Quelques classes caractéristiques en théorie des nombres

Max Karoubi[1] et Thierry Lambre[2]

Abstract : Let A be an arbitrary ring. We introduce a Dennis trace map mod n, from $K_1(A;\mathbf{Z}/n)$ to the Hochschild homology group with coefficients $HH_1(A;\mathbf{Z}/n)$. If A is the ring of integers in a number field, explicit elements of $K_1(A,\mathbf{Z}/n)$ are constructed and the values of their Dennis trace mod n are computed. If F is a quadratic field, we obtain 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 ; this trace leads to an unexpected relationship between the first case of Fermat last theorem, K-theory and the number of roots of Mirimanoff polynomials.

Résumé : Pour un anneau A arbitraire, nous construisons une trace de Dennis à coefficients, de source le groupe de K-théorie $K_1(A;\mathbf{Z}/n)$, de but le groupe d'homologie de Hochschild $HH_1(A;\mathbf{Z}/n)$. Lorsque A est l'anneau des entiers d'un corps de nombres, nous construisons des éléments explicites du groupe $K_1(A;\mathbf{Z}/n)$ et évaluons leurs traces de Dennis. Dans le cas des corps quadratiques, nous en déduisons des éléments non triviaux du groupe des classes de A. Dans le cas cyclotomique, cette trace est intimement reliée aux dérivées logarithmiques de Kummer, ce qui permet de formuler un lien inattendu entre le premier cas du dernier théorème de Fermat, la K-théorie et le nombre de racines des polynômes de Mirimanoff.

Mots-clés : K-théorie à coefficients, trace de Dennis à coefficients, groupe des classes, corps quadratiques et cyclotomiques, dérivée logarithmique.

[1]Université Denis Diderot (Paris VII), UFR de Mathématiques, UMR 7586 du CNRS, case 7012, 2 place Jussieu, 75251 Paris Cedex 05, France (courriel : karoubi@math.jussieu.fr).

[2]Université Paris-Sud (Paris XI), Département de Mathématiques, UMR 7586 et 8628 du CNRS, 91405 Orsay Cedex, France (courriel : thierry.lambre@math.u-psud.fr).

Classifications AMS 1991 : Primaire 11 R 29, 19 D 55. Secondaire 11 R 18, 18 F 30, 19 F 99

Dans tout ce texte, nous utiliserons les conventions suivantes. Soit M un groupe et n un entier naturel. On définit $\cdot n : M \to M$ par $\cdot n(z) = nz$ si le groupe est noté additivement et par $\cdot n(z) = z^n$ si le groupe est noté multiplicativement. On pose $M_{(n)} = \ker(\cdot n)$, $M^{(n)} = \mathrm{Im}(\cdot n)$ et $M/(n) = M/M^{(n)}$.

Tous les anneaux sont supposés unitaires. Le groupe des unités d'un anneau A est noté $A^\times$. La classe mod. n d'un entier $a \in \mathbf{Z}$ est notée $\overline{a}$.

Introduction :

Soit k un anneau commutatif unitaire et soit A une k-algèbre (associative, unitaire). K. Dennis [10], A. Connes [7] et M. Karoubi [11] ont construit des homomorphismes "classes caractéristiques" $D_i : K_i(A) \to HH_i(A)$, $(i \geq 0)$ et $ch_{i,\ell} : K_i(A) \to HC_{i+2\ell}(A)$, $(i \geq 0$ et $\ell \geq 0)$, 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 $ch_{i,\ell}$).

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, [14]). En remplaçant la K-théorie usuelle par la K-théorie à coefficients $\mathbf{Z}/n$, nous construisons pour $i = 1$ une trace de Dennis à coefficients $\overline{D}_1 : K_1(A;\mathbf{Z}/n) \to HH_1(A;\mathbf{Z}/n)$. Pour un anneau de Dedekind A, nous explicitons le groupe $K_1(A;\mathbf{Z}/n)$ ainsi que cette trace $\overline{D}_1$. Celle-ci s'avère suffisamment riche pour détecter sous certaines conditions des éléments de n-torsion du groupe des classes. Des exemples détaillés sont proposés pour les corps quadratiques. Dans le cas d'un corps cyclotomique, ces classes caractéristiques se trouvent reliées de manière inattendue aux dérivées logarithmiques de Kummer et aux polynômes introduits au début du siècle par M. Mirimanoff lors de ses recherches sur le dernier théorème de Fermat.

Les résultats principaux de cet article sont les suivants.

Théorème 1 *Soit A un anneau unitaire et soit $n \geq 2$ un entier naturel. Il existe un morphisme naturel de groupes $\overline{D}_1$ s'insérant dans le diagramme commutatif suivant où les lignes sont exactes.*

$$\begin{tikzcd}
K_1(A) \arrow[r, ".n"] \arrow[d, "D_1"] & K_1(A) \arrow[r, "\rho"] \arrow[d, "D_1"] & K_1(A;\mathbf{Z}/n) \arrow[r, "\partial"] \arrow[d, "\overline{D}_1"] & K_0(A) \arrow[r, ".n"] \arrow[d, "D_0"] & K_0(A) \arrow[r] \arrow[d, "D_0"] & K_0(A)/(n) \arrow[d, "\overline{D}_0"] \\
HH_1(A) \arrow[r, ".n"] & HH_1(A) \arrow[r, "\rho"] & HH_1(A;\mathbf{Z}/n) \arrow[r, "\partial"] & HH_0(A) \arrow[r, ".n"] & HH_0(A) \arrow[r] & HH_0(A;\mathbf{Z}/n)
\end{tikzcd}$$

Soit A un anneau de Dedekind de corps des fractions F. On désigne par $I(A)$le monoïde des idéaux fractionnaires de A. Posons

$$\mathcal{U}(A;\mathbf{Z}/n) := \{x \in F^\times/(n) \mid \exists\ I \in I(A),\ xA = I^n\}\cdot$$

Théorème 2 *Le groupe $K_1(A;\mathbf{Z}/n)$ d'un anneau de Dedekind A est isomorphe au groupe $\mathcal{U}(A;\mathbf{Z}/n) \oplus SK_1(A)/(n)\cdot$*

Lorsque A est l'anneau des entiers d'un corps de nombres F, le lemme suivant permet de construire des éléments du groupe $K_1(A; \mathbf{Z}/n)$.

Lemme 3 *("lemme N-N_1") Soit A l'anneau des entiers d' un corps de nombres F. Notons $Cl(A)$ le groupe des classes de A. Soit u un élément non nul de A. Pour que l'élément $[u]$ de $F^\times/(n)$ appartienne à $K_1(A; \mathbf{Z}/n)$, il suffit que la norme $N(u)$ soit une puissance n-ième dans $\mathbf{Z}$ et que $(N(u), N_1(u)) = 1$, $N_1(u)$ étant le coefficient de X dans le polynôme caractéristique de u, considéré comme endomorphisme du $\mathbf{Q}$-espace vectoriel F.*

En appliquant ces deux résultats aux corps quadratiques, nous aboutissons au

Théorème 4 *Soit A l'anneau des entiers d'un corps de nombres quadratique F. Soit n un diviseur impair du discriminant δ de F. Si F est réel, on suppose que l'unité fondamentale $\varepsilon = \dfrac{\varepsilon_1 + \varepsilon_2\sqrt{\delta}}{2}$ est telle que n divise ε_2. Alors, il existe une "classe caractéristique secondaire"*

$$d_1^{(n)} : Cl(A)_{(n)} \to \mathbf{Z}/n,$$

non triviale en général.

Dans le cas où $A = \mathbf{Z}[\zeta]$ est l'anneau des entiers du corps cyclotomique $\mathbf{Q}[\zeta_p]$ (avec p impair), la conjugaison complexe scinde le groupe $K_1(A; \mathbf{Z}/p)$ en deux sous-groupes dont la partie antisymétrique est notée $K_1^-(A; \mathbf{Z}/p)$ et s'insére dans la suite exacte courte

$$1 \longrightarrow \mu_p \longrightarrow K_1^-(A; \mathbf{Z}/p) \longrightarrow Cl(A)^-_{(p)} \longrightarrow 1$$

où $Cl(A)$ est le groupe des classes de A. Posons

$$d_p^- = \dim_{\mathbf{Z}/p} Cl(A)^-_{(p)} = \dim_{\mathbf{Z}/p} K_1^-(A; \mathbf{Z}/p) - 1\cdot$$

Les nombres premiers réguliers sont caractérisés par $d_p^- = 0$. La théorie analytique des nombres montre que pour $p \geq 7$, on a $d_p^- \leq (p-1)/4\cdot$

Si (p, a, b, c) satisfont aux hypothèses du premier cas du dernier théorème de Fermat (c'est-à-dire si p premier impair, a, b, c trois entiers tels que $a^p = b^p + c^p$ avec $(a, b, c) = 1$ et p ne divisant pas abc), l'élément

$$z = \frac{a - b\zeta}{a - b\zeta^{-1}} \bmod F^{\times(p)}$$

de $F^\times/(p)$ appartient à $K_1^-(A;\mathbf{Z}/p)$. En calculant la trace de Dennis à coefficients de cet élément on aboutit à la minoration $d_p \geq 1$, ce qui prouve le théorème de Kummer sur les nombres premiers réguliers. Les coefficients de cette trace de Dennis sont d'ailleurs liés aux dérivées logarithmiques de Kummer. Cette trace permet également d'obtenir une autre minoration de d_p, qui s'exprime à l'aide des polynômes de Mirimanoff $M_k(X) \in \mathbf{Z}/p[X]$, $(1 \leq k \leq p-1)$, définis par $M_k(X) = \sum_{j=1}^{p-1} j^{k-1}X^j$. Pour $t \in \mathbf{Z}/p\backslash\{0,1,-1\}$, posons

$$r_p(t) := \sharp\{k,\ 1 \leq k \leq \frac{p-1}{2},\ M_{2k+1}(t) \neq 0\}$$

et

$$r_p = \min\{r_p(t),\ t \in \mathbf{Z}/p \setminus \{0,1,-1\}\}\cdot$$

Les nombres $r_p(t)$ et r_p sont liés aux congruences de Kummer et à la divisibilité des nombres de Bernoulli. Nous montrons la minoration suivante de d_p^-, très voisine d'une minoration obtenue précedemment par Brückner à l'aide de développements de fonctions logarithmes.

Théorème 5 *Si (p,a,b,c) satisfont aux hypothèses du premier cas du dernier théorème de Fermat, alors on a*

$$d_p^- \geq r_p(a/b) - 2.$$

Nous en déduisons que les nombres $r_p(t)$ et r_p sont également liés au théorème de Fermat-Wiles sous la forme suivante.

Corollaire 6 *Soit p un nombre premier. Si $r_p \geq (p+11)/4$, alors le premier cas du dernier théorème de Fermat est satisfait pour p.*

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. Nous remercions également le rapporteur anonyme de la Note aux C.R. Acd.Sci. ([12]) pour nous avoir signalé la référence [6]. Signalons enfin que dans le cas des anneaux commutatifs, J. Berrick (National University of Singapore), a construit ([4]) des invariants voisins des notres au moyen de “matrices entrelacées”.

1 La trace de Dennis à coefficients.

Après avoir rappelé en 1.1 les propriétés du groupe $K_1(A;\mathbf{Z}/n)$, on définit en 1.3 le groupe $HH_1(A;\mathbf{Z}/n)$. La trace de Dennis à coefficients nécessite une notion adaptée de trace pour une 1-forme différentielle non commutative. Cette construction est détaillée en 1.4 et la trace de Dennis à coefficients est construite en 1.5. Si l'anneau considéré est commutatif, une construction plus élémentaire est proposée en 1.6 grâce aux formes différentielles à la de Rham. Des traces d'ordres supérieurs, de source $K_i(A;\mathbf{Z}/n)$, de but $HC_i^-(A;\mathbf{Z}/n)$ ou $HH_i(A;\mathbf{Z}/n)$ $(i \geq 1)$, sont définies en 1.7. Ces définitions 1.7 ne sont utilisées nulle part ailleurs dans le texte.

