \mathscr{U}(B; \mathbb{Z}/n)$, cqfd.

Donnons une première application aux corps quadratiques. L'égalité

$$K_1(A; \mathbb{Z}/n) = \mathscr{U}(A; \mathbb{Z}/n)$$

et le lemme (N-N_1) permettent en effet de retrouver un théorème obtenu par Y. Yamamoto [19] à l'aide de méthodes distinctes.

Théorème 1.6. *Soit F un corps de nombres quadratique d'anneau d'entiers A, de discriminant δ et soit n un entier impair. On suppose qu'il existe deux couples (α, b) et (α', b') dans $\mathbb{Z}^2$ satisfaisant aux relations $\alpha^2 - 4b^n = \alpha'^2 - 4b'^n = \delta$ avec $(\alpha, b) = (\alpha', b') = 1$. On suppose de plus que pour tout diviseur premier p de n, les conditions ci-dessous sont satisfaites.*

a) *α (resp. α') n'est pas une puissance p-ième modulo b (resp. b');*

b) *$(\alpha + \alpha')/2$ est une puissance p-ième modulo b et modulo b'.*

Alors:

Si $\delta < -4$ le groupe des classes de A contient un sous groupe isomorphe à $\mathbb{Z}/n \oplus \mathbb{Z}/n$.

Si $\delta > 0$, le groupe des classes de A contient un sous groupe isomorphe à $\mathbb{Z}/n$.

Démonstration. L'application $f\colon A \to \mathbb{Z}/b$ définie par $f\big((x + y\sqrt{\delta})/2\big) = (x + y\alpha)/2$ est un morphisme d'anneaux. On note $f_1^{(d)}\colon K_1(A; \mathbb{Z}/d) \to K_1(\mathbb{Z}/b; \mathbb{Z}/d)$ l'application induite par f en K-théorie à coefficients d. Remarquons que $K_1(\mathbb{Z}/b; \mathbb{Z}/d) = (\mathbb{Z}/b)^\times/(d)$. L'élément $u = (\alpha + \sqrt{\delta})/2$ de A est de norme $N(u) = b^n$, de trace $\mathrm{tr}(u) = N_1(u) = \alpha$. D'après le lemme ($N$-$N_1$), pour tout diviseur d de n, l'élément $[u] \in F^\times/(d)$ appartient à $K_1(A; \mathbb{Z}/d)$. Soit p un diviseur premier de n. De $f(u) = \alpha$, on déduit $f_1^{(p)}([u]) = [\alpha]$, quantité distincte de 1 d'après l'hypothèse a). Pour tout diviseur premier p de n, l'élément $[u]$ de $K_1(A; \mathbb{Z}/p)$ n'est donc pas trivial. Montrons que $[u] \in F^\times/(n)$ définit un élément d'ordre n de $K_1(A; \mathbb{Z}/n)$. Supposons $[u]$ d'ordre m avec $1 \leqq m < n$. Il existe alors un nombre premier p tel que $mp \mid n$. De $[u]^{n/p} = 1$, on tire $u^{n/p} = z^n$ avec $z \in A^\times$, soit encore $u \in F^{\times(p)}$ et donc $[u]$ trivial dans $K_1(A; \mathbb{Z}/p)$. On vient de montrer que ceci est impossible. On a donc $[u]$ d'ordre n dans $K_1(A; \mathbb{Z}/n)$. Le sous-groupe H de $K_1(A; \mathbb{Z}/n)$ engendré par $[u]$ est donc isomorphe à $\mathbb{Z}/n$.

On introduit de manière analogue $u' = (\alpha' + \sqrt{\delta})/2$ et on obtient de même un sous-groupe H' de $K_1(A; \mathbb{Z}/n)$, également isomorphe à $\mathbb{Z}/n$. Pour montrer la somme directe $H \oplus H'$ dans $K_1(A; \mathbb{Z}/n)$, on remarque que $f(u') = (\alpha' + \alpha)/2 \in \mathbb{Z}/b$. Si $u' \in H$, c'est-à-dire $u' = u^m$ avec $1 \leqq m < n$, l'égalité $f_1^{(p)}([u']) = f_1^{(p)}([u])^m$, satisfaite pour tout diviseur premier p de n, s'écrit encore $[(\alpha + \alpha')/2] = [\alpha]^m$, ce qui donne $[\alpha]^m = 1$ d'après l'hypothèse b). On en déduit comme ci-dessus qu'il existe un nombre premier p tel que $mp \mid n$ pour lequel $\alpha \in (\mathbb{Z}/b)^{\times(p)}$, ce qui fournit la contradiction recherchée. On montre de même $u \notin H'$. En conclusion, sous les hypothèses proposées, le groupe $K_1(A; \mathbb{Z}/n)$ contient un sous-groupe isomorphe à $\mathbb{Z}/n \oplus \mathbb{Z}/n$. De l'extension 1.1 (†), on déduit que si F est imaginaire, $\mathrm{Cl}(A)_{(n)}$

contient $\mathbb{Z}/n \oplus \mathbb{Z}/n$ en facteur direct. Si $\delta > 0$, $A^\times/(n)$ est isomorphe à $\mathbb{Z}/n$ et donc $\mathrm{Cl}(A)_{(n)}$ contient $\mathbb{Z}/n$ en facteur direct.

Remarque 1.7. Dans le cas où F est réel d'unité fondamentale ε telle qu'il existe un diviseur premier p pour lequel $f(\varepsilon) \in (\mathbb{Z}/b)^{\times(p)}$, le groupe des classes contient un sous-groupe isomorphe à $\mathbb{Z}/n \oplus \mathbb{Z}/n$. En effet, soit $t = \partial([u])$ toujours avec $u = (\alpha + \sqrt{\delta})/2$. Montrons que t est d'ordre n dans $\mathrm{Cl}(A)$. Supposons $t^m = 0$ avec $1 \leqq m < n$. On en déduit $[u]^m \in \ker \partial$, soit $u^m = \varepsilon^l$, ce qui donne $[\alpha]^m = f_1^{(p)}([u]^m) = f_1^{(p)}(\varepsilon)^l = 1$ puisque $f(\varepsilon) \in (\mathbb{Z}/b)^{\times(p)}$. On en déduit $\alpha \in (\mathbb{Z}/b)^{\times(p)}$, situation exclue. Le sous-groupe $H(t)$ engendré par t dans $\mathrm{Cl}(A)$ est donc isomorphe à $\mathbb{Z}/n$. La fin de la démonstration est analogue à celle du théorème. Les sous-groupes $H(t)$ et $H(t')$ engendrés respectivement par $t = \partial\big([(\alpha + \sqrt{\delta})/2]\big)$ et $t' = \partial\big([(\alpha' + \sqrt{\delta})/2]\big)$ sont en somme directe dans $\mathrm{Cl}(A)$.

Ces éléments du groupe des classes ont été construits pour la première fois par Yamamoto ([19]). À partir de ces éléments, cet auteur a montré que pour tout $n > 1$, il existe une infinité de corps quadratiques réels et imaginaires dont le groupe des classes contient un facteur $\mathbb{Z}/n$.

Citons une autre application.

Proposition 1.8. *Soit F un corps de nombres d'anneau d'entiers A et soit $n \geqq 2$ un entier naturel. On suppose qu'il existe $z \in A$ tel que $N(z) = \pm b^n$, $\big(N(z), N_1(z)\big) = 1$ et que pour tout diviseur m de n, $1 \leqq m < n$, $\pm b^m$ ne soit pas la norme d'un élément de F. Alors $\mathrm{Cl}(A)_{(n)}$ possède un élément d'ordre n.*

Démonstration. D'après le lemme (N-N_1), $[z]$ appartient à $\mathscr{U}(A; \mathbb{Z}/n)$. Si $[z]$ est d'ordre m, $1 \leqq m < n$, il existe $u \in F^\times$ tel que $z^m = u^n$, c'est-à-dire $z = \mu u^s$ avec $s = n/m$ et $\mu \in \mu_m(F)$. L'équation $N(z) = N(u)^s$ s'écrit $b^m = \pm N(u)$, ce qui n'est pas. Notons $\partial\colon \mathscr{U}(A; \mathbb{Z}/n) \to \mathrm{Cl}(A)_{(n)}$ et supposons à présent que $\partial([z]) = 0$. Dans ce cas, il existe $u \in F^\times$, $\xi \in \mu$ et des entiers l_i tels que $z = \xi^{l_0} \varepsilon_1^{l_1} \cdots \varepsilon_r^{l_r} u^n$, d'où l'on déduit $N(z) = \pm N(u)^n$ soit $b = \pm N(u)$, ce qui n'est pas.