1.1 Le groupe $K_1(A;\mathbf{Z}/n)$.

Soit A un anneau. On note $Proj(A)$ la catégorie des A-modules à droite, projectifs et de type fini. Soit $P \in Proj(A)$ et $\alpha \in Aut_A(P)$. Rappelons que le groupe de Bass $K_1(A)$ peut-être vu comme le quotient du groupe abélien libre engendré par les classes d'isomorphie de paires (P,α) modulo le sous-groupe engendré par les deux types d'éléments suivants :

(a) $(P,\alpha)+(P,\beta)-(P,\alpha\beta)$

(b) $(P_1 \oplus P_2, \alpha_1 \oplus \alpha_2)-(P_1,\alpha_1)-(P_2,\alpha_2)$.

On note $[P,\alpha] \in K_1(A)$ la classe de (P,α)

Soient A et B deux anneaux unitaires et soit $\varphi : Proj(A) \to Proj(B)$ un foncteur additif. Le foncteur φ est dit cofinal ([2], VII.1, p. 345) si tout objet R de $Proj(B)$ est facteur direct d'un objet de la forme $\varphi(P)$ avec P objet de $Proj(A)$, c'est-à-dire $\varphi(P) \cong R \oplus S$ avec $S \in Ob(Proj(B))$.

À un tel foncteur cofinal φ, on associe la catégorie $\mathcal{C}(\varphi)$ dont les objets sont les triplets (P,α,Q) avec $P \in Ob(Proj(A))$, $Q \in Ob(Proj(A))$, et où α est un isomorphisme de B-modules $\varphi(P) \cong \varphi(Q)$.

Un morphisme dans $\mathcal{C}(\varphi)$ de source (P,α,Q), de but (P_1,α_1,Q_1) est un couple (f,g) de morphismes de A-modules $f : P \to P_1$ et $g : Q \to Q_1$ tels que $\varphi(g)\circ\alpha = \alpha_1 \circ \varphi(f)$. L'ensemble des classes d'isomorphie d'objets de la catégorie $\mathcal{C}(\varphi)$ est un monoïde abélien ; on note $K(\mathcal{C}(\varphi))$ le groupe de Grothendieck associé.

Définition 7 *Le quotient de $K(\mathcal{C}(\varphi))$ par le sous-groupe N engendré par les éléments*

$$(P,\alpha,Q)+(Q,\beta,R)-(P,\beta\alpha,R)$$

est noté $K(\varphi)$. On désigne par $[P,\alpha,Q]$ la classe de $(P,\alpha,Q) \in Ob(\mathcal{C})$.

Remarque 8. Soit $\alpha' : P \to Q$ un isomorphisme de A-modules. Alors l'élément $x = [P,\varphi(\alpha'),Q] \in K(\varphi)$ est nul. En effet (α', id_Q) est un isomorphisme de la catégorie $\mathcal{C}$ de source $[P,\varphi(\alpha'),Q]$, de but $[Q,\mathrm{id}_{\varphi(Q)},Q]$, donc $x = [Q, \mathrm{id}_{\varphi(Q)}, Q] = 0$. On en déduit qu'on peut toujours supposer qu'un élément de $K(\varphi)$ est de la forme $[P, \alpha, L]$ avec L libre car si $[P, \alpha, Q]$ appartient à $K(\varphi)$ et si $Q \oplus R$ est isomorphe à un module libre L, on a $[P, \alpha, Q] = [P \oplus R, \alpha \oplus \mathrm{id}_{nR}, L]$.

D'après [2], VII.5, p. 375, on a

Théorème 9 *Soient A et B deux anneaux unitaires et soit $\varphi : Proj(A) \to Proj(B)$ un foncteur cofinal. Alors, on a une suite exacte de groupes abéliens*

$$K_1(A) \xrightarrow{\varphi_1} K_1(B) \xrightarrow{\rho} K(\varphi) \xrightarrow{\partial} K_0(A) \xrightarrow{\varphi_0} K_0(B)$$

où les applications φ_1, ∂ et φ_0 sont définies ainsi

$$\varphi_1([P, \alpha]) = [\varphi(P), \varphi(\alpha)],$$

$$\partial([P, \alpha, Q]) = [P] - [Q],$$

$$\varphi_0([P]) = [\varphi(P)].$$

Pour $[R, \lambda] \in K_1(B)$, l'application ρ est définie par cofinalité de φ en écrivant $R \oplus S \cong \varphi(P)$ et en posant $\rho([R, \lambda]) = [P, \lambda \oplus id_S, P]$.

Remarque 10. De cette suite exacte, on déduit que le groupe $K(\varphi)$ est l'extension

$$1 \longrightarrow K_1(A)/\varphi_1(K_1(A)) \xrightarrow{\rho} K(\varphi) \xrightarrow{\partial} Ker(\varphi_0) \longrightarrow 0\,.$$

Appliquons cette construction au contexte suivant.

Définition 11 *Soit n un entier, $n \geq 2$. Le foncteur $.n : Proj(A) \to Proj(A)$ est défini par $.n(P) = nP = P \oplus \cdots \oplus P$ et $.n(f) = nf = f \oplus \cdots \oplus f$ (n facteurs). Le groupe $K(.n)$ est noté $K_1(A; \mathbf{Z}/n)$. Un élément de $K_1(A; \mathbf{Z}/n)$ est de la forme $[P, \alpha, Q]$, où P et Q sont dans $Proj(A)$ et où α est un isomorphisme de A-modules $nP \cong nQ$.*

On a par conséquent la suite exacte de K-théorie à coefficients

$$K_1(A) \xrightarrow{.n} K_1(A) \xrightarrow{\rho} K_1(A; \mathbf{Z}/n) \xrightarrow{\partial} K_0(A) \xrightarrow{.n} K_0(A)$$

L'extension de la remarque ci-dessus s'écrit

$$(\ddagger) \qquad 1 \longrightarrow K_1(A)/(n) \xrightarrow{\rho} K_1(A; \mathbf{Z}/n) \xrightarrow{\partial} K_0(A)_{(n)} \longrightarrow 0$$

avec $\rho([P,\alpha]) = [P, \alpha \oplus id_{(n-1)P}, P]$ et $\partial([P,\alpha,Q]) = [P]-[Q]$. Cette extension fournit le premier exemple de calcul de K-théorie à coefficients.

Exemple : Soit A un anneau commutatif local. Pour $n \geq 2$, le groupe $K_1(A;\mathbf{Z}/n)$ est égal à $A^\times/(n)$.

Revenons au cas général. On a les relations intéressantes suivantes.

Lemme 12 *Soit A un anneau et soit n un entier, $n > 1$.*
Si $n \not\equiv 2 \bmod 4$, on a $nK_1(A;\mathbf{Z}/n) = 0$;
et si $n \equiv 2 \bmod 4$, on a $2nK_1(A;\mathbf{Z}/n) = 0$.
En particulier, si p est un nombre premier impair, $K_1(A,\mathbf{Z}/p)$ est un $\mathbf{Z}/p$-espace vectoriel.

Preuve : montrons d'abord que pour tout $n > 1$, on a $2nK_1(A;\mathbf{Z}/n) = 0$. Si p et q sont deux entiers et si $P \in \mathrm{Proj}(A)$, on a un isomorphisme $p(qP) \cong q(pP)$. Pour $q = p = n$, notons $v_P : n^2P \cong n^2P$ cet isomorphisme. La relation évidente $v_P^2 = \mathrm{id}$ montre que l'élément $x_P = [P, v_P, P]$ de $K_1(A;\mathbf{Z}/n)$ est tel que $2x_P = 0$. Soit $x = [P,\alpha,Q] \in K_1(A;\mathbf{Z}/n)$; on a $nx = [nP,\beta,nQ]$ avec $\beta = v_Q \circ n\alpha \circ v_P$, ce qui donne $nx = x_Q + x' + x_P$ avec $x' = [nP, n\alpha, nQ] = 0$. On en déduit $2nx = 0$, ce qui montre $2nK_1(A;\mathbf{Z}/n) = 0$.

Par ailleurs, la suite exacte de K-théorie à coefficients donne $n^2K_1(A;\mathbf{Z}/n) = 0$. Pour n impair, les relations $2nK_1(A;\mathbf{Z}/n) = 0$ et $n^2K_1(A;\mathbf{Z}/n) = 0$ conduisent à $nK_1(A;\mathbf{Z}/n) = 0$.

Il reste à montrer que pour $n \equiv 0 \bmod 4$, on a également $nK_1(A;\mathbf{Z}/n) = 0$. Fixons une notation : pour $\sigma \in \mathfrak{S}_n$ et $P \in \mathrm{Proj}(A)$, on note σ l'automorphisme de nP défini pour $(z_1,\ldots,z_n) \in nP$ par $\sigma(z_1,\ldots,z_n) = z_{\sigma(1)},\ldots,z_{\sigma(n)} \in nP$. On vérifie facilement que pour tout $n > 0$ et tout $P \in \mathrm{Proj}(A)$, l'isomorphisme $v_P : n(nP) \cong n(nP)$ est le produit de $\dfrac{n(n-1)}{2}$ transpositions à supports disjoints. Ce nombre est pair si $n \equiv 0$ ou $1 \bmod 4$. La proposition suivante montre que dans ce cas, l'élément $[P, v_P, P]$ de $K_1(A;\mathbf{Z}/n)$ est nul et par suite que $nK_1(A;\mathbf{Z}/n) = 0$. □

Proposition 13 *Soit $n \geq 4$ et $\tau \in \mathfrak{S}_n$ le produit de deux transpositions à supports disjoints. Alors pour tout $P \in \mathrm{Proj}(A)$ l'élément $[P,\tau,P]$ de $K_1(A;\mathbf{Z}/n)$ est nul.*

Preuve : dans $\mathfrak{S}_n$, τ est conjugué à $\tau' = (12)(34)$. Dans $K_1(A;\mathbf{Z}/n)$, on a donc $[P,\tau,P] = [P,\tau',P]$. La matrice $T' \in \mathrm{GL}(\mathbf{Z})$ de τ' appartient à $[\mathrm{GL}(\mathbf{Z}), \mathrm{GL}(\mathbf{Z})]$ donc $[P,\tau',P] = 0$. □

1.2 L'algèbre différentielle graduée $\Omega^*_{nc}(A)$.

Soit k un anneau commutatif unitaire et soit A une k-algèbre unitaire. Désignons par $\mu : A\otimes_k A \to A$ la multiplication de A. Posons $\Omega^1_{nc}(A) := \ker \mu$. On sait que $\Omega^1_{nc}(A)$ est le sous-bimodule de $A \otimes_k A$ engendré par

$$\{1 \otimes a - a \otimes 1, a \in A\}\cdot$$

On introduit la 1-forme différentielle non commutative

$$d_{nc}a := 1 \otimes a - a \otimes 1.$$

La structure de A-bimodule évident de $\Omega^1_{nc}(A)$ se lit en terme de formes différentielles par la relation

$$(*) \qquad d_{nc}(a_1) \cdot a_2 = d_{nc}(a_1 a_2) - a_1 d_{nc}a_2$$

de sorte que tout élément de $\Omega^1_{nc}(A)$ s'écrit comme somme de 1-formes différentielles $a_0 d_{nc}a_1$. En tant que k-module, on a $\Omega^1_{nc}(A) \cong A \otimes_k (A/k)$.

A partir de $\Omega^1_{nc}(A)$, on construit une k-algèbre différentielle graduée $\Omega^*_{nc}(A)$ en posant $\Omega^r_{nc}(A) := \Omega^1_{nc}(A) \otimes_A \ldots \otimes_A \Omega^1_{nc}(A)$ (r facteurs). La structure de A-module à droite sur $\Omega^r_{nc}(A)$ se définit en jouant à saute-moutons à l'aide de la formule $(*)$:

$$a_0 d_{nc}a_1 \ldots d_{nc}a_r \cdot \alpha = a_0 d_{nc}a_1 \ldots d_{nc}(a_r\alpha) - a_0 d_{nc}a_1 \ldots d_{nc}a_{r-1} \cdot a_r d_{nc}\alpha = \text{etc}\,.$$

Tout élément de $\Omega^r_{nc}(A)$ est somme de r-formes différentielles du type

$$a_0 d_{nc}a_1 \ldots d_{nc}a_r.$$

C'est encore la relation $(*)$ qui définit le produit de $\omega_r \in \Omega^r_{nc}(A)$ par $\omega_s \in \Omega^s_{nc}(A)$.

En tant que k-module, on a $\Omega^r_{nc}(A) = A\otimes(A/k)^{\otimes r}$ et le bord de Hochschild de A admet une expression très simple dans l'algèbre $\Omega^*_{nc}(A)$: pour $\omega_r \in \Omega^r_{nc}(A)$ avec $\omega_r = \omega' d_{nc}\alpha$, $\alpha \in A$, on a $b(\omega_r) = (-1)^{r-1}(\omega'\alpha - \alpha\omega')$. Le complexe de Hochschild normalisé, traditionnellement noté $(\overline{C}_*(A), b)$ n'est autre que $(\Omega^*_{nc}(A), b)$. Pour $\omega \in \Omega^*_{nc}(A)$ tel que $b(\omega) = 0$, on note $[\omega]$ sa classe d'homologie de Hochschild.

1.3 Le k-module gradué $HH_*(A; \mathbf{Z}/n)$.

Soit k un anneau commutatif unitaire, soient (C_*, d) et (C'_*, d') des complexes (de chaînes) de k-modules et soit $f : (C_*, d) \to (C'_*, d')$ un morphisme de complexes. Le cône de f est le complexe de chaînes $(\mathrm{co}(f), \partial)$ défini par $\mathrm{co}(f)_r = C'_r \oplus C_{r-1}$ et $\partial(a', a) = (d'(a') + f(a), -d(a))$. De la suite exacte courte de complexes

$$0 \to (C'_*, d') \to (\mathrm{co}(f), \partial) \to (C_*, d)_{[1]} \to 0$$

on déduit une suite exacte longue d'homologie dont le connectant $H_r\left((C_*, d)_{[1]}\right) \to H_{r-1}(C'_*, d')$ n'est autre que $H_{r-1}(f)$.

Définition 14 *Soient k un anneau commutatif unitaire et A une k-algèbre unitaire. Soit $(\Omega_*(A), b)$ le complexe de Hochschild de A. L'homologie du cône de l'application $.n : (\Omega_*(A), b) \to (\Omega_*(A), b)$ définie par $.n(a_0 \otimes a_1 \otimes \ldots \otimes a_r) = na_0 \otimes a_1 \otimes \ldots \otimes a_r$ s'appelle l'homologie de Hochschild à coefficients $\mathbf{Z}/n$ de l'algèbre A. On note cette homologie $HH_*(A; \mathbf{Z}/n)$.*

Pour $(\omega_r, \omega_{r-1}) \in \Omega^r(A) \oplus \Omega^{r-1}(A)$ telle que $\partial(\omega_r, \omega_{r-1}) = 0$, on note $[\omega_r, \omega_{r-1}]$ sa classe d'homologie de Hochschild à coefficients.

De cette définition de $HH_*(A; \mathbf{Z}/n)$, on extrait la suite exacte longue

$$\cdots \longrightarrow HH_1(A) \xrightarrow{.n} HH_1(A) \xrightarrow{\rho} HH_1(A; \mathbf{Z}/n) \xrightarrow{\partial} HH_0(A)$$

$$\xrightarrow{.n} HH_0(A) \longrightarrow HH_0(A; \mathbf{Z}/n) \cdot$$

avec $\rho([\omega_r]) = [\omega_r, 0]$ et $\partial([\omega_r, \omega_{r-1}]) = [\omega_{r-1}]$.

1.4 Calcul différentiel non commutatif d'ordre 1.

Soit P un A-module projectif, à droite, de type fini. Un système de coordonnées de P (cf. [5], II.46) est une suite $\mathcal{S} = (x_j, \varphi_j)_{1 \le j \le r}$ avec $x_j \in P$, $\varphi_j \in P^* = \mathrm{Hom}_A(P, A)$ telle que pour tout $x \in P$, on ait $x = \sum_{j=1}^r x_j \varphi_j(x)$.

Soit $u \in \mathrm{End}P$. Par définition, la matrice de u dans le système de coordonnées $\mathcal{S}$ est la matrice $U = (U_{ij}) \in \mathrm{Mat}_{r,r}(A)$ définie par $U_{ij} = \varphi_i \circ u(x_j)$. La quantité $\sum_{i=1}^r \varphi_i \circ u(x_i) \in A$ s'appelle la trace de u relativement au système de coordonnées $\mathcal{S}$. On la note $\mathrm{tr}(u, \mathcal{S})$, ou $\mathrm{tr}(u)$. On pose $\mathrm{rg}(P) = \mathrm{rg}(P, \mathcal{S}) = \mathrm{tr}(\mathrm{id}_P, \mathcal{S}) = \sum_{i=1}^r \varphi_i(x_i) \in A$. Ces quantités dépendent du système de coordonnées $\mathcal{S}$ choisi.

La connexion de Levi-Civita de P (cf. [7] et [11]) est l'application $d_P : P \to P \otimes_A \Omega^1(A)$ dont l'expression dans le système de coordonnées $\mathcal{S}$ est

$$d_P\left(\sum_{j=1}^{r} x_j\varphi_j(x)\right) = \sum_{j=1}^{r} x_j d_{nc}(\varphi_j(x))\,.$$

Comme toute connexion, d_P n'est pas une application A-linéaire mais satisfait à la relation :

$$d_P(xa) = d_P(x)a + xd_{nc}a\ ,\ x \in P\ ,\ a \in A\,.$$

Définition 15 *Soit $\alpha : P \to Q$ une application A-linéaire à droite entre les modules projectifs de type fini P et Q. Soient d_P et d_Q les connexions de Levi-Civita de P et Q. L'application A-linéaire*

$$\begin{aligned} &d_{nc}\alpha : P \to Q \otimes_A \Omega^1(A) \text{ est définie par}\\ &d_{nc}\alpha = d_Q \circ \alpha - (\alpha \otimes \mathrm{id}) \circ d_P\,. \end{aligned}$$

L'abus d'écriture fréquent qui consiste à poser $d_P = d_Q = d_{nc}$ conduit à la formule $d_{nc}(\alpha(x)) = d_{nc}\alpha(x) + \alpha(d_{nc}x)$, $x \in P$.

Soient $\mathcal{S} = (x_j, \varphi_j)_{1\le j\le r}$ et $\mathcal{S}' = (y_i, \psi_i)_{1\le i\le s}$ des systèmes de coordonnées respectifs de P et Q. Il est facile de donner une interprétation matricielle de l'application $d\alpha$. Si $M = (M_{ij}) \in \mathrm{Mat}_{s,r}(A)$ est la matrice de α, exprimée dans les systèmes de coordonnées $\mathcal{S}$ et $\mathcal{S}'$, avec $M_{ij} = \psi_i \circ \alpha(x_j)$, un calcul simple montre que pour $x = \sum_{j=1}^{r} x_j\varphi_j(x)$, on a $d_{nc}\alpha(x) = \sum_{i,j} y_i d(M_{ij})\varphi_j(x)$, ce qui permet de dire que $d_{nc}\alpha$ a pour matrice $d_{nc}M = (d_{nc}M_{ij}) \in \mathrm{Mat}_{s,r}(\Omega^1(A))$ dans les systèmes $\mathcal{S}$ et $\mathcal{S}'$.

Supposons de plus que $\alpha : P \to Q$ soit un isomorphisme de A-modules. Soit $N \in \mathrm{Mat}_{s,r}(A)$ la matrice de α^{-1} exprimée dans les systèmes de coordonnées $\mathcal{S}'$ et $\mathcal{S}$. On a $MN = \mathrm{mat}_{\mathcal{S}'}(\mathrm{id}_Q)$ et $NM = \mathrm{mat}_{\mathcal{S}}(\mathrm{id}_P)$. L'application composée $P \xrightarrow{d_{nc}\alpha} Q \otimes_A \Omega^1(A) \xrightarrow{\alpha^{-1}\otimes\mathrm{id}} P \otimes_A \Omega^1(A))$, évidemment notée $\alpha^{-1}d_{nc}\alpha$ est A-linéaire, de matrice $NdM \in \mathrm{Mat}_{r,r}(\Omega^1(A))$. La trace de cette matrice, $\mathrm{tr}(NdM) \in \Omega^1(A)$, s'appelle la trace de $\alpha^{-1}d_{nc}\alpha$ dans les systèmes de coordonnées $\mathcal{S}$ et $\mathcal{S}'$.

Proposition 16 *Soient P et Q deux A-modules à droite, projectifs et de type fini, de systèmes de coordonnées respectifs $\mathcal{S}$ et $\mathcal{S}'$. Posons $p = \mathrm{rg}(P, \mathcal{S})$ et $q = \mathrm{rg}(Q, \mathcal{S}')$. Soit $\alpha : P \to Q$ un isomorphisme de A-modules et soit*

$\mathrm{tr}(\alpha^{-1}d_{nc}\alpha) \in \Omega^1(A)$ *la trace de* $\alpha^{-1}d_{nc}\alpha$*, exprimée dans les systèmes de coordonnés* $\mathcal{S}$ *et* $\mathcal{S}'$*.*

Alors le bord de Hochschild de $\mathrm{tr}(\alpha^{-1}d_{nc}\alpha)$ *est donné par* $b(\mathrm{tr}(\alpha^{-1}d_{nc}\alpha)) = q - p \in A$*.*

PREUVE : on a $\mathrm{tr}(\alpha^{-1}d_{nc}\alpha) = \mathrm{tr}(Nd_{nc}M)$ d'où
$b(\mathrm{tr}(\alpha^{-1}d_{nc}\alpha)) = b(\mathrm{tr}Nd_{nc}M) = -\mathrm{tr}NM + \mathrm{tr}MN = -\mathrm{tr}(\mathrm{id}_P, \mathcal{S}) + \mathrm{tr}(\mathrm{id}_Q, \mathcal{S}')$.
□

REMARQUE 17. Dans la proposition ci-dessus, si $P = Q$ et si $\mathcal{S} = \mathcal{S}'$, alors pour tout automorphismes α de P, $\mathrm{tr}(\alpha^{-1}d_{nc}\alpha, \mathcal{S})$ est un cycle de Hochschild. Dans ce cas on note $[\mathrm{tr}(\alpha^{-1}d_{nc}\alpha] \in HH_1(A)$, sa classe d'homologie de Hochschild.

Nous utiliserons également le résultat suivant, de preuve facile laissée au lecteur.

Proposition 18 *Soient* P*,* Q *et* R *des* A*-modules à droite, projectifs et de type fini ; soient* $\alpha \in \mathrm{Hom}_A(P, Q)$*,* $\beta \in \mathrm{Hom}_A(Q, R)$*. Alors on a la relation*

$$d_{nc}(\beta \circ \alpha) = d_{nc}\beta \circ \alpha + \beta \circ d_{nc}\alpha\,.$$

En particulier $\alpha^{-1}d_{nc}\alpha = -d_{nc}\alpha^{-1} \circ \alpha$*.*

1.5 La trace de Dennis à coefficients $\overline{D}_1$.

Pour tout entier $r \geq 0$, K. Dennis ([10]) a construit un morphisme $D_r : K_r(A) \to HH_r(A)$. Rappelons que si $r = 0$ et $[P] \in K_0(A)$, on a $D_0([P]) = \mathrm{rg}(P, \mathcal{S}) \bmod [A, A]$ et que si $r = 1$ et $[P, \alpha] \in K_1(A)$, on a $D_1([P, \alpha]) = [\mathrm{tr}(\alpha^{-1}d_{nc}\alpha)] \in HH_1(A)$.