Pour les corps quadratiques, cette proposition prend la forme suivante.

Proposition 1.9. *Soit F un corps quadratique d'anneau d'entiers A et de discriminant δ et soit n un entier impair. On suppose qu'il existe $(\alpha, b) \in \mathbb{Z}^2$ tel que $\alpha^2 - 4b^n = \delta$, avec $(\alpha, b) = 1$. On suppose de plus que pour tout diviseur m de n $(1 \leqq m < n)$, et pour tout entier β, la quantité $\delta\beta^2 \pm 4b^m$ n'est pas un carré parfait. Alors il existe un élément d'ordre n dans $\mathrm{Cl}(A)_{(n)}$.*

Démonstration. On applique la proposition 1.8 à l'entier $z = (\alpha + \sqrt{\delta})/2$. L'équation $\pm b^m = N(u)$ conduit à $\delta\beta^2 \pm 4b^n$ carré parfait.

Exemples 1.10.

$$n = 9, \quad \alpha = 1, \quad b = 3, \quad \delta = 1^2 - 4 \cdot 3^9 = -78\,731.$$

$$n = 15, \quad \alpha = 1, \quad b = 4, \quad \delta = 1^2 - 4 \cdot 4^{15} = -4\,294\,967\,295.$$

$$n = 21, \quad \alpha = 17, \quad b = 4, \quad \delta = 17^2 - 4 \cdot 4^{21} = -17\,592\,186\,044\,127.$$

2. La trace de Dennis relative

Soient k un anneau et A une k-algèbre. Pour tout entier $r \geqq 0$, K. Dennis ([9]) a construit un morphisme $D_r\colon K_r(A) \to HH_r(A)$, où $HH_*(A)$ est le k-module gradué d'homologie de Hochschild de A. Rappelons que si $r = 0$ et $[P] \in K_0(A)$, on a $D_0([P]) = \mathrm{rg}(P, \mathscr{S}) \bmod [A, A]$, où $\mathscr{S} = (x_j, \varphi_j)_{1 \leqq j \leqq r}$ est un système de coordonnées sur P ([5], II. 46). Nous supposons comme toujours A commutative. Désignons par $\Omega^1_{\mathrm{dR}}(A)$ le A-module des différentielles de Kähler de A. Pour $x = [P, \alpha] \in K_1(A)$, on a $D_1(x) = \det(\alpha)^{-1}\, d\big(\det(\alpha)\big)$. En écrivant $K_1(A) = A^\times \oplus SK_1(A)$, on en déduit que la restriction de D_1 à $SK_1(A)$ est nulle et que la restriction de la trace de Dennis à $A^\times$ est la dérivée logarithmique, c'est-à-dire que pour $u \in A^\times$, on a $D_1(u) = u^{-1}\, du$.

La notion de connexion sur un module P, projectif et de type fini, permet de définir la trace de Dennis relative. Rappelons ([7], [10]) qu'une application k-linéaire

$$\nabla\colon P \to P \otimes_A \Omega^1_{\mathrm{dR}}(A)$$

est une connexion si elle satisfait $\nabla(xa) = \nabla(x)a + x\, da$ avec $x \in P$ et $a \in A$.

Soit $\mathscr{S} = (x_j, \varphi_j)_{1 \leqq j \leqq r}$ un système de coordonnées sur P ([5], II. 46). La connexion de Levi-Civita de P est l'application $d_{P,\mathscr{S}}\colon P \to P \otimes_A \Omega^1_{\mathrm{dR}}(A)$ définie pour $x = \sum_{j=1}^{r} x_j \varphi_j(x)$ par $d_{P,\mathscr{S}}(x) = \sum_{j=1}^{r} x_j\, d\varphi_j(x)$. Ceci montre qu'on peut toujours construire une connexion sur un module projectif de type fini.

Soient P et Q deux A-modules projectifs de type fini et soit $\alpha\colon P \to Q$ une application A-linéaire. Soient ∇ et ∇' des connexions sur P et Q respectivement. On définit l'application A-linéaire $d\alpha = d(\alpha, \nabla, \nabla')$ de source P, de but $Q \otimes_A \Omega^1_{\mathrm{dR}}(A)$ par

$$d(\alpha, \nabla, \nabla') = \nabla' \circ \alpha - (\alpha \otimes \mathrm{id}) \circ \nabla.$$

Supposons de plus que α soit un isomorphisme de A-module. En choisissant des systèmes de coordonnées sur P et Q, l'application A-linéaire

$$\alpha^{-1}\, d\alpha := (\alpha^{-1} \otimes \mathrm{id}) \circ d(\alpha, \nabla, \nabla')$$

admet une matrice carrée à coefficients dans $\Omega^1_{\mathrm{dR}}(A)$ dont la trace est notée $\mathrm{tr}(\alpha^{-1}\, d\alpha)$.

Théorème 2.1. *Soient k un anneau, A une k-algèbre et $n \geqq 2$ un entier. Soit $D_1^{(n)}\colon K_1(A; \mathbb{Z}/n) \to \Omega^1_{\mathrm{dR}}(A)/(n)$ l'application définie pour $x = [P, \alpha, Q]$ dans $K_1(A; \mathbb{Z}/n)$ par $D_1^{(n)}(x) = \mathrm{tr}\big(\alpha^{-1} \circ d(\alpha, n\nabla, n\nabla')\big) \bmod n\Omega^1_{\mathrm{dR}}(A)$, où ∇ et ∇' sont des connexions sur P et Q respectivement. Alors l'application $D_1^{(n)}$ est un morphisme de groupes.*

Démonstration. On a $K_1(A; \mathbb{Z}/n) = K\big(\mathrm{co}(\bigoplus n)\big)/N$. Soit (P, α, Q) un objet de $\mathrm{co}(\bigoplus n)$. Si ∇ est une connexion sur P et si ∇' et ∇'_1 sont deux connexions sur Q, on a $\alpha^{-1} \circ d(\alpha, n\nabla, n\nabla') - \alpha^{-1} \circ d(\alpha, n\nabla, n\nabla'_1) = \alpha^{-1} \circ n(\nabla' - \nabla'_1) \circ \alpha$, application A-linéaire dont

la trace, égale à celle de $n(\nabla' - \nabla'_1)$, est bien congrue à 0 modulo $n\Omega^1_{dR}(A)$. Ceci montre que pour $(P, \alpha, Q) \in \mathrm{Ob}\big(\mathrm{co}(\bigoplus n)\big)$, le choix des connexions sur Q n'intervient pas pour la définition de $\mathrm{tr}(\alpha^{-1}\, d\alpha)$ modulo $n\Omega^1_{dR}(A)$. Par un argument analogue, on s'assure que cette trace modulo $n\Omega^1_{dR}(A)$ ne dépend pas du choix de la connexion sur P. Nous omettons à présent de préciser les connexions choisies.