Théorème 19 *Soient* A *un anneau unitaire,* n *un entier,* $n \geq 2$ *et soit* $x = [P_1, \alpha, P_2] \in K_1(A; \mathbf{Z}/n)$*. Après avoir fixé des systèmes de coordonnées* $\mathcal{S}_1$ *et* $\mathcal{S}_2$ *sur* P_1 *et* P_2*, on pose* $p_1 = \mathrm{rg}(P_1, \mathcal{S}_1), p_2 = \mathrm{rg}(P_2, \mathcal{S}_2)$ *et* $\overline{D}_1(x) = [\mathrm{tr}(\alpha^{-1}d_{nc}\alpha), p_1 - p_2] \in HH_1(A; \mathbf{Z}/n)$*.*

Alors l'application $\overline{D}_1$ *est un morphisme de groupes s'insérant dans le diagramme commutatif à lignes exactes ci-dessous*

$$\begin{tikzcd}
K_1(A) \arrow[r, ".n"] \arrow[d, "D_1"] & K_1(A) \arrow[r, "\rho"] \arrow[d, "D_1"] & K_1(A;\mathbf{Z}/n) \arrow[r, "\partial"] \arrow[d, "\overline{D}_1"] & K_0(A) \arrow[r, ".n"] \arrow[d, "D_0"] & K_0(A) \arrow[r] \arrow[d, "D_0"] & K_0(A)/(n) \arrow[d, "\overline{D}_0"] \\
HH_1(A) \arrow[r, ".n"] & HH_1(A) \arrow[r, "\rho"] & HH_1(A;\mathbf{Z}/n) \arrow[r, "\partial"] & HH_0(A) \arrow[r, ".n"] & HH_0(A) \arrow[r] & HH_0(A;\mathbf{Z}/n)
\end{tikzcd}$$

PREUVE : la quantité $c = \big(\mathrm{tr}(\alpha^{-1}d_{nc}\alpha), p_1 - p - 2\big)$ est un cycle du cône de la multiplication $.n : (\Omega^*(A), b) \to (\Omega^*(A), b)$. En effet,

$$\partial(c) = b(\mathrm{tr}(\alpha^{-1}d_{nc}\alpha)) + n(p_1 - p_2);$$

or

$$b(\mathrm{tr}(\alpha^{-1}d_{nc}\alpha)) = \mathrm{rg}(nP_2, n\mathcal{S}_2) - \mathrm{rg}(nP_1, n\mathcal{S}_1),$$

donc $\partial(c) = 0$.

Soit $[c] = [\mathrm{tr}\alpha^{-1}d_{nc}\alpha, p_1 - p_2] \in HH_1(A, \mathbf{Z}/n)$ la classe d'homologie du cycle c. Cette classe est indépendante du choix du représentant (P_1, α, P_2) de x. Supposons d'abord $(P_1, \alpha, P_2) \cong (P_1', \alpha', P_2')$ dans la catégorie $\mathcal{C}$. Il existe dans ce cas un couple d'isomorphismes $f_i : P_i \cong P_i'$ tel que $\alpha' \circ (nf_1) = (nf_2) \circ \alpha$. Choisissons des systèmes de coordonnées ${\mathcal{S}'}_i$ sur P_i'. Posons

$$\begin{aligned} c &= (\mathrm{tr}\alpha^{-1}d_{nc}\alpha, \mathrm{rg}(P_1, \mathcal{S}_1) - \mathrm{rg}(P_2, \mathcal{S}_2)) \text{ et} \\ c' &= (\mathrm{tr}\alpha'^{-1}d_{nc}\alpha', \mathrm{rg}(P_1', {\mathcal{S}'}_1) - \mathrm{rg}(P_2', {\mathcal{S}'}_2))\,. \end{aligned}$$

On a $\partial c = \partial c' = 0$. Introduisons

$$\begin{aligned} \omega_1 &= \mathrm{tr}(f_2^{-1}d_{nc}f_2 - f_1^{-1}d_{nc}f_1) \text{ et} \\ \omega_2 &= \mathrm{tr}((\alpha')^{-1}d_{nc}(nf_2)d_{nc}(\alpha \circ nf_1^{-1}) + (nf_1)\alpha^{-1}d_{nc}\alpha d_{nc}(nf_1^{-1})); \end{aligned}$$

on a $\omega_i \in \Omega^i(A)$ et $\partial(\omega_2, \omega_1) = c' - c$, c'est-à-dire $[c'] = [c]$ dans $HH_1(A, \mathbf{Z}/n)$.

Le même argument montre que la classe de c est indépendante du choix des systèmes de coordonnés $\mathcal{S}_1$ et $\mathcal{S}_2$ retenus sur P_1 et P_2.

Montrons à présent qu'on a un morphisme de groupes

$$D : K_0(\mathcal{C}) \to HH_1(A; \mathbf{Z}/n)$$

en posant $D(\widehat{(P_1, \alpha, P_2)}) = [\mathrm{tr}(\alpha^{-1}d_{nc}\alpha), \mathrm{rg}(P_1, \mathcal{S}_1) - \mathrm{rg}(P_2, \mathcal{S}_2)]$. Pour $i = 1, 2, 3$, soient $t_i = \widehat{(P_i, \alpha_i, Q_i)}$ trois éléments de $K_0(\mathcal{C})$ tels que $t_1 + t_2 = t_3$. Après avoir fixé des systèmes de coordonnées $\mathcal{S}_i$ et ${\mathcal{S}'}_i$ sur P_i et Q_i $(i = 1, 2)$, on choisit $\mathcal{S}_1 \cup \mathcal{S}_2$ (resp. ${\mathcal{S}'}_1 \cup {\mathcal{S}'}_2$) comme système de coordonnées de P_3 (resp. Q_3).

Posons $c_i = (\mathrm{tr}(\alpha_i^{-1}d_{nc}\alpha_i), \mathrm{rg}(P_i, \mathcal{S}_i) - \mathrm{rg}(Q_i, \mathcal{S}_i))$ pour $i = 1, 2$.

De $\alpha_3 = \alpha_1 \oplus \alpha_2$ et du choix proposé pour les systèmes de coordonnées, on tire immédiatement $c_3 = c_1 + c_2$. Cette égalité entre cocycles entraîne$[c_1] + [c_2] = [c_3]$.

Il reste à montrer $D(N) = 0$, où N est le sous-groupe de $K_0(\mathcal{C})$ tel que $K_1(A; \mathbf{Z}/n) = K_0(\mathcal{C})/N$. Soient $z_1 = \widehat{(P_1, \alpha, P_2)}$ et $z_2 = \widehat{(P_2, \beta, P_3)}$ deux éléments de $K_0(\mathcal{C})$; on pose $z = \widehat{(P_1, \beta\alpha, P_3)}$. Après avoir choisi des systèmes de coordonnées $\mathcal{S}_i$ sur P_i, on pose

$$\begin{aligned}
c_1 &= (tr\alpha^{-1}d_{nc}\alpha, \mathrm{rg}(P_1, \mathcal{S}_1) - \mathrm{rg}(P_2, \mathcal{S}_2))\,, \\
c_2 &= (\mathrm{tr}\beta^{-1}d_{nc}\beta, \mathrm{rg}(P_2, \mathcal{S}_2) - \mathrm{rg}(P_3, \mathcal{S}_3)\,, \\
c &= (\mathrm{tr}(\beta\alpha)^{-1}d_{nc}(\beta\alpha), \mathrm{rg}(P_1, \mathcal{S}_1) - \mathrm{rg}(P_3, \mathcal{S}_3))\,, \\
\theta_2 &= -\mathrm{tr}(\alpha^{-1}\beta^{-1}d_{nc}\beta d_{nc}\alpha)\,, \\
\theta_1 &= 0\,.
\end{aligned}$$

On a $c_1 + c_2 - c_3 = \partial(\theta_2, \theta_1)$, ce qui montre que l'application D factorise en un morphisme $D_1^{(n)} : K_1(A, \mathbf{Z}/n) \to HH_1(A; \mathbf{Z}/n)$. En remarquant que $\mathrm{tr}(\alpha \oplus \mathrm{id})^{-1}d(\alpha \oplus \mathrm{id}) = \mathrm{tr}(\alpha^{-1}d\alpha)$, il est immédiat de vérifier que les diagrammes commutent. $\square$

Corollaire 20 *Posons* $\widetilde{HH_1}(A; \mathbf{Z}/n) = HH_1(A; \mathbf{Z}/n)/\mathrm{Im}(\rho\circ D_1)$. *La "classe caractéristique secondaire"*

$$\overline{d}_1 : K_0(A)_{(n)} \to \widetilde{HH_1}(A; \mathbf{Z}/n)\,.$$

définie pour $x = \partial(y) \in K_0(A)_{(n)}$ *par* $\overline{d}_1(x) = \overline{D}_1(y) \bmod Im\rho \circ D_1$ *est un morphisme de groupes abéliens.*

Nous montrerons plus loin que cette classe caractéristique secondaire n'est pas triviale en général.

1.6 Le cas des algèbres commutatives.

Si l'algèbre A est commutative, on peut simplifier notablement la construction de la trace de Dennis à coefficients en transitant par le A-module $\Omega^1_{dR}(A)$ des différentielles de Kähler de A. Fixons pour cela un peu de vocabulaire.

Le module des différentielles de Kähler de A est le A-module $\Omega^1_{dR}(A) := \ker\mu/(\ker\mu)^2$, où $\mu : A \otimes_k A \to A$ est la multiplication de A. Ce A-module est engendré par les symboles da, $a \in A$, soumis aux relations $d\lambda = 0$, $\lambda \in k$, $d(a_0a_1) = a_0da_1 + a_1da_0$.

On sait que lorsque A est commutative, la trace de Dennis D_1 est essentiellement la dérivée logarithmique. En effet, de la commutativité de A, on déduit

$$HH_1(A) = \Omega^1_{nc}(A)/[A, \Omega^1_{nc}(A)].$$

L'application $\gamma : HH_1(A) \to \Omega^1_{dR}(A)$ définie par $\gamma([a_0 d_{nc} a_1]) = a_0 da_1$ est un isomorphisme. On en déduit le morphisme surjectif de A-bimodules $\rho : \Omega^1_{nc}(A) \to \Omega^1_{dR}(A)$ défini par $\rho(a_0 d_{nc} a_1) = a_0 da_1$.

Pour $x = [P, \alpha] \in K_1(A)$, on obtient facilement $\gamma \circ D_1(x) = \det(\alpha)^{-1} d(\det(\alpha))$. 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 $\gamma \circ D_1(u) = u^{-1} du$.

Soit P un A-module projectif de type fini sur A et soit $\mathcal{S} = (x_j, \varphi_j)_{1 \le j \le r}$ un système de coordonnées sur P. La connexion de Levi-Civita commutative de P est l'application $d'_P : P \to P \otimes_A \Omega^1_{dR}(A)$ définie pour $x = \sum_{j=1}^r x_j \varphi_j(x)$ par $d'_p(x) = \sum_{j=1}^r x_j d\varphi_j(x)$. Remarquons que si $d_P : P \to P \otimes_A \Omega^1_{nc}(A)$ désigne la connexion de Levi-Civita non commutative, le diagramme suivant est commutatif.

$$\begin{tikzcd}
P \arrow[r, "d'_P"] \arrow[d, "d_P"] & P \otimes_A \Omega^1_{dR}(A) \\
P \otimes_A \Omega^1_{nc}(A) \arrow[ur, "\mathrm{id} \otimes \rho"'] &
\end{tikzcd}$$

Soient P et Q deux A-modules projectifs de type fini et soit $\alpha : P \to Q$ une application A-linéaire. Soient

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

et

$$\nabla' : Q \to Q \otimes_A \Omega^1_{dR}(A)$$

des connexions sur P et Q respectivement. On définit l'application A-linéaire $d\alpha = d(\alpha, \nabla, \nabla')$ de source P, de but $Q \otimes_A \Omega^1_{dR}(A)$ par

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

Soit $\alpha : P \to Q$ 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 $\Omega^1_{dR}(A)$ dont la trace est notée $tr(\alpha^{-1}d\alpha)$.

Théorème 21 *Soient k un anneau commutatif unitaire, A une k-algèbre commutative et soit $n \geq 2$ un entier.*

Soit

$$D_1^{(n)} : K_1(A; \mathbf{Z}/n) \to \Omega^1_{dR}(A)/(n)$$

l'application définie pour $x = [P, \alpha, Q]$ dans $K_1(A, \mathbf{Z}/n)$ par

$$D_1^{(n)}(x) = tr(\alpha^{-1} \circ d(\alpha, n\nabla, n\nabla')) \bmod n\Omega^1_{dR}(A),$$

où ∇ et ∇' sont des connexions sur P et Q respectivement.

Alors l'application $D_1^{(n)}$ est un morphisme de groupes abéliens.