Si les objets (P, α, Q) et (P_1, α_1, Q_1) sont isomorphes dans la catégorie $\mathrm{co}(\bigoplus n)$, il existe des applications A-linéaires f et g telles que $\alpha_1 = ng \circ \alpha \circ nf^{-1}$. Un rapide calcul donne

$$\mathrm{tr}(\alpha_1^{-1}\, d\alpha_1) = n\,\mathrm{tr}(g^{-1}\, dg) + \mathrm{tr}(\alpha^{-1}\, d\alpha) + n\,\mathrm{tr}(f\, df^{-1})$$

soit $\mathrm{tr}(\alpha_1^{-1}\, d\alpha_1) \equiv \mathrm{tr}(\alpha^{-1}\, d\alpha) \bmod n\Omega^1_{dR}(A)$, ce qui montre que seule la classe d'isomorphie de l'objet (P, α, Q) intervient pour la définition de la trace à coefficients. Enfin, les relations banales

$$\mathrm{tr}\big((\alpha_1 \oplus \alpha_2)^{-1}\, d(\alpha_1 \oplus \alpha_2)\big) = \mathrm{tr}(\alpha_1^{-1}\, d\alpha_1) + \mathrm{tr}(\alpha_2^{-1}\, d\alpha_2)$$

et $\mathrm{tr}\big((\alpha\beta)^{-1}\, d(\alpha\beta)\big) = \mathrm{tr}(\alpha^{-1}\, d\alpha) + \mathrm{tr}(\beta^{-1}\, d\beta)$ montrent qu'on a un morphisme de groupes $D_1^{(n)}$ de source $K_1(A; \mathbb{Z}/n)$ de but $\Omega^1_{dR}(A)/(n)$ en posant

$$D_1^{(n)}([P, \alpha, Q]) = \mathrm{tr}(\alpha^{-1}\, d\alpha) \bmod n\Omega^1_{dR}(A).$$

Exemple 2.2. On suppose $K_0(A) = \mathbb{Z}$. Alors

$$K_1(A; \mathbb{Z}/n) = K_1(A)/(n) = A^\times/(n) \oplus SK_1(A)/(n).$$

La restriction de la trace de Dennis $D_1^{(n)}$ au facteur $SK_1(A)/(n)$ est nulle tandis que la restriction de la trace de Dennis $D_1^{(n)}$ au facteur $A^\times/(n)$ est donnée par

$$D_1^{(n)}([a]) = a^{-1}\, da \bmod n\Omega^1_{dR}(A).$$

Cette situation s'applique en particulier lorsque A est local.

Pour tout anneau, l'image de $K_1(A)$ par la trace de Dennis D_1 est le sous-groupe $dA^\times/A^\times$ de $\Omega^1_{dR}(A)$ engendré par $\{u^{-1}\, du, u \in A^\times\}$. Notons ∂ le connectant introduit en 1 ($\star$). Du théorème 2.1, on déduit:

Corollaire 2.3. *Soient A une k-algèbre et $n \geqq 2$ un entier. On désigne par $dA^\times/A^\times$ le sous-groupe de $\Omega^1_{dR}(A)$ engendré par $\{u^{-1}\, du, u \in A^\times\}$. Soit S le sous-groupe de $\Omega^1_{dR}(A)$ engendré par $n\Omega^1_{dR}(A)$ et $dA^\times/A^\times$. La "classe caractéristique secondaire"*

$$d_1^{(n)} \colon \tilde{K}_0(A)_{(n)} \to \Omega^1_{dR}(A)/S$$

définie pour $x = \partial(y) \in \tilde{K}_0(A)_{(n)}$ par $d_1^{(n)}(x) = D_1^{(n)}(y) \bmod S$ est un morphisme de groupes abéliens, non trivial en général.

La trace de Dennis relative de l'anneau A des entiers d'un corps de nombres F admet une expression locale assez simple. Notons $\mathscr{R} \subset \mathrm{Spec}(A)$ l'ensemble des idéaux premiers de

A au-dessus des idéaux premiers ramifiés de $\mathbb{Z}$ dans A (on a $\mathfrak{p} \in \mathscr{R}$ lorsque $\mathfrak{p} \cap \mathbb{Z}$ est un nombre premier ramifié dans A). Si $\mathfrak{p} \notin \mathscr{R}$, il est bien connu que $\Omega^1_{\mathrm{dR}}(A_\mathfrak{p}) = 0$. Il en résulte $\Omega^1_{\mathrm{dR}}(A) \cong \bigoplus_{\mathfrak{p} \in \mathscr{R}} \Omega^1_{\mathrm{dR}}(A_\mathfrak{p})$. L'application $i'_\mathfrak{p}\colon A \to A_\mathfrak{p}$ induit une application

$$i_\mathfrak{p}\colon \mathscr{U}(A; \mathbb{Z}/n) \to \mathscr{U}(A_\mathfrak{p}; \mathbb{Z}/n) \cong A_\mathfrak{p}^\times/(n).$$

L'application $i := \bigoplus_{\mathfrak{p} \in \mathscr{R}} i_\mathfrak{p}$ s'insère dans le diagramme commutatif suivant:

$$\begin{array}{ccc} \mathscr{U}(A; \mathbb{Z}/n) & \xrightarrow{D_1^{(n)}} & \Omega^1_{\mathrm{dR}}(A)/(n) \\ \Big\downarrow{\scriptstyle i} & & \Big\downarrow{\scriptstyle j} \\ \bigoplus_{\mathfrak{p} \in \mathscr{R}} \mathscr{U}(A_\mathfrak{p}; \mathbb{Z}/n) & \xrightarrow[\bigoplus_\mathfrak{p} D^{(n)}_{1,\mathfrak{p}}]{} & \bigoplus_{\mathfrak{p} \in \mathscr{R}} \Omega^1_{\mathrm{dR}}(A_\mathfrak{p})/(n) \end{array}$$

où j est un isomorphisme. D'après 2.2, on a $D^{(n)}_{1,\mathfrak{p}}([u_\mathfrak{p}]) = u_\mathfrak{p}^{-1}\, du_\mathfrak{p} \bmod n\Omega^1_{\mathrm{dR}}(A_\mathfrak{p})$. Cette formule conduit au résultat suivant.

Proposition 2.4. *Soit u un élément de A satisfaisant aux hypothèses du lemme $(N\text{-}N_1)$. On suppose de plus que $N(u)$ est premier à n. Posons $v = \prod_{\sigma \neq \mathrm{id}} \sigma(u)$. Alors*

$$D_1^{(n)}([u]) = N(u)^{-1} v\, du \bmod n\Omega^1_{\mathrm{dR}}(A).$$

Démonstration. Par commutativité du diagramme, on a

$$j\big(D_1^{(n)}([u])\big) = \big(D^{(n)}_{1,\mathfrak{p}}([u_\mathfrak{p}])\big)_{\mathfrak{p} \in \mathscr{R}},$$

quantité égale à $j\big(N(u)^{-1} v\, du\big)$, ce qui suffit puisque j est un isomorphisme.

Lorsque l'anneau A possède "peu" d'unités, la proposition suivante permet de détecter des éléments non triviaux du groupe des classes.

Proposition 2.5. *Soit F un corps de nombres d'anneaux d'entiers A. On pose $r = r_1 + r_2 - 1$ et $A^\times = \mu \times \prod_{i=1}^{r} \mathbb{Z}\varepsilon_i$. Soit n un diviseur du discriminant du corps F.*

On suppose:

1) *Pour tout $\xi \in \mu$, $\xi^{-1}\, d\xi \equiv 0 \bmod n\Omega^1_{\mathrm{dR}}(A)$.*

2) *Pour tout i, $1 \leqq i \leqq r$, $\varepsilon_i^{-1}\, d\varepsilon_i \equiv 0 \bmod n\Omega^1_{\mathrm{dR}}(A)$.*

3) *Il existe $u \in A$ avec $N(u) = b^n$, $\big(N(u), N_1(u)\big) = 1$, et $u^{-1}\, du \not\equiv 0 \bmod n\Omega^1_{\mathrm{dR}}(A)$.*

Alors $\mathrm{Cl}(A)_{(n)} \neq 0$.