Remarque 22. Supposons de plus que l'algèbre A soit intègre et que n soit un entier premier à la caractéristique de A. La suite exacte longue 1.3 conduit à l'isomorphisme $HH_1(A; \mathbf{Z}/n) \cong HH_1(A)/(n)$. Notons $\overline{\gamma} : HH_1(A)/(n) \to \Omega^1_{dR}(A)/(n)$ l'isomorphime induit de $\gamma : HH_1(A) \simeq \Omega^1_{dR}(A)$. A l'aide des connections de Levi-Civita, on vérifie que l'application $D_1^{(n)}$ s'insère dans le diagramme commutatif

$$\begin{tikzcd} K_1(A; \mathbf{Z}/n) \arrow[r, "\overline{D}_1"] \arrow[dr, "D_1^{(n)}"'] & HH_1(A; \mathbf{Z}/n) \arrow[d, "\overline{\gamma}"] \\ & \Omega^1_{dR}(A)/(n) \end{tikzcd}$$

Preuve du théorème 23 : avec les notations de 1.1, on a $K_1(A; \mathbf{Z}/n) = K_0(\mathcal{C})/N$. Soit (P, α, Q) un objet de $\mathcal{C}$.

Si ∇ et ∇_1 sont deux connexions sur P et si ∇' est une connexion sur Q, on a

$$\alpha^{-1} \circ d(\alpha, n\nabla, n\nabla') - \alpha^{-1} \circ d(\alpha, n\nabla_1, n\nabla') = n(\nabla - \nabla_1),$$

application A-linéaire dont la trace est congrue à 0 modulo $n\Omega^1_{dR}(A)$.

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 $n\Omega^1_{dR}(A)$.

Ces deux remarques montrent que pour $(P, \alpha, Q) \in Ob(\mathcal{C})$, le choix des connexions sur P ou Q n'intervient pas pour la définition de $tr(\alpha^{-1}d\alpha)$ modulo $n\Omega^1_{dR}(A)$. C'est pourquoi, pour alléger, 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 $\mathcal{C}$, il existe des applications A-linéaires f et g telles que $\alpha_1 = ng \circ \alpha \circ nf^{-1}$. Un rapide calcul donne

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

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

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

et

$$\mathrm{tr}\left((\alpha\beta)^{-1}d(\alpha\beta)\right) = \mathrm{tr}(\alpha^{-1}d\alpha) + \mathrm{tr}(\beta^{-1}d\beta)$$

montrent qu'on a un morphisme de groupes $D_1^{(n)}$ de source $K_1(A; \mathbf{Z}/n)$ 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. Soit A un anneau commutatif. On suppose $K_0(A) = \mathbf{Z}$. Alors, $K_1(A; \mathbf{Z}/n) = K_1(A)/(n) = A^\times/(n) \oplus SK_1(A)/(n)$. 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 commutatif, 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 $\{u^{-1}du,\ u \in A^\times\}$. Du théorème 23, on déduit :

Corollaire 23 *Soient k un anneau commutatif unitaire, A une k-algèbre commutative et n un entier. On désigne par $A^\times$ le groupe des unités de A et 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"*

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

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.

Nous verrons plus bas que ce morphisme n'est pas trivial.

1.7 Les traces d'ordre supérieur.

Soit A une k-algèbre. Désignons par $HH_*(A)$, $HC_*^-(A)$ et $HC_*^{per}(A)$ respectivement les homologies de Hochschild, "cyclique négative" et "cyclique périodique" de A (voir [17], 1.1 et 5.1 pour les définitions). Soit $D_* : K_*(A) \to HH_*(A)$ la trace de Dennis [10] et $\gamma_* : K_*(A) \to HC_*^-(A)$ le caractère de Chern universel ([8], II). Pour tout $r \geq 0$, Weibel ([25], p. 541) a montré qu'on a un diagramme commutatif

$(0)_r$
$$\begin{tikzcd} K_r(A) \arrow[r, "\gamma_r"] \arrow[d, "D_r"] & HC_r^-(A) \arrow[r, "I_r"] \arrow[dl, "h_r"] & HC_r^{per}(A) \\ HH_r(A) & & \end{tikzcd}$$

Nous montrons ici que pour tout $r \geq 1$ et tout $n \geq 2$, il existe un diagramme commutatif

$(0)_r^n$
$$\begin{tikzcd} K_r(A;\mathbf{Z}/n) \arrow[r, "\gamma_r^{(n)}"] \arrow[d, "D_r^{(n)}"] & HC_r^-(A;\mathbf{Z}/n) \arrow[r, "I_r^{(n)}"] \arrow[dl, "h_r^{(n)}"] & HC_r^{per}(A;\mathbf{Z}/n) \\ HH_r(A;\mathbf{Z}/n) & & \end{tikzcd}$$

reliant la K-théorie à coefficients de A aux diverses homologies à coefficients au moyen d'applications $\gamma_r^{(n)}$ et $D_r^{(n)}$ qui sont précisées plus bas.

Notons $C_*(A)$, $CC_*(A)^-$ et $CC_*^{per}(A)$ les complexes de chaînes des homologies de Hochschild, cyclique négative et périodique de A. La correspondance de Dold-Kan ([26], 8.4) $DK : Ch_+ \to AbS$ réalise une équivalence entre la catégorie Ch_+ des complexes de chaînes gradués positivement et la catégorie des groupes abéliens simpliciaux. Notons $|\ |: AbS \to Top$ le foncteur réalisation géométrique et $X : Ch_* \to Top$ la composée de ces deux foncteurs. Les espaces $\mathcal{H}(A) = X(C_*(A))$, $\mathcal{H}^-(A) = X(CC_*^-(A))$ et $\mathcal{H}^{per}(A) = X(CC_*^{per}(A))$ sont des espaces classifiants pour les homologies de Hochschild ou cycliques. Pour $r \geq 0$, on a $\pi_r(\mathcal{H}(A)) = HH_r(A)$, $\pi_r(\mathcal{H}^-(A)) = HC_*^-(A)$ et $\pi_r(\mathcal{H}^{per}(A)) = HC_*^{per}(A)$. D'après [25], prop. 4.3, on a

Proposition 24 *Pour toute algèbre A, il existe dans la catégorie Top un diagramme commutatif*

(1)
$$\begin{tikzcd} BGLA^+ \arrow[r, "\gamma"] \arrow[d, "D"] & \mathcal{H}^-(A) \arrow[r, "I"] \arrow[dl, "h"] & \mathcal{H}^{per}(A) \\ \mathcal{H}(A) & & \end{tikzcd}$$

tel que pour $r \geq 0$, en appliquant le foncteur $\pi_r(-)$ au diagramme (1), on obtienne le diagramme $(0)_r$.

Il est naturel de chercher à obtenir le diagramme $(0)_r^n$ par application du foncteur $\pi_r(-; \mathbf{Z}/n)$ au diagramme (1). Ce foncteur n'est défini que pour $r \geq 2$. Une désuspension permet l'étude du cas $r = 1$.

Rappelons (voir [19]), que pour $r \geq 2$, on pose $\pi_r(-; \mathbf{Z}/n) = [M_n^r, -]$ où M_n^r est l'espace de Moore $S^{r-1} \cup_\alpha e^r$ avec α de degré n.

Pour $r \geq 2$, on pose $K_r(A; \mathbf{Z}/n) = \pi_r(BGLA^+; \mathbf{Z}/n)$. La structure de H-espace de $BGLA^+$ permet de définir une application $.n : BGLA^+ \to BGLA^+$ induisant la multiplication par n sur $\pi_r(BGLA^+)$. La fibre homotopique $\mathcal{F}$ de $.n : BGLA^+ \to BGLA^+$ est telle que pour $r \geq 1$, on a $\pi_r(\mathcal{F}) = \pi_{r+1}(BGLA^+; \mathbf{Z}/n)$.

Rappelons également que l'homologie à coefficients $H_*(C_*; \mathbf{Z}/n)$ d'un complexe de chaînes C_* (définie en 1.3 comme l'homologie du cône $co(.n)$ de la multiplication $.n : C_* \to C_*$) est telle que pour $r \geq 2$, on ait $H_r(C_*; \mathbf{Z}/n) = \pi_r(X(C_*); \mathbf{Z}/n)$.

En conclusion, on a

Proposition 25 *Pour $r \geq 2$, le diagramme $(0)_r^n$ est obtenu par application du foncteur $\pi_r(-; \mathbf{Z}/n)$ au diagramme (1).*

Pour $r = 1$, contentons-nous de traiter le cas de l'homologie cyclique négative en détaillant la construction de l'application $\gamma_1^{(n)}$ du diagramme $(0)_1^n$. Les constructions pour l'homologie de Hochschild ou périodique sont analogues.

Soit SA le cône de l'anneau A au sens de [13], p. 269. D'après [23], prop. 3.2, pour $r \geq 1$, on a $K_r(SA) \cong K_{r-1}(A)$. En particulier, $\pi_2(BGL(SA)^+) \cong K_1(A)$. D'après [27], thm. 10.1 et sa remarque 2, pour $r \geq 1$, on a $HC_r^-(SA) \cong HC_{r-1}^-(A)$. En particulier, $\pi_2(\mathcal{H}^-(SA)) \cong HC_1^-(A)$.

L'application $\gamma' : BGL(SA)^+ \to \mathcal{H}^-(SA)$ obtenue en appliquant la proposition 25 à l'anneau SA permet de définir $\gamma_1^{(n)} = \pi_1(\gamma'; \mathbf{Z}/n)$, $K_1(A; \mathbf{Z}/n) = \pi_2(BGL(SA)^+; \mathbf{Z}/n)$ et $HC_1^-(A; \mathbf{Z}/n)) = \pi_2(\mathcal{H}^-(SA); \mathbf{Z}/n)$. On a $\gamma_1^{(n)} : K_1(A; \mathbf{Z}/n) \to HC_1^-(A; \mathbf{Z}/n)$. Les suites exactes longues de Barratt pour l'homotopie à coefficients ([19], p. 3) nous donnent

Proposition 26 *On a le diagramme commutatif naturel à lignes exactes*

$$\begin{tikzcd}
K_1(A) \arrow[r, ".n"] \arrow[d, "\gamma_1"] & K_1(A) \arrow[r, "\rho"] \arrow[d, "\gamma_1"] & K_1(A; \mathbf{Z}/n) \arrow[r, "\partial"] \arrow[d, "\gamma_1^{(n)}"] & K_0(A) \arrow[r, ".n"] \arrow[d, "\gamma_0"] & K_0(A) \arrow[r] \arrow[d, "\gamma_0"] & K_0(A)/(n) \arrow[d, "\overline{\gamma}_0"] \\
HC_1^-(A) \arrow[r, ".n"] & HC_1^-(A) \arrow[r, "\rho"] & HC_1^-(A; \mathbf{Z}/n) \arrow[r, "\partial"] & HC_0^-(A) \arrow[r, ".n"] & HC_0^-(A) \arrow[r] & HC_0^-(A; \mathbf{Z}/n)
\end{tikzcd}$$

REMARQUE 27. Il est raisonnable de conjecturer que l'application composée

$$K_1(A; \mathbf{Z}/n) \xrightarrow{\gamma_1^{(n)}} HC_1^-(A; \mathbf{Z}/n) \xrightarrow{h_1^{(n)}} HH_1(A; \mathbf{Z}/n)$$

est celle décrite en 1.5.

2 Étude de l'anneau des entiers d'un corps de nombres.

Soit A l'anneau des entiers d'un corps de nombres F. D'après [3], on a $K_1(A) = A^\times$. L'extension (‡) 1.1 s'écrit donc

$$(\dagger) \qquad 1 \longrightarrow A^\times/(n) \xrightarrow{\rho} K_1(A; \mathbf{Z}/n) \xrightarrow{\partial} Cl(A)_{(n)} \longrightarrow 0$$

ce qui montre que $K_1(A; \mathbf{Z}/n)$ est une extension de la n-torsion du groupe des classes de A par un quotient du groupe des unités de A.

La trace de Dennis $D_1^{(n)}$ et la classe caractéristique secondaire $d_1^{(n)}$ construites en 1.6 s'insèrent dans le diagramme commutatif

$$\begin{tikzcd} K_1(A;\mathbf{Z}/n) \arrow[r, "\partial"] \arrow[d, "D_1^{(n)}"'] & Cl(A)_{(n)} \arrow[r] \arrow[d, "d_1^{(n)}"] & 0 \\ \Omega^1_{dR}(A)/(n) \arrow[r] & \Omega^1_{dR}(A)/S \arrow[r] & 0 \end{tikzcd}$$

En 2.1, on montre que $K_1(A;\mathbf{Z}/n)$ est isomorphe à un groupe noté $\mathcal{U}(A;\mathbf{Z}/n)$ construit à partir d'idéaux fractionnaires de A. Le lemme (N-N_1) de la section 2.2 fournit un critère de construction d'éléments de $\mathcal{U}(A;\mathbf{Z}/n)$. En 2.3, on décrit le lien entre $K_1(A;\mathbf{Z}/n)$ et le groupe des adèles restreints $\widehat{A}$ de A. Les traces $D_1^{(n)}$ et $d_1^{(n)}$ sont détaillées en 2.5.

2.1 Description de $K_1(A;\mathbf{Z}/n)$ en termes d'idéaux.

Soit A un anneau de Dedekind, de corps des fractions F et soit $n \geq 2$ un entier. On désigne par $I(A)$ le monoïde des idéaux fractionnaires de A. Pour $x \in F$, on pose $[x] = x \bmod F^{\times(n)}$. Considérons le sous-groupe $\mathcal{U}(A;\mathbf{Z}/n)$ de $F^\times/(n)$ défini par

$$\mathcal{U}(A;\mathbf{Z}/n) := \{x \in F^\times/(n) \mid \exists\, I \in I(A),\ xA = I^n\}\cdot$$

Théorème 28 *Soit A un anneau de Dedekind. Alors, on a un isomorphisme*

$$K_1(A;\mathbf{Z}/n) \cong \mathcal{U}(A;\mathbf{Z}/n) \oplus SK_1(A)/(n).$$

Preuve : on sait que dans un anneau de Dedekind, tout module P projectif de type fini et de rang r est de la forme $P = (r-1)A \oplus I$ où I est un idéal fractionnaire de A. Soit $[P, \alpha, L]$ un élément de $K_1(A;\mathbf{Z}/n)$ avec $P = (r-1)A \oplus I$ et $L = rA$. L'isomorphisme $\alpha : nP \cong nL$ montre qu'il existe $x \in F^\times$ tel que $I^n = xA$. Définissons $\det^{(n)} : K_1(A;\mathbf{Z}/n) \to \mathcal{U}(A;\mathbf{Z}/n)$ par $\det^{(n)}([P,\alpha,L]) = [x]$. On vérifie que $\det^{(n)}$ est bien définie et que c'est un morphisme de groupes. Pour obtenir le facteur direct $\mathcal{U}(A;\mathbf{Z}/n)$ de $K_1(A;\mathbf{Z}/n)$, on construit un morphisme $s : \mathcal{U}(A;\mathbf{Z}/n) \to K_1(A;\mathbf{Z}/n)$ tel que $\det^{(n)} \circ s = \mathrm{id}_{\mathcal{U}(A;\mathbf{Z}/n)}$. Soit $[x] \in \mathcal{U}(A;\mathbf{Z}/n)$ avec $xA = I^n$ où I est un idéal fractionnaire de A. On pose $s([x]) = [A, \mathrm{id}_{(n-1)A} \oplus \cdot x, I]$. On vérifie que s est bien définie. Pour montrer $s([x][y]) = s([x]) + s([y])$, posons $xA = I^n$, $yA = J^n$, $s([x]) = u$, $s([y]) = v$, $s([x][y]) = w$, avec $u = [A, f, I]$, $f = \mathrm{id}_{(n-1)A} \oplus \cdot x$,

$v = [A, g, J]$, $g = \cdot y \oplus \mathrm{id}_{(n-1)A}$, $w = [A, h, IJ]$, $h = \cdot xy \oplus \mathrm{id}_{(n-1)A}$. On a $u+v = [A \oplus A, h_1, I \oplus J]$ où h_1 est l'isomorphisme $\mathrm{id}_{(n-1)A} \oplus \cdot x \oplus \cdot y \oplus \mathrm{id}_{(n-1)A}$. Posons $h_2 = \mathrm{id}_{nA} \oplus h$. Dans la catégorie $\mathcal{C}$, (*cf.* 1.1), les objets $(A \oplus A, h_1, I \oplus J)$ et $(A \oplus A, \mathrm{id}_{nA} \oplus h, A \oplus IJ)$ sont isomorphes. Dans $K_1(A; \mathbf{Z}/n)$, on a par conséquent $u + v = [A \oplus A, h_1, I \oplus J] = [A, \mathrm{id}_{nA}, A] + [A, h, IJ] = 0 + w = w$, ce qui montre que s est un morphisme de groupes. On vérifie la relation $\det^{(n)} \circ s = \mathrm{id}_{\mathcal{U}(A;\mathbf{Z}/n)}$, ce qui montre

$$K_1(A; \mathbf{Z}/n) = \mathcal{U}(A; \mathbf{Z}/n) \oplus \ker\ \det^{(n)} .$$

Introduisons le diagramme

$$\begin{tikzcd}
K_1(A) \arrow[r, "\cdot n"] \arrow[d, "\det"] & K_1(A) \arrow[r, "\rho"] \arrow[d, "\det"] & K_1(A; \mathbf{Z}/n) \arrow[r, "\partial"] \arrow[d, "\det^{(n)}"] & K_0(A) \arrow[r, "\cdot n"] \arrow[d, "\mathrm{id}"] & K_0(A) \arrow[d, "\mathrm{id}"] \\
A^\times \arrow[r, "\cdot n"] & A^\times \arrow[r, "\rho'"] & \mathcal{U}(A; \mathbf{Z}/n) \arrow[r, "\partial'"] & K_0(A) \arrow[r, "\cdot n"] & K_0(A)
\end{tikzcd}$$

où les applications ρ' et ∂' sont définies par $\rho'(a) = [a]$, $\partial'([x]) = [I^{-1}]$. Ce diagramme est commutatif à lignes exactes. La suite exacte des noyaux des flèches verticales conduit à $\ker \det^{(n)} \cong SK_1(A)/(n)$.

Corollaire 29 *Soit A l'anneau des entiers d'un corps de nombres F. Alors*

$$K_1(A; \mathbf{Z}/n) \cong \mathcal{U}(A; \mathbf{Z}/n).$$

En effet, d'après [BMS], on a $SK_1(A) = 0$.

2.2 Le lemme $(N\text{-}N_1)$ de construction d'éléments de $K_1(A; \mathbf{Z}/n)$.

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

Pour $z \in L$, on désigne 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 30 *Soit $z \in L$ (resp. B) et $h \in F$ (resp. A). Alors on a*

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

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 31 *Soit L/F une extension de corps de nombres et soient A l'anneau des entiers de F et B la fermeture intégrale de A dans L. Soit n un entier ≥ 2. Considérons un élément u de B tel que*

$$\begin{aligned} & N(u) = ea^n \text{ avec } e \in A^\times,\ a \in A \\ \text{et} \quad & (N(u), N_1(u)) = A. \end{aligned}$$

En désignant par $[u]$ la classe de u dans $L^\times/(n)$, on a alors

$$[u] \in K_1(B; \mathbf{Z}/n).$$

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

Pour montrer que $[u]$ appartient à $K_1(A; \mathbf{Z}/n)$, on remarque que la puissance n-ième de l'idéal fractionnaire $I = (u, a)$ de B est principale. En effet $I^n = (u^n, N(u)) = (u^n, u \prod_{\sigma \neq \mathrm{id}} \sigma(u))$; et puisque $(u, \sigma(u)) = B$, on en déduit $I^n = uB$. Ceci montre $[u] \in \mathcal{U}(B; \mathbf{Z}/n)$. □

2.3 Description de $K_1(A; \mathbf{Z}/n)$ en termes d'adèles.

Soit A l'anneau des entiers d'un corps de nombres F. Notons $Spec(A)$ le spectre premier de A. Pour $\mathfrak{p}$ dans $Spec(A)$, on désigne par $\widehat{A}_\mathfrak{p}$ le complété $\mathfrak{p}$-adique de l'anneau de valuation discrète $A_\mathfrak{p}$. L'anneau $\widehat{A} = \prod_{\mathfrak{p} \in Spec(A)} \widehat{A}_\mathfrak{p}$, appelé anneau des adèles restreints de A, s'insère dans le diagramme commutatif

$$\begin{tikzcd} A \arrow[r, hook] \arrow[d, hook] & \widehat{A} \arrow[d, hook] \\ F \arrow[r] & \widehat{F} \end{tikzcd}$$

où on a posé $\widehat{F} = F \otimes_A \widehat{A}$.

Considérons le diagramme

$$\begin{tikzcd} \mathcal{U}(A;\mathbf{Z}/n) \arrow[r, "j"] \arrow[d, "\imath"'] & F^\times/(n) \arrow[d, "\bar{\imath}"] \\ \widehat{A}^\times/(n) \arrow[r, "\bar{j}"'] & \widehat{F}^\times/(n) \end{tikzcd}$$

Les applications $\imath$, j et $\overline{j}$ sont trivialement injectives. Dans l'anneau $\widehat{A}$, on s'est restreint aux places archimédiennes. D'après [1], Chap. X.I, dans cette situation, l'application $\bar{\imath}$ est également injective. La somme amalgamée $\widehat{A}^\times/(n) \oplus_{\widehat{F}^\times/(n)} F^\times/(n)$ est donc égale à $\widehat{A}^\times/(n) \cap F^\times/(n)$. Soit $x \in F^\times/(n)$. L'élément $[x] = x \bmod F^{\times(n)}$ de $F^\times/(n)$ appartient à $\widehat{A}^\times/(n)$ si et seulement si $n \mid v_{\mathfrak{p}}(x_{\mathfrak{p}})$ pour tout $\mathfrak{p} \in Spec(A)$, c'est-à-dire qu'on a $xA = I^n$ avec I idéal fractionnaire. En conclusion, nous avons :

Proposition 32 *Soit A l'anneau des entiers d'un corps de nombres F et soit $n \geq 2$ un entier. Alors le groupe $K_1(A;\mathbf{Z}/n)$ s'identifie au sous-groupe $\widehat{A}^\times/(n) \cap F^\times/(n)$ de $\widehat{F}^\times/(n)$.*

Corollaire 33 *Soit A l'anneau des entiers d'un corps de nombres F. Posons $\widehat{A} = \prod_{\mathfrak{p}} \widehat{A}_{\mathfrak{p}}$. Alors l'application $K_1(A;\mathbf{Z}n) \to K_1(\widehat{A};\mathbf{Z}/n)$ induite par $A \to \widehat{A}$ est l'inclusion $\widehat{A}^\times/(n) \cap F^\times/(n) \to \widehat{A}^\times/(n)$.*

Preuve : Calculons $K_1(\widehat{A};\mathbf{Z}/n)$. Rappelons pour cela que si $(A_i)_{i\in I}$ est une famille d'anneaux commutatifs de rang stable $d \geq 2$ au sens de [2], p. 231, on a $K_1(\prod_{i\in I} A_i) \cong \prod_{i\in I} K_1(A_i)$ et $\widetilde{K}_0(\prod_{i\in I} A_i) \cong \prod_{i\in I} \widetilde{K}_0(A_i)$. Les anneaux de la famille $(\widehat{A}_{\mathfrak{p}})_{\mathfrak{p}\in Spec(A)}$ sont tous de rang stable $d = 2$. De $\widetilde{K}_0(\widehat{A}_{\mathfrak{p}})_{(n)} = 0$ et $K_1(\widehat{A}_{\mathfrak{p}}) = \widehat{A}_{\mathfrak{p}}^\times$, on tire $K_1(\widehat{A}) = \widehat{A}^\times$. L'extension (‡ 1.1) nous mène à

$$K_1(\widehat{A};\mathbf{Z}/p) = \widehat{A}^\times/(n).$$

2.4 Description de $\Omega^1_{dR}(A)/(n)$.

On désigne toujours par A l'anneau des entiers d'un corps de nombres F. L'anneau $A \otimes \mathbf{Z}_p$ est toujours considéré comme une algèbre sur l'anneau $\mathbf{Z}_p$

des entiers p-adiques. Désignons par δ le discriminant du corps F. D'après [15], prop. 1.5, on a les égalités suivantes

$$\Omega^1_{dR}(A) = \Omega^1_{dR}(\widehat{A}) = \oplus_{p|\delta}\Omega^1_{dR}(A \otimes \mathbf{Z}_p).$$

Supposons n et p premiers entre eux, alors n appartient à $(\mathbf{Z}_p)^\times$ et $\Omega^1_{dR}(A \otimes \mathbf{Z}_p)/(n) = 0$. On en déduit :

Proposition 34 *Soit F un corps de nombres d'anneaux d'entiers A et de discriminant δ. Soit $n > 1$ un entier.*
a) Si $n \mid \delta$, alors $\Omega^1_{dR}(\widehat{A})/(n) = \Omega^1_{dR}(A)/(n) = \oplus_{p|(n,\delta)}\Omega^1_{dR}(A \otimes \mathbf{Z}_p)/(n)$.
En particulier, si p est un nombre premier ramifié dans A, on a

$$\Omega^1_{dR}(A)/(p) \cong \Omega^1_{dR}(A \otimes \mathbf{Z}_p)/(p).$$

b) si $(n, \delta) = 1$, alors $\Omega^1_{dR}(\widehat{A})/(n) = \Omega^1_{dR}(A)/(n) = 0$.
En particulier, si p est un nombre premier non ramifié dans A, alors on a $\Omega^1_{dR}(A)/(p) = 0$.