Démonstration. Les hypothèses 1 et 2 montrent que $dA^\times/A^\times \equiv 0 \bmod n\Omega^1_{\mathrm{dR}}(A)$. L'application $d_1^{(n)}$, de source $\mathrm{Cl}(A)_{(n)}$ est donc de but $\Omega^1_{\mathrm{dR}}(A)/(n)$. D'après le lemme $(N\text{-}N_1)$, les hypothèses 3 fournissent l'élément $[u] = u \bmod F^{\times(n)}$ de $K_1(A; \mathbb{Z}/n)$. De cet élément, on

déduit $x = \partial([u])$ dans $\mathrm{Cl}(A)_{(n)}$. On a $d_1^{(n)}(x) = u^{-1}\,du \bmod n\Omega^1_{\mathrm{dR}}(A)$, quantité non nulle par hypothèse, ce qui montre que x est non trivial.

Exemple 2.6. Posons $x = \sqrt[3]{182}$ et soit $F = \mathbb{Q}[x]$, d'anneau d'entiers $A = \mathbb{Z}[x]$, d'unité fondamentale $\varepsilon = 17 - 3x$. Pour $p = 3$, l'élément $u = 5 - 2x$ définit un élément non nul de $\mathrm{Cl}(A)_{(p)}$.

Donnons d'autres exemples construits sur des corps quadratiques. Soit F un corps quadratique de discriminant δ, d'anneau d'entiers A. Si $\delta < 0$, on exclut systématiquement les deux cas $\delta = -3$ et $\delta = -4$ pour lesquels le groupe des classes est trivial et le groupe des unités n'est pas réduit à $\mathbb{Z}/2$. On pose $\omega = \sqrt{\delta}/2$ ou $(1 + \sqrt{\delta})/2$ suivant que $\delta \equiv 0$ ou $1 \bmod 4$. Soit n un diviseur impair de δ. On a $\Omega^1_{\mathrm{dR}}(A)/(n) \cong \mathbb{Z}/n\,d\omega$ avec $\omega\,d\omega = d\omega/2$ si $\delta \equiv 1 \bmod 4$ et $\omega\,d\omega = 0$ sinon. Si $z = (\alpha + \beta\sqrt{\delta})/2$ est un entier de F, on vérifie la relation $z^{-1}\,dz \equiv 2\beta/\alpha\,d\omega \bmod n\Omega^1_{\mathrm{dR}}(A)$. Si $\delta < 0$ ou si $\delta > 0$ est d'unité fondamentale $\varepsilon = (\varepsilon_1 + \varepsilon_2\sqrt{\delta})/2$ avec $\varepsilon_2 \equiv 0 \bmod n$, on a $dA^\times/A^\times \equiv 0 \bmod n\Omega^1_{\mathrm{dR}}(A)$. On en déduit $\Omega^1_{\mathrm{dR}}(A)/S \cong \Omega^1_{\mathrm{dR}}(A)/(n)$. La classe caractéristique secondaire 2.3 s'écrit

$$d_1^{(n)} \colon \mathrm{Cl}(A)_{(n)} \to \mathbb{Z}/n\,d\omega.$$

Si $u = (\alpha + \beta\sqrt{\delta})/2$ est un élément de A tel que $(\beta, n) = (\alpha, n) = 1$, alors

$$u^{-1}\,du \equiv 2\beta/\alpha\,d\omega \bmod n$$

est une quantité non nulle de $\mathbb{Z}/n\,d\omega$. De tout ceci, on déduit que la proposition 2.5 prend la forme:

Proposition 2.7. *Soit F un corps quadratique de discriminant δ (avec $\delta \neq -3$ ou -4) et d'anneau d'entiers A. Soit n un diviseur impair de δ. Si F est réel, on suppose que l'unité fondamentale $\varepsilon = (\varepsilon_1 + \varepsilon_2\sqrt{\delta})/2$ est telle que n divise ε_2. Soit $(\alpha, \beta, b) \in \mathbb{Z}^3$ une solution de l'équation $\alpha^2 - 4b^n = \delta\beta^2$ avec $(b, \alpha) = (\beta, n) = (\alpha, n) = 1$. Alors $\mathrm{Cl}(A)$ possède un élément d'ordre n.*

En se restreignant aux éléments u de la forme $(\alpha + \sqrt{\delta})/2$, on obtient

Proposition 2.8. *Soient α, b et n trois entiers avec n impair, $(\alpha, b) = (\alpha, n) = 1$. On pose $\delta = \alpha^2 - 4b^n$. On suppose que n divise δ et que δ est le discriminant d'un corps quadratique F d'anneau d'entiers A. Si δ est positif, on suppose de plus que l'unité fondamentale $\varepsilon = (\varepsilon_1 + \varepsilon_2\sqrt{\delta})/2$ de A est telle que n divise ε_2. Alors $\mathrm{Cl}(A)_{(n)}$ possède un élément d'ordre n.*

Exemples 2.9.

$$n = 3, \quad \alpha = 17, \quad b = -2, \quad \delta = 17^2 - 4 \cdot (-2)^3 = 231, \quad \varepsilon_1 = 430, \quad \varepsilon_2 = 24.$$

$$n = 15, \quad \alpha = 1, \quad b = 4, \quad \delta = 1^2 - 4 \cdot 4^{15} = -4\,294\,967\,295.$$

3. La trace de Dennis relative du corps cyclotomique

Soit p un nombre premier impair et soit $\zeta = \zeta_p$ une racine primitive p-ième de l'unité. Le corps cyclotomique $F = \mathbb{Q}[\zeta]$ est une extension galoisienne de degré $p - 1$ de $\mathbb{Q}$, de groupe de Galois $G = (\mathbb{Z}/p)^\times$. Soit g un générateur de G. On désigne par s, $1 < s \leqq p - 1$,

l'entier tel que $g\zeta = \zeta^s$. La conjugaison complexe $g^{(p-1)/2}$ est notée σ. L'anneau A des entiers de F est $\mathbb{Z}[\zeta]$. Soient $\mathrm{Cl}(A)$ le groupe des classes de A et $h = h_p$ le nombre de classes de A. Le sous-corps maximal réel $\mathbb{Q}[\zeta + \zeta^{-1}]$ de F a pour nombre de classes h^+. On sait que $h^+|h$ et que h^+ est le nombre de classes de A invariantes par conjugaison complexe. La p-torsion du groupe des classes $\mathrm{Cl}(A)$ se décompose en $\mathrm{Cl}(A)_{(p)} = \mathrm{Cl}(A)^-_{(p)} \oplus \mathrm{Cl}(A)^+_{(p)}$ avec $\mathrm{Cl}(A)^{\pm}_{(p)} = \ker(\sigma \mp \mathrm{id})$. On sait que si p^a désigne le nombre d'éléments de $\mathrm{Cl}(A)^-_{(p)}$, alors p^a divise $h^- = h/h^+$. Posons $\mathscr{U}_p := \mathscr{U}(\mathbb{Z}[\zeta_p]; \mathbb{Z}/p)$.

La conjugaison complexe sur A définit une involution toujours notée σ sur $\mathscr{U}_p$. L'extension 1.1 (†) se scinde en deux parties dont la partie antisymétrique s'écrit

$$(\dagger^-) \qquad 1 \to \mu_p \to \mathscr{U}_p^- \xrightarrow{\partial} \mathrm{Cl}(A)^-_{(p)} \to 1$$

avec $\mathscr{U}_p^- = \ker(\sigma + \mathrm{id})$. On pose $d_p^- := \dim_{\mathbb{Z}/p} \mathrm{Cl}(A)^-_{(p)} = \dim_{\mathbb{Z}/p} \mathscr{U}_p^- - 1$.

Rappelons qu'un nombre premier p est *régulier* s'il ne divise pas le nombre de classes h_p. On en déduit $d_p^- = 0$. Réciproquement, si $d_p^- = 0$, p ne divise pas h_p^- d'après un théorème de Kummer ([18], 5.6), ceci entraîne que p ne divise pas h_p^+ et donc p est régulier.

On dit que (p, a, b, c) satisfont aux hypothèses du premier cas du dernier théorème de Fermat (en abrégé DTF1) si p est un nombre premier impair et si $a^p = b^p + c^p$ avec $(a, b, c) = (p, abc) = 1$ (on parle du second cas si p divise abc). Nous allons montrer qu'une solution (p, a, b, c) à DTF1 permet de construire un élément z de $\mathscr{U}_p^-$ dont la trace de Dennis relative est non triviale. On en déduit $d_p^- \geqq 1$, ce qui conduit au théorème de Kummer 3.4.