2.5 Description de la trace de Dennis à coefficients

Soit A l'anneau des entiers d'un corps de nombres F et soit n un diviseur du discriminant de F. Pour les éléments de $K_1(A; \mathbf{Z}/n)$ obtenus grâce au lemme (N-N_1), il est facile de décrire la trace de Dennis à coefficients. Supposons que $u \in A$ satisfasse aux hypothèses du lemme (N-N_1) et que de plus $N(u)$ soit un entier premier à n. Posons $v = \prod_{\sigma \neq \mathrm{id}} \sigma(u)$. On a $v \in A$ et $uv = N(u)$. Dans $\Omega^1_{dR}(A)/(n)$, on en déduit $D_1^{(p)}([u]) = N(u)^{-1} v du \bmod n$.

L'égalité $K_1(A; \mathbf{Z}/n) \cong F^\times/(n) \cap \widehat{A}^\times/(n)$ permet également de décrire localement la trace de Dennis à coefficients. Pour cela, on remarque que le diagramme suivant est commutatif.

$$\begin{tikzcd}
K_1(A; \mathbf{Z}/n) \arrow[r, "D_1^{(n)}"] \arrow[d, hook] & \Omega^1_{dR}(A)/(n) \arrow[d, equal] \\
K_1(\widehat{A}; \mathbf{Z}/n) \arrow[r, "D_1^{(n)}"] & \Omega^1_{dR}(\widehat{A})/(n)
\end{tikzcd}$$

Pour connaître la trace de Dennis à coefficients de A, il suffit donc de connaître celle de $\widehat{A}$. Soit p un nombre premier ramifié dans A. Localement, la trace de Dennis à coefficients est essentiellement une dérivée logarithmique modulo p. En effet, on écrit

$$K_1(\widehat{A};\mathbf{Z}/p) = \prod_{\mathfrak{p}\cap\mathbf{Z}\neq(p)} \widehat{A}_{\mathfrak{p}}^{\times}/(p) \oplus \prod_{\mathfrak{p}\cap\mathbf{Z}=(p)} \widehat{A}_{\mathfrak{p}}^{\times}/(p).$$

La restriction de $D_1^{(p)}$ au premier facteur de cette décomposition est évidemment nulle puisque pour $\mathfrak{p}\cap\mathbf{Z}\neq(p)$, on a $\Omega^1_{dR}(\widehat{A}_{\mathfrak{p}})/(p)=0$. Pour $\mathfrak{p}\cap\mathbf{Z}=(p)$ et $[u_{\mathfrak{p}}]\in\widehat{A}_{\mathfrak{p}}^{\times}/(p)$, d'après l'exemple du théorème 23, on a

$$D_1^{(p)}([u_{\mathfrak{p}}]) = u_{\mathfrak{p}}^{-1}du_{\mathfrak{p}} \bmod p\Omega^1_{dR}(\widehat{A}_{\mathfrak{p}}).$$

3 Applications aux corps de petit degré.

3.1 Un théorème de Y. Yamamoto.

L'égalité $K_1(A;\mathbf{Z}/n) = \mathcal{U}(A;\mathbf{Z}/n)$ et le lemme (N,N_1) permettent de retrouver un théorème montré par Y. Yamamoto [28] à l'aide de méthodes distinctes.

Théorème 35 *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 $\mathbf{Z}^2$ 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 $\mathbf{Z}/n\oplus\mathbf{Z}/n$.

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

Preuve : L'application $f : A \to \mathbf{Z}/b$ définie par $f((x+y\sqrt{\delta})/2) = (x+y\alpha)/2$ est un morphisme d'anneaux. On note $f_1^{(d))} : K_1(A;\mathbf{Z}/d) \to K_1(\mathbf{Z}/b;\mathbf{Z}/d)$ l'application induite par f en K-théorie à coefficients d. Remarquons que $K_1(\mathbf{Z}/b;\mathbf{Z}/d) = (\mathbf{Z}/b)^\times/(d)$. 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 $K_1(A;\mathbf{Z}/d)$. 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 $K_1(A;\mathbf{Z}/p)$ n'est donc pas trivial. Montrons que $[u] \in F^\times/(n)$ définit un élément d'ordre n de $K_1(A;\mathbf{Z}/n)$. Supposons $[u]$ d'ordre m avec $1 \leq m < n$. Il existe 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 $K_1(A;\mathbf{Z}/p)$. On vient de montrer que ceci est impossible. On a donc $[u]$ d'ordre n dans $K_1(A;\mathbf{Z}/n)$. Le sous-groupe H de $K_1(A;\mathbf{Z}/n)$ engendré par $[u]$ est donc isomorphe à $\mathbf{Z}/n$.

On introduit de manière analogue $u' = (\alpha'+\sqrt{\delta})/2$ et on obtient de même un sous-groupe H' de $K_1(A;\mathbf{Z}/n)$, également isomorphe à $\mathbf{Z}/n$. Pour montrer la somme directe $H \oplus H'$dans $K_1(A;\mathbf{Z}/n)$, on remarque que $f(u') = (\alpha'+\alpha)/2 \in \mathbf{Z}/b$. Si $u' \in H$, c'est-à-dire $u' = u^m$ avec $1 \leq m < n$, 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 $\alpha \in (\mathbf{Z}/b)^{\times(p)}$, ce qui fournit la contradiction recherchée. On montre de même $u \notin H'$. En conclusion, sous les hypothèses proposées, le groupe $K_1(A;\mathbf{Z}/n)$ contient un sous-groupe isomorphe à $\mathbf{Z}/n \oplus \mathbf{Z}/n$. De l'extension (†) p. 20, on déduit que si F est imaginaire, $Cl(A)_{(n)}$ contient $\mathbf{Z}/n \oplus \mathbf{Z}/n$ en facteur direct. Si $\delta > 0$, $A^\times/(n)$ est isomorphe à $\mathbf{Z}/n$ et donc $Cl(A)_n$ contient $\mathbf{Z}/n$ en facteur direct.

Remarque 36. Dans le cas où F est réel d'unité fondamentale ε telle qu'il existe un diviseur premier p pour lequel $f(\varepsilon) \in (\mathbf{Z}/b)^{\times(p)}$, le groupe des classes contient un sous-groupe isomorphe à $\mathbf{Z}/n \oplus \mathbf{Z}/n$. En effet, soit $t = \partial([u])$ toujours avec $u = (\alpha+\sqrt{\delta})/2$. Montrons que t est d'ordre n dans $Cl(A)$. Supposons $t^m = 0$ avec $1 \leq m < n$. 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 $f(\varepsilon) \in (\mathbf{Z}/b)^{\times(p)}$. on en déduit $\alpha \in (\mathbf{Z}/b)^{\times(p)}$, situation exclue. Le sous-groupe $H(t)$ engendré par t dans $Cl(A)$ est donc isomorphe à $\mathbf{Z}/n$. La fin de la démonstration est analogue à celle du théorème. Les sous-groupes $H(t)$ et $H(t')$ engendrés respectivement par $t = \partial([(\alpha+\sqrt{\delta})/2])$ et $t' = \partial([(\alpha'+\sqrt{\delta})/2])$ sont en somme directe dans $Cl(A)$.

Ces éléments du groupe des classes ont été construits pour la première fois par Yamamoto ([28]). 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 $\mathbf{Z}/n$. □

3.2 Construction d'éléments non triviaux de $Cl(A)_{(n)}$.

Soit F un corps de nombres d'anneaux d'entiers A. Soit r_1 (resp. $2r_2$) le nombre de plongements réels (resp. complexes) de F. Si $r = r_1 + r_2 - 1$, on a $rg(A^\times) = r$ et $A^\times = K_1(A) = \mu \times \prod_{i=1}^{r} \mathbf{Z}\varepsilon_i$ où μ est le groupe des racines de l'unité contenues dans A et où $\{\varepsilon_i,\ 1 \leq i \leq r\}$ est un système fondamental d'unités de A.

Lorsque A possède "peu" d'unités, l'extension (†) p. 20 permet d'obtenir des élements non triviaux de $Cl(A)_{(n)}$ à partir d'éléments de $K_1(A;\mathbf{Z}/n)$.

L'égalité $K_1(A;\mathbf{Z}/n) = \mathcal{U}(A;\mathbf{Z}/n)$ et le lemme (N-N_1) conduisent au résultat suivant :

Proposition 37 *Soit F un corps de nombres, d'anneau d'entiers A et soit n un entier naturel. On suppose qu'il existe $z \in A$ tel que $N(z) = b^n$, $(N(z), N_1(z)) = 1$ et que pour tout diviseur m de n, $1 \leq m < n$, b^m ne soit pas la norme d'un élément de F. Alors $[z] = z \bmod F^{\times(n)}$ est un élément d'ordre n de $K_1(A;\mathbf{Z}/n)$.*
Si $r_1 + r_2 - 1 = 0$, on a $Cl(A)_{(n)} \neq 0$. Si $r_1 + r_2 - 1 \neq 0$ et si $-b$ n'est pas la norme d'un élément de F, alors $Cl(A)_{(n)} \neq 0$.

Preuve : d'après le lemme (N-N_1), $[z]$ appartient à $K_1(A;\mathbf{Z}/n)$. Si $[z]$ est d'ordre m, $1 \leq m < n$, il existe $u \in F^\times$ tel que $z^m = u^n$, c'est-à-dire $z = u^s$ avec $s = n/m$. L'équation $N(z) = N(u)^s$ s'écrit $b^m = N(u)$, ce qui n'est pas. Notons comme toujours $\partial : K_1(A;\mathbf{Z}/p) \to Cl(A)_{(n)}$ 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 $N(z) = \pm N(u)^n$ (avec le signe + si $r = 0$) soit $b = \pm N(u)$, ce qui n'est pas.

□

La classe caractéristique secondaire

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

introduite en 1.6, corollaire 23 conduit au résultat suivant.

Proposition 38 *Soit F un corps de nombres d'anneaux d'entiers A. On pose $r = r_1 + r_2 - 1$ et $A^\times = \mu \times \prod_{i=1}^{r} \mathbf{Z}\varepsilon_i$. Soit n un diviseur du discriminant du corps F.*

On suppose
1) Pour tout $\xi \in \mu$, $\xi^{-1}d\xi \equiv 0 \bmod n\Omega^1_{dR}(A)$.
2) Pour tout i, $1 \leq i \leq r$, $\varepsilon_i^{-1}d\varepsilon_i \equiv 0 \bmod n\Omega^1_{dR}(A)$.
3) Il existe $u \in A$ avec $N(u) = b^n$, $(N(u), N_1(u)) = 1$, et
$u^{-1}du \not\equiv 0 \bmod n\Omega^1_{dR}(A)$. Alors $Cl(A)_{(n)} \neq 0$.