Au vocabulaire près, le résultat suivant est connu.

Proposition 3.1. *Soit (p, a, b, c) une solution à* DTF1. *Pour $1 \leqq \ell \leqq (p-1)/2$, les éléments $z_\ell = (a - b\zeta^{s^\ell})(a - b\zeta^{-s^\ell})^{-1}$ de F sont tels que $[z_\ell] = z_\ell \bmod F^{\times(n)}$ appartiennent à $\mathscr{U}_p^-$.*

Démonstration. Sous les hypothèses DTF1, les idéaux fractionnaires principaux $(a - b\zeta^\ell)$, $1 \leqq \ell \leqq p-1$ sont deux à deux premiers entre eux. On en déduit que chacun de ces idéaux s'écrit sous la forme $(a - b\zeta^\ell) = I_\ell^p$, où les I_ℓ sont des idéaux fractionnaires. Par conséquent, pour $1 \leqq \ell \leqq p-1$, les éléments $a - b\zeta^\ell \bmod F^{\times(p)}$ appartiennent à $\mathscr{U}_p$, cqfd.

Effectuons une réduction modulo p. Pour cela soit $\varphi\colon A \to A/p$ la projection canonique. Posons $\lambda = 1 - \varphi(\zeta)$. Alors $A/(p) = \mathbb{Z}/p[\lambda]$ avec $\lambda^{p-1} = 0$. De $A/(p)$ local, on tire $K_1(A/p; \mathbb{Z}/p) = (A/p)^\times/(p) = (1 + \lambda\mathbb{Z}/p[\lambda], \times)$. Par ailleurs, $\Omega^1_{\mathrm{dR}}\big(A/(p)\big) = \mathbb{Z}/p[\lambda]\, d\lambda$ avec $\lambda^{p-2}\, d\lambda = 0$.

Proposition 3.2. *Soit p un nombre premier impair et soit x un élément de $(\mathbb{Z}/p)\backslash\{0, 1\}$. On pose $y = x - 1$ et on considère les éléments $w = x - y(1-\lambda)$ et $\sigma(w) = x - y(1-\lambda)^{-1}$ de $(A/p)^\times$. Soit $z' = z'(x)$ l'élément de $K_1^-(A/p; \mathbb{Z}/p)$ défini par $z' = w/\sigma(w) \bmod (A/p)^{\times(p)}$. Alors, si $x \in \mathbb{Z}/p\backslash\{0, 1, 1/2\}$, l'élément $z'(x)$ ci-dessus de $K_1^-(A/p; \mathbb{Z}/p)$ n'est pas colinéaire à l'élément $1 - \lambda$.*

Démonstration. On compare les traces $D_1^{(p)}\big(z'(x)\big)$ et $D_1^{(p)}(1-\lambda)$. On a

$$D_1^{(p)}\big(z'(x)\big) = w^{-1}\, dw - \sigma(w)^{-1}\, d\sigma(w).$$

Puisque $w = 1 + y\lambda$, on a $w^{-1} = \sum_{k \geqq 0} (-1)^k y^k \lambda^k$, $dw = y\,d\lambda$ et

$$w^{-1}\,dw = \sum_{k \geqq 0} (-1)^k y^{k+1} \lambda^k\,d\lambda.$$

De $\sigma(w) = \dfrac{1-\lambda x}{1-\lambda}$, on déduit $\sigma(w)^{-1} = 1 + \sum_{k \geqq 1} x^{k-1} y \lambda^k$ tandis que $d\sigma(w) = -y \sum_{k \geqq 1} k\lambda^{k-1}\,d\lambda$ et par suite

$$\sigma(w)^{-1}\,d\sigma(w) = -y\,d\lambda - y(y+2)\lambda\,d\lambda - y(3+2y+xy)\lambda^2\,d\lambda + o(\lambda^2)\,d\lambda,$$

où par commodité, $o(\lambda^j)$ désigne un élément indéterminé de $\lambda^{j+1}\mathbb{Z}/p[\lambda]$. Ces expressions de $w^{-1}\,dw$ et $\sigma(w)^{-1}\,d\sigma(w)$ conduisent à

$$D_1^{(p)}\big(z'(x)\big) = 2y\,d\lambda + 2y\lambda\,d\lambda + (3y + 3y^2 + 2y^3)\lambda^2\,d\lambda + o(\lambda^2)\,d\lambda.$$

Par ailleurs $D_1^{(p)}(1-\lambda) = -(1-\lambda)^{-1}\,d\lambda = -\sum_{k \geqq 0} \lambda^k\,d\lambda$. Supposons $z'(x)$ et $1-\lambda$ colinéaires. La comparaison des coefficients en $d\lambda$ et en $\lambda^2\,d\lambda$ des traces de Dennis de $z'(x)$ et $1-\lambda$ conduit à l'égalité $2y^3 + 3y^2 + y = 0$. Puisque $y \neq 0$, on en déduit que $y \in (\mathbb{Z}/p)^\times$ est solution de l'équation $2X^2 + 3X + 1 = 0$ dans $\mathbb{Z}/p$. Ceci conduit à $y = -1$ ou $y = -1/2$. Or nécessairement $y \neq -1$ car sinon $x = 0$, ce qui est exclu. Par ailleurs, $y = -1/2$ équivaut à $x = 1/2$, situation également exclue, cqfd.

Proposition 3.3. *Soit (p, a, b, c) une solution à* DTF1 *avec $p > 3$. Alors $d_p^- \geqq 1$.*

Démonstration. Désignons par $\varphi_1 : \mathscr{U}_p \to K_1(A/p; \mathbb{Z}/p)$ l'application induite par φ en K-théorie à coefficients. Avec les notations de la proposition précédente, l'élément $z = (a - b\zeta)(a - b\zeta^{-1})^{-1}$ de F est tel que $\varphi_1([z]) = z'(x)$ avec $x = \bar{a}/\bar{c}$. On a nécessairement $x \neq 0$. Si $x = 1/2$, l'élément $z_1 = (a - c\zeta)(a - c\zeta^{-1})^{-1}$ est tel que $\varphi_1([z_1]) = z'(x_1)$ avec $x_1 = \bar{a}/\bar{b}$. Les hypothèses DTF1 montrent que pour $p > 3$, il est impossible d'avoir simultanément $x = x_1 = 1/2$. La proposition précédente s'applique donc pour l'un des deux éléments z ou z_1, cqfd.

On a remarqué plus haut que $d_p^- = 0$ caractérise les nombres premiers réguliers. On a donc montré:

Corollaire 3.4 (Kummer, 1847)**.** *Soit p un nombre premier régulier. Alors le premier cas du dernier théorème de Fermat est satisfait pour p.*

4. Un calcul de dérivée logarithmique

Soit p un nombre premier impair et soit R' l'anneau $\mathbb{Z}[X]/(X^p - 1) = \mathbb{Z}[t]$ avec $t = X \bmod (X^p - 1)$. Le groupe $G = (\mathbb{Z}/p)^\times$ opère dans R' par $gt = t^s$ (avec g générateur de G et $(s, p) = 1$). Le groupe de K-théorie relative de l'anneau $R = R'/(p)$ est $K_1(R; \mathbb{Z}/p) = \big(1 + (1-t)\mathbb{Z}/p[1-t], \times\big)$. Le module des différentielles de Kähler $\Omega^1_{\mathrm{dR}}(R)/(p)$ est isomorphe à $\mathbb{Z}/p[X]\,dX/(X-1)^p\,dX$.

Dans ce paragraphe, x désigne un élément de $\mathbb{Z}/p \backslash \{0, 1\}$ et $y = x - 1$.

On considère le sous-espace vectoriel $V(x)$ de $K_1(R;\mathbb{Z}/p)$ engendré par l'orbite de $(x-yt)(x-yt^{-1})^{-1}$ sous l'action de G. La trace de Dennis relative permet de minorer la dimension de $V(x)$ (cf. 4.8).

L'action de G sur $\Omega^1_{\mathrm{dR}}(R)$ est donnée par $g(t^i\,dt) = g(t)^i\,dg(t) = st^{s(i+1)-1}\,dt$. Pour $1 \leqq k \leqq p-1$, les relations

$$g(t^{s^k}t^{-1}\,dt) = st^{s^{k+1}}t^{-1}\,dt, \quad \sigma(t^{s^k}t^{-1}\,dt) = -t^{-s^k}t^{-1}\,dt$$

et

$$g(t^{-1}\,dt) = st^{-1}\,dt, \quad \sigma(t^{-1}\,dt) = -t^{-1}\,dt$$

conduisent à la décomposition commode suivante.

Proposition 4.1. *Posons* $f_0^- = t^{-1}\,dt$, *et pour* $1 \leqq \ell \leqq (p-1)/2$,

$$f_\ell^\pm = (t^{s^\ell} \mp t^{-s^\ell})t^{-1}\,dt.$$

On a alors

$$\Omega^1_{\mathrm{dR}}(R) = \Omega^-_{\mathrm{dR}}(R) \oplus \Omega^+_{\mathrm{dR}}(R)$$

où $\Omega^-_{\mathrm{dR}}(R)$ *est de dimension* $(p+1)/2$, *de base* $(f_0^-, f_1^-, \ldots, f_{(p-1)/2}^-)$ *et où* $\Omega^+_{\mathrm{dR}}(R)$ *est de dimension* $(p-1)/2$, *de base* $(f_1^+, \ldots, f_{(p-1)/2}^+)$.

De plus, en désignant par g un générateur du groupe de Galois $G = \mathrm{Gal}(F/\mathbb{Q})$ *et en notant* σ *l'involution* $g^{(p-1)/2}$, *on a les relations* $g(f_0^-) = sf_0^-$, $g(f_\ell^\pm) = sf_{\ell+1}^\pm$, $1 \leqq \ell < (p-1)/2$, $g(f_{(p-1)/2}^\pm) = \mp sf_1^\pm$ *et* $\sigma(f_0^-) = -f_0^-$, $\sigma(f_\ell^\pm) = \pm f_\ell^\pm$, $1 \leqq \ell \leqq (p-1)/2$.

Définition 4.2. Pour $1 \leqq k \leqq (p-1)/2$, on introduit les éléments

$$\alpha_k = (x/y)^{s^{k-1}} + (y/x)^{s^{k-1}}$$

de $\mathbb{Z}/p$ et les éléments suivants de $K_1(R;\mathbb{Z}/p)$: $v_k(x) = x - yt^{s^k} \bmod R^{\times(p)}$,

$$\sigma\big(v_k(x)\big) = x - yt^{-s^k} \bmod R^{\times(p)}$$

et

$$z_k(x) = v_k(x)/\sigma\big(v_k(x)\big).$$

Proposition 4.3. *Dans la base* $(f_0^-, \ldots, f_{(p-1)/2}^-)$ *de* $\Omega^-_{\mathrm{dR}}(R)$, *la trace de Dennis de* $z_1(x)$ *s'écrit*

$$D_1^{(p)}\big(z_1(x)\big) = -s(x-1)\left(2f_0^- + \sum_{k=1}^{(p-1)/2} \alpha_k f_k^-\right).$$

Démonstration. On a $D_1^{(p)}\big(z_1(x)\big) = v_1^{-1}(x)\,dv_1(x) - \sigma\big(v_1(x)\big)^{-1}\,d\sigma\big(v_1(x)\big)$. Pour calculer $v_1^{-1}(x)$, écrivons $v_1(x) = -yt^s\big(1-(x/y)t^{-s}\big)$. L'identité

$$\big(1-(x/y)t^{-s}\big)\big(1+(x/y)t^{-s}+\cdots+(x/y)^{p-1}t^{-(p-1)s}\big) = 1 - x/y = -1/y$$

conduit à

$$v_1^{-1}(x) = t^{-s}\big(1+(x/y)t^{-s}+\cdots+(x/y)^{p-1}t^{-(p-1)s}\big).$$

Puisque $dv_1(x) = -syt^s t^{-1}\,dt$, on obtient

$$v_1^{-1}(x)\,dv_1(x) = -sy\left(t^{-1}\,dt + \sum_{i=1}^{p-1}(x/y)^i t^{-is}t^{-1}\,dt\right) = -sy\left(t^{-1}\,dt + \sum_{k=1}^{p-1}(x/y)^{s^{k-1}}t^{s^k}t^{-1}\,dt\right)$$

soit encore

$$v_1^{-1}(x)\,dv_1(x) = -sy\left(t^{-1}\,dt + \sum_{k=1}^{(p-1)/2}(x/y)^{s^{k-1}}t^{s^k}t^{-1}\,dt + \sum_{k=1}^{(p-1)/2}(x/y)^{-s^{k-1}}t^{-s^k}t^{-1}\,dt\right).$$

Pour obtenir l'expression de $v_1^{-1}(x)\,dv_1(x)$ dans la base proposée de $\Omega^-_{\mathrm{dR}}(R)$, introduisons $\beta_k = (x/y)^{s^{k-1}} - (y/x)^{s^{k-1}}$. On a

$$v_1^{-1}(x)\,dv_1(x) = -sy\left(f_0^- + \frac{1}{2}\sum_{k=1}^{(p-1)/2}\alpha_k f_k^- + \frac{1}{2}\sum_{k=1}^{(p-1)/2}\beta_k f_k^+\right).$$

Le calcul de $\sigma\big(v_1(x)\big)^{-1}\,d\sigma\big(v_1(x)\big)$ se déduit immédiatement de cette dernière relation car $D_1^{(p)}$ est équivariante, $\sigma(f_0^-) = -f_0^-$, $\sigma(f_k^\pm) = \pm f_k^\pm$. On obtient

$$\sigma\big(v^1(x)\big)^{-1}\,d\sigma\big(v_1(x)\big) = -sy\left(-f_0^- - \frac{1}{2}\sum_{k=1}^{(p-1)/2}\alpha_k f_k^- + \frac{1}{2}\sum_{k=1}^{(p-1)/2}\beta_k f_k^+\right),$$

d'où finalement l'expression proposée pour $D_1^{(p)}\big(z_1(x)\big) = D_1^{(p)}\big(v_1(x)\big) - D_1^{(p)}\big(\sigma v_1(x)\big)$.

Définition 4.4. On note $V(x)$ le sous-espace vectoriel de $K_1^-(R;\mathbb{Z}/p)$ engendré par l'orbite de $z_1(x)$ sous l'action du groupe de Galois G, c'est-à-dire

$$V(x) = \mathrm{Vect}_{\mathbb{Z}/p}\big(z_k(x), 1 \leqq k \leqq (p-1)/2\big).$$

Proposition 4.5. *Soit $C = C(x)$ la matrice circulante d'ordre $(p-1)/2$ à coefficients dans $\mathbb{Z}/p$*

$$C = C(x) = \begin{pmatrix} \alpha_1, & \alpha_2, & \dots, & \alpha_{\frac{p-1}{2}} \\ \alpha_{\frac{p-1}{2}}, & \alpha_1, & \dots, & \alpha_{\frac{p-3}{2}} \\ \vdots & \ddots & \ddots & \vdots \\ \alpha_2, & \alpha_3, & \dots, & \alpha_1 \end{pmatrix}.$$

Alors

$$\dim_{\mathbb{Z}/p} V(x) \geqq \operatorname{rg}\big(C(x)\big).$$

Démonstration. À une constante près, les composantes de $D_1^{(p)}\big(z_1(x)\big)$ dans la base $(f_0^-, f_1^-, \ldots, f_{(p-1)/2}^-)$ de $\Omega_{\mathrm{dR}}^-(R)$ sont $(2, \alpha_1, \ldots, \alpha_{(p-1)/2})$. Puisque $z_k(x) = g^k\big(z_1(x)\big)$ et compte tenu de l'action de g sur les vecteurs de base $(f_0^-, f_1^-, \ldots, f_{(p-1)/2}^-)$, on en déduit que la matrice des composantes respectives de $D_1^{(p)}\big(z_1(x)\big), D_1^{(p)}\big(z_2(x)\big), \ldots, D_1^{(p)}\big(z_{(p-1)/2}(x)\big)$ a le même rang que la matrice $C(x)$. L'image de $V(x)$ par la trace de Dennis $D_1^{(p)}$ a pour dimension le rang de $C(x)$, cqfd.

Le calcul du rang de la matrice $C(x)$ nécessite l'introduction des polynômes de Mirimanoff.

Définition 4.6. Les polynômes de Mirimanoff $M_k(X) \in \mathbb{Z}/p[X]$ sont définis pour $1 \leqq k \leqq p-1$ par

$$M_k(X) = \sum_{j=1}^{p-1} j^{k-1} X^j.$$

Pour $t \in \mathbb{Z}/p$, on pose $r_p(t) = \#\{k \mid 1 \leqq k \leqq (p-1)/2, M_{2k+1}(t) \neq 0\}$. C'est le nombre de polynômes de Mirimanoff $M_j(X)$ non nuls en la valeur t et d'indice j impair.

Proposition 4.7. *Soit x un élément de $\mathbb{Z}/p\backslash\{0,1\}$. Les valeurs propres de la matrice $C(x)$ sont $M_{2k+1}(x/y)$, $1 \leqq k \leqq (p-1)/2$. Le rang de la matrice $C(x)$ est $r_p(x/y)$.*

Démonstration. Soit s le générateur de $(\mathbb{Z}/p)^\times$ qui détermine l'action du groupe de Galois G sur A et soit $v = s^2$ le générateur de $\mathbb{Z}/(p-1)/2 \subset (\mathbb{Z}/p)^\times$. Les valeurs propres de la matrice C sont alors

$$\begin{aligned}
\lambda_k &= \sum_{j=1}^{(p-1)/2} \alpha_j (v^k)^{j-1} \\
&= \sum_{j=1}^{(p-1)/2} (x/y)^{s^{j-1}} (s^{j-1})^{2k} + \sum_{j=1}^{(p-1)/2} (x/y)^{s^{j-1+(p-1)/2}} (s^{j-1+(p-1)/2})^{2k} \\
&= \sum_{j=1}^{p-1} j^{2k} (x/y)^j \\
&= M_{2k+1}(x/y).
\end{aligned}$$

Le rang de $C(x)$ est le nombre de valeurs propres non nulles. Ces valeurs propres étant les $M_{2k+1}(x/y)$, le rang de $C(x)$ est bien $r_p(x/y)$.

En résumé, nous avons montré:

Théorème 4.8. *Soient $x \in \mathbb{Z}/p\backslash\{0,1\}$. Posons $y = x - 1$. Alors*

$$\dim_{\mathbb{Z}/p} V(x) \geqq r_p(x/y).$$

Remarque 4.9. Soit r_p le plus petit des $r_p(t)$ pour $t \in \mathbb{Z}/p\backslash\{0,1,1/2\}$. Alors, pour tout $x \in \mathbb{Z}/p\backslash\{0,1,1/2\}$, on a $(p-1)/2 \geqq \dim_{\mathbb{Z}/p} V(x) \geqq r_p$.

5. Lien avec les dérivées logarithmiques de Kummer

Dans ses recherches sur le dernier théorème de Fermat pour les nombres premiers irréguliers, Kummer a introduit certaines "dérivées logarithmiques". Un élément $z = \sum_{i=0}^{p-1} a_i \zeta^i$ de A, non divisible par $1-\zeta$ détermine un élément de $K_1(A/p;\mathbb{Z}/p)$ encore noté z. Pour $1 \leqq k \leqq p-2$, la dérivée logarithmique $\ell_k(z)$ est définie comme la classe modulo p de l'entier

$$\frac{d^k}{dX^k}\left(\log\left(\sum_{i=0}^{p-2} a_i e^{iX}\right)\right)_{X=0}.$$

Kummer a montré que ℓ_k: $\big(K_1(A/p;\mathbb{Z}/p),\times\big) \to (\mathbb{Z}/p,+)$ est un morphisme de groupes.

Soient x et y deux éléments de $(\mathbb{Z}/p)^\times$ tels que $x-y=1$. L'élément $z'(x) = \dfrac{x-y\zeta}{x-y\zeta^{-1}}$ de $K_1^-(A/p;\mathbb{Z}/p)$ est tel que $\ell_{2k}\big(z'(x)\big) = 0$, $\ell_{2k+1}\big(z'(x)\big) = 2\ell_{2k+1}(x-y\zeta)$.

Mirimanoff a montré (cf. [15], VII ou [8]) que pour $1 \leqq k \leqq (p-3)/2$, on a l'égalité $\ell_{2k+1}(x-y\zeta) = -xM_{2k+1}(x/y)$. Ceci permet de formuler un lien entre la trace de Dennis relative et les dérivées logarithmiques de Kummer.

Proposition 5.1. *Soient* $z_k(x) = (x-yt^{s^k})(x-yt^{s^{-k}})^{-1} \bmod(R)^{\times(p)}$ *les éléments de* $K_1(R;\mathbb{Z}/p)$ *introduits en* 4.2. *Soit* $C(x) \in \mathrm{Mat}_{(p-1)/2}(\mathbb{Z}/p)$ *la matrice des coordonnées des traces de Dennis relatives* $D_1^{(p)}\big(z_1(x)\big), D_1^{(p)}\big(z_2(x)\big), \ldots, D_1^{(p)}\big(z_{(p-1)/2}(x)\big)$ *dans la base de* $\Omega^-_{\mathrm{dR}}(R)$ *décrite dans la proposition* 4.1. *Alors, à une constante près, la matrice* $C(x)$ *a pour valeurs propres les dérivées logarithmiques de Kummer* $\ell_{2k+1}(x-y\zeta)$.

Exploitons à présent les calculs du paragraphe 4 pour obtenir une minoration de d_p^-. Supposons que (p,a,b,c) satisfont aux hypothèses DTF1. Notons $\bar{a}$, $\bar{b}$ et $\bar{c}$ les classes respectives de a, b et c dans $\mathbb{Z}/p$. Introduisons le sous-espace vectoriel $V(p,a,b,c)$ de $K_1^-(A;\mathbb{Z}/p)$ engendré par l'orbite de

$$z = z_1 = \frac{a-b\zeta^s}{a-b\zeta^{-s}} \bmod F^{\times(p)},$$

c'est-à-dire $V(p,a,b,c) = \mathrm{Vect}_{\mathbb{Z}/p}\big(z_k, 1 \leqq k \leqq (p-1)/2\big)$.

Proposition 5.2. *On pose* $x = \bar{a}/\bar{c}$ *et* $y = 1-x = \bar{b}/\bar{c}$. *Avec les notations de la section précédente, on a* $1 \geqq \dim_{\mathbb{Z}/p} V(x) - \dim_{\mathbb{Z}/p} V(p,a,b,c) \geqq 0$.

Démonstration. Soient φ: $A \to A/p$ la surjection canonique et ψ: $R \to A/p$ le morphisme d'anneaux défini par $\psi(t) = 1-\lambda$. On désigne par φ_1: $K_1(A;\mathbb{Z}/p)$ et ψ_1: $K_1(R;\mathbb{Z}/p) \to K_1(A/p;\mathbb{Z}/p)$ les applications induites en K-théorie à coefficients. Dans $K_1(A;\mathbb{Z}/p)$, l'image de $V(p,a,b,c)$ par φ_1 coïncide avec l'image de $V(x)$ par ψ_1, ce qui montre que la dimension de $V(p,a,b,c)$ est supérieure à celle de $\psi_1\big(V(x)\big)$. On vérifie aisément que ψ_1 est surjective de noyau de dimension 1. On en déduit l'inégalité proposée.

Theorème 5.3. *Soient* (p, a, b, c) *des entiers satisfaisant aux hypothèses* DTF1. *Alors, on a les inégalités* $d_p^- \geqq r_p(\bar{a}/\bar{c}) - 2 \geqq r_p - 2$.

Démonstration. D'après le théorème 4.8 et la proposition ci-dessus, on a les inégalités

$$d_p^- \geqq \dim_{\mathbb{Z}/p} K_1^-(A; \mathbb{Z}/p) - 1 \geqq \dim_{\mathbb{Z}/p} V(p, a, b, c) - 1$$

$$\geqq \dim_{\mathbb{Z}/p} V(\bar{a}/\bar{c}) - 2 \geqq r_p(\bar{a}/\bar{c}) - 2 \geqq r_p - 2.$$

Remarque 5.4. À une normalisation près, les calculs ci-dessus correspondent à ceux effectués par Brückner ([6]). Soit χ' la restriction de la trace de Dennis $D_1^{(p)}$ à l'espace $V(\bar{a}/\bar{c})$. Notre trace χ' est à comparer avec le morphisme χ de [6], 2.1. Les quantités $f_i(\eta)$ introduites en [6], 3.5 sont telles que $f_i(\eta) \cong (-1)^{i-1} y M_{i-1}(\bar{a}/\bar{c}) \bmod p$ et la minoration $d_p^- \geqq r_p - 2$ correspond à l'inégalité [6], 5.1. À partir de cette minoration, Brückner montre que le premier cas du dernier théorème de Fermat est vrai si $p \geqq 2^{d_p+3} - 2d_p - 3$, où $d_p = \dim_{\mathbb{Z}/p} \mathrm{Cl}(A)_{(p)}$.

On peut aussi exploiter l'inégalité $d_p^- \geqq r_p - 2$ en procédant comme suit.

Proposition 5.5. *Soit* p *un nombre premier. On a* $d_p^- < (p+3)/4$.

Démonstration. La quantité $p^{d_p^-}$ divise h^-. D'après [13] et [14], on a $h^- \leqq 2p(p/24)^{\frac{p-1}{4}}$. On en déduit

$$d_p^- - \frac{p+3}{4} \leqq \frac{\ln(2)}{\ln(p)} - \frac{(p-1)\ln(24)}{4\ln(p)}.$$

Le second membre de cette inégalité est négatif pour $p \geqq 2$, cqfd.

De l'inégalité $d_p^- < (p+3)/4$ valable pour tout p et de l'inégalité $d_p^- \geqq r_p - 2$, conditionnelle à une solution à DTF1, on déduit le résultat suivant.

Scholie 5.6. *Soit* $p \geqq 3$ *un nombre premier. Si* $r_p \geqq (p+11)/4$, *alors le premier cas du dernier théorème de Fermat est satisfait pour* p.

L'inégalité $d_p^- \geqq r_p - 2$ proposée au théorème 5.3 peut se retrouver par un autre raisonnement. Le nombre r_p est relié à la divisibilité des nombres de Bernoulli au moyen des congruences de Kummer. Rappelons en premier lieu que les nombres de Bernoulli $B_k \in \mathbb{Q}$ sont définis par

$$\frac{X}{\exp(X) - 1} = \sum_{k \geqq 0} B_k \frac{X^k}{k!}.$$

Soit $i(p)$ l'indice d'irrégularité de p défini comme le nombre de nombres de Bernoulli divisibles par p (c'est-à-dire dont le numérateur est divisible par p). On a

$$i(p) = \#\{k, 1 \leqq k \leqq (p-3)/2, p | B_{2k}\}.$$

Rappelons en second lieu que pour $x \in \mathbb{Z}/p \backslash \{0, 1\}$, on dit que x satisfait les congruences de Kummer $(\mathscr{K})$ si

$$(\mathscr{K}) \qquad B_{p-(2k+1)} M_{2k+1}(x) \equiv 0 \bmod p \quad (1 \leqq k \leqq (p-3)/2).$$

Il est clair que si x est solution des congruences de Kummer, on a l'inégalité $r_p(x) \leqq i(p)$. Par ailleurs, Kummer a montré que si (p, a, b, c) satisfont aux hypothèses DTF1, alors $x = \bar{a}/\bar{c}$ satisfait les congruences $(\mathscr{K})$ (cf. [15], VII ou [8]). On en déduit $r_p \leqq i(p)$. Cette inégalité est conditionnelle à l'existence d'une solution à DTF1. L'inégalité $i(p) \leqq d_p^-$, indépendante d'une éventuelle solution à DTF1, résulte d'un théorème de Ribet [16].

Bibliographie

[1] *Artin, E.* et *Tate, J.*, Class field theory, Benjamin, New York 1967.
[2] *Bass, H.*, Algebraic K-theory, Benjamin, New York 1968.
[3] *Bass, H.*, *Milnor, J.* et *Serre, J.-P.*, Solution of the congruence subgroup problem for SL_n ($n \geqq 3$) and Sp_{2n} ($n \geqq 2$), Publ. Math. Inst. Hautes Ét. Sci. **33** (1967), 59–137.
[4] *Berrick, J.*, Intertwiners and the K-theory of commutative rings, prépublication 2000.
[5] *Bourbaki, N.*, Algèbre, chap. 1–3, Hermann, Paris 1970.
[6] *Brückner, H.*, Zum ersten Fall der Fermatschen Vermutung, J. reine angew. Math. **274–276** (1975), 21–26.
[7] *Connes, A.*, Non-commutative differential geometry, Publ. Math. Inst. Hautes Études Sci. **62** (1985), 257–360.
[8] *Granville, A.*, The Kummer-Wieferich-Skula approach to the first case of Fermat's last theorem, Proceedings of the 3rd conference of the Canadian Number theory Association, August 18–25 1991, Advances in Number theory, ed. F.-Q. Gouveâ et N. Yui, Clarendon Press, Oxford 1993.
[9] *Igusa, K.*, What happens to Hatcher and Wagoner's formula for $\pi_0 C/M$ when the first Postnikov invariant of M is trivial?, Springer Lect. Notes Math. **1046** (1984), 104–72.
[10] *Karoubi, M.*, Homologie cyclique et K-théorie, Astérisque **149** (1987).
[11] *Karoubi, M.* et *Lambre, T.*, Quelques classes caractéristiques en théorie des nombres, C. R. Acad. Sci. Paris **330** (I) (2000), 755–760.
[12] *Lambre, T.*, Quelques exemples de lemme de première perturbation en homologie cyclique, Comm. Algebra **23** (1995), 525–541.
[13] *Lepistö, T.*, On the growth of the first factor of the class number of the prime cyclotomic field, Ann. Acad. Sci. Fennicae, Helsinki (A, I) **577** (1974), 21 pages.
[14] *Metsänkylä, T.*, Class numbers and μ-invariants of cyclotomic fields, Proc. Amer. Math. Soc. **43**, 2 (1974), 299–300.
[15] *Ribenboim, P.*, 13 lectures on Fermat's Last Theorem, Springer, Berlin 1974.
[16] *Ribet, K.*, A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$, Invent. Math. **34** (1976), 151–162.
[17] *Rosenberg, J.*, Algebraic K-theory and its applications, Springer Grad. Texts Math. **147**, Berlin 1994.
[18] *Washington, L.*, Introduction to cyclotomic Fields, Springer Grad. Texts Math. **83**, Berlin 1982.
[19] *Yamamoto, Y.*, On unramified Galois extensions of quadratic number fields, Osaka J. Math. **7** (1970), 57–76.

Université Denis Diderot (Paris 7), UFR de Mathématiques, UMR 7586 du CNRS, case 7012, 2 place Jussieu, 75251 Paris Cedex 05, France
e-mail: karoubi@math.jussieu.fr

Université Paris-Sud (Paris 11), Département de Mathématiques, UMR 7586 et 8628 du CNRS, 91405 Orsay Cedex, France
e-mail: thierry.lambre@math.u-psud.fr

Eingegangen 4. Mai 2000, in revidierter Fassung 30. Januar 2001