Preuve : les hypothèses 1 et 2 montrent que $dA^\times/A^\times \equiv 0 \bmod n\Omega^1_{dR}(A)$. L'application $d_1^{(n)}$, de source $Cl(A)_{(n)}$ est donc de but $\Omega^1_{dR}(A)/(n)$. D'après le lemme (N-N_1), les hypothèses 3 fournissent l'élément $[u] = u \bmod F^{\times(n)}$ de $K_1(A; \mathbf{Z}/n)$. De cet élément, on déduit $x = \partial([u])$ dans $Cl(A)_{(n)}$. On a $d_1^{(n)}(x) = u^{-1}du \bmod n\Omega^1_{dR}(A)$, quantité non nulle par hypothèse, ce qui montre que x est non trivial. □

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

3.3 Exemples de n-torsion du groupe des classes : cas d'un corps quadratique imaginaire.

Proposition 39 *Soit F un corps quadratique d'anneau d'entiers A et de discriminant $\delta < 0$ et soit n un entier impair. On suppose qu'il existe $(\alpha, b) \in \mathbf{Z}^2$ tel que $\alpha^2 - 4b^n = \delta$, avec $(\alpha, b) = 1$. On suppose de plus que pour tout diviseur m de n, $1 \leq m < n$, la quantité $\delta + 4b^n$ n'est pas un carré parfait. Alors $Cl(A)_{(n)} \neq 0$.*

Remarque 40. Sous les mêmes hypothèses, si δ est positif et si de plus $\pm b$ n'est pas une norme, la conclusion $Cl(A)_{(n)} \neq 0$ subsiste.

Preuve : on applique la proposition 37 à $z = \dfrac{\alpha + \sqrt{\delta}}{2}$. L'équation $z^m = u^n$ conduit à $\delta + 4b^n$ carré parfait.

Dans les quelques exemples ci-dessous, l'anneau A des entiers du corps $\mathbf{Q}[\sqrt{\delta}]$ est tel que $Cl(A)_{(n)} \neq 0$.

$n = 3$
$\delta = -104 = 2^2 - 4 \cdot 3^3 = 4 \cdot\ (-26)$
$\delta = -5\ 320 = 2^2 - 4 \cdot\ 11^3 = 4 \cdot\ (-1330)$
$\delta = -48\ 664 = 2^2 - 4 \cdot\ 23^3 = 4 \cdot\ (-12\ 166)$
$n = 5$
$\delta = -127 = 1^2 - 4 \cdot\ 2^5$
$\delta = -12\ 499 = 1^2 - 4 \cdot\ 5^5$
$\delta = -31\ 103 = 1^2 - 4 \cdot\ 6^5$
$\delta = -131\ 071 = 1^2 - 4 \cdot\ 8^5$
$\delta = -399\ 999 = 1^2 - 4 \cdot\ 10^5$
$n = 7$
$\delta = -511 = 1^2 - 4 \cdot\ 2^7$
$\delta = -65\ 535 = 1^2 - 4 \cdot\ 4^7$
$\delta = -312\ 499 = 1^2 - 4 \cdot\ 5^7$
$n = 9$
$\delta = -2047 = 1^2 - 2^9$
$\delta = -78\ 728 = 2^2 - 3^9 = 4 \cdot\ (-19\ 682)$
$\delta = -78731 = 1^2 - 3^9$
$n = 11$
$\delta = -8191 = 1^2 - 2^{11}$
$\delta = -708\ 584 = 2^2 - 3^{11} = 4 \cdot\ (-177\ 146)$
$\delta = -708\ 587 = 1^2 - 3^{11}$

3.4 Exemples de n-torsion ramifiée du groupe des classes : cas d'un corps quadratique

Soit F un corps de nombres quadratique de discriminant δ. Si $\delta < 0$, on exclut les deux cas $\delta = -4$ et $\delta = -3$ pour lesquels le groupe des classes est trivial et le groupe des unités n'est pas réduit à $\mathbf{Z}/2$.

On pose $\omega = \frac{\sqrt{\delta}}{2}$ ou $\omega = \frac{1+\sqrt{\delta}}{2}$ suivant que $\delta \equiv\ 0 \bmod 4$ ou $\delta \equiv 1 \bmod 4$. L'anneau A des entiers du corps F est $\mathbf{Z}[\omega]$. Posons $P = X^2 - \delta$ si $\delta \equiv\ 0 \bmod 4$ et $P = X^2 - X + (1-\delta)/4$ sinon. L'homologie de Hochschild de A est donnée par la

Proposition 41
a) Si $\delta \equiv 1 \bmod 4$, *on a* $\Omega^1_{dR}(A) = \mathbf{Z}/\delta\ d\omega$ *et* $\omega d\omega = \frac{1}{2} d\omega$.

b) Si $\delta \equiv 0 \bmod 4$, on a $\Omega^1_{dR}(A) = \mathbf{Z}/(\delta/2)\ d\omega \oplus \mathbf{Z}/2\ \omega d\omega$.

On en déduit

Proposition 42
a) Soit n un diviseur impair du discriminant δ du corps quadratique F. Alors on a $\Omega^1_{dR}(A)/(n) = \mathbf{Z}/n d\omega$ avec $\omega d\omega = \frac{1}{2} d\omega$ si $\delta \equiv 1 \bmod 4$ et $\omega d\omega = 0$ si $\delta \equiv 0 \bmod 4$.
b) on suppose $\delta \equiv 0 \bmod 4$ et n diviseur pair de δ. Alors on a

$$\Omega^1_{dR}(A)/(n) = \mathbf{Z}/n\ d\omega \oplus \mathbf{Z}/2\ \omega d\omega.$$

Tout élément z de A s'écrit $z = \dfrac{\alpha + \beta\sqrt{\delta}}{2}$ avec α et β dans $\mathbf{Z}$. On note $N(z)$ sa norme, $N_1(z) = tr(z)$ sa trace et $\sigma(z)$ son conjugué. On a $\sigma(z) = \dfrac{\alpha - \beta\sqrt{\delta}}{2}$, $tr(z) = \alpha$ et $N(z) = \dfrac{\alpha^2 - \delta\beta^2}{4}$. Dans $\Omega^1_{dR}(A)$, on a la relation $N(z)z^{-1}dz = \sigma(z)dz$.

Supposons que n soit un diviseur impair du discriminant δ. De $N(z) \equiv \alpha^2/4 \mod n\mathbf{Z}$ et de $\sigma(z)dz \equiv \frac{\alpha\beta}{2} d\omega \mod n\Omega^1_{dR}(A)$, on déduit que si $(N(z), n) = 1$, on a $z^{-1}dz \equiv \dfrac{2\beta}{\alpha} d\omega \mod n\Omega^1_{dR}(A)$.

En particulier, si F est réel et si $\varepsilon = \dfrac{\varepsilon_1 + \varepsilon_2\sqrt{\delta}}{2}$ est l'unité fondamentale de A, on a toujours $(\varepsilon_1, n) = 1$ et donc $\varepsilon^{-1}d\varepsilon \equiv 0 \bmod n\Omega^1_{dR}(A)$ si et seulement si n divise ε_2. Dans ce cas, on a $dA^\times/A^\times \equiv 0 \bmod n\Omega^1_{dR}(A)$. On en déduit

$$\Omega^1_{dR}(A)/(n, dA^\times/A^\times) = \Omega^1_{dR}(A)/(n) = \mathbf{Z}/n\ dw.$$

On obtient la classe caractéristique

$$d_1^{(n)} : Cl(A)_{(n)} \to \mathbf{Z}/n\ dw$$

Enfin, si $u = \dfrac{\alpha + \beta\sqrt{\delta}}{2}$ est un élément de A tel que $(\beta, n) = (\alpha, n) = 1$, alors $u^{-1}du \equiv \frac{2\beta}{\alpha} d\omega \bmod n$ est une quantité non nulle de $\mathbf{Z}/n\ d\omega$. De tout ceci, on déduit que la proposition 38 prend la forme :

Proposition 43 *Soit F un corps quadratique de discriminant δ et d'anneau d'entiers A. Soit n un diviseur impair de δ. Si F est réel, on suppose que l'unité fondamentale $\varepsilon = \dfrac{\varepsilon_1 + \varepsilon_2\sqrt{\delta}}{2}$ est telle que $n|\varepsilon_2$. Soient $(\alpha, \beta, b)) \in \mathbf{Z}^3$ une solution de l'équation $\alpha^2 - 4b^n = \delta\beta^2$ avec $(b, \alpha) = (\beta, n) = (\alpha, n) = 1$. Alors $Cl(A)$ possède un élément d'ordre n.*

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

Proposition 44 *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 $\varepsilon = \dfrac{\varepsilon_1+\varepsilon_2\sqrt{\delta}}{2}$ de A est telle que $n|\varepsilon_2$. Alors $Cl(A)_{(n)} \neq 0$.*

Dans les quelques exemples ci-dessous, l'anneau A des entiers du corps $\mathbf{Q}[\sqrt{\delta}]$ est tel que $Cl(A)$ possède un élément d'ordre n.
$n = 3$
$\delta = 231 = 17^2 - 4\cdot(-2)^3 = \mathbf{3}\cdot 107$, d'unité fondamentale $\varepsilon = (430+24\sqrt{\delta})/2$.
$\delta = -231 = 5^2 - 4\cdot\ 4^3 = -\mathbf{3}\cdot\ 7\cdot\ 11$
$\delta = -255 = 1^2 - 4\cdot\ 4^3 = -\mathbf{3}\cdot\ 5\cdot\ 17$
$\delta = -16\ 383 = 1^2 - 4\cdot\ 16^3 = -\mathbf{3}\cdot\ 43\cdot\ 127$
$\delta = -62\ 484 = 4^2 - 4\cdot\ 25^3 = 4\cdot\ (-\mathbf{3}\cdot\ 41\cdot\ 127)$
$\delta = -3\ 999\ 999 = 1^2 - 4\cdot\ 100^3 = -\mathbf{3}\cdot\ 23\cdot\ 29\cdot\ 1999$
$n = 5$
$\delta = -236\ 195 = 1^2 - 4\cdot\ 9^5 = -\mathbf{5}\cdot\ 97\cdot\ 487$
$\delta = -644\ 195 = 3^2 - 4\cdot\ 11^5 = -\mathbf{5}\cdot\ 19\cdot\ 6\ 781$
$\delta = -9\ 904\ 380 = 4^2 - 4\cdot\ 19^2 = 4\cdot\ (-3\cdot\ \mathbf{5}\cdot\ 383\cdot\ 431)$
$n = 7$
$\delta = -511 = 1^2 - 4\cdot\ 2^7 = -\mathbf{7}\cdot\ 23$
$\delta = -65\ 527 = 3^2 - 4\cdot\ 4^7 = -\mathbf{7}\cdot\ 11\cdot\ 23\cdot\ 37$
$n = 11$
$\delta = -708\ 587 = 1^2 - 4\cdot\ 3^{11} = -\mathbf{11}\cdot\ 37\cdot\ 1741$
$n = 15$
$\delta = -4\ 294\ 967\ 295 = 1^2 - 4\cdot\ 4^{15} = -\mathbf{3}\cdot\ \mathbf{5}\cdot\ 17\cdot\ 257\cdot\ 65\ 537$

4 Applications à la cyclotomie.

4.1 Notations et stratégie générale.

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

G. On désigne par s, $1 < s \leq p-1$, 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 $\mathbf{Z}[\zeta]$. Soient $Cl(A)$ le groupe des classes de A et $h = h_p$ le nombre de classes de A. Le sous-corps maximal réel $\mathbf{Q}[\zeta + \zeta^{-1}]$ de F a pour nombre de classes h^+. On sait que $h^+ \mid h$ et que h^+ est le nombre de classes de A invariantes par conjugaison complexe. La p-torsion du groupe des classes $Cl(A)$ se décompose en $Cl(A)_{(p)} = Cl(A)^-_{(p)} \oplus Cl(A)^+_{(p)}$ avec $Cl(A)^{\pm}_{(p)} = \ker(\sigma \mp \mathrm{id})$. On sait que si p^a désigne le nombre d'éléments de $Cl(A)^-_{(p)}$, alors p^a divise $h^- = h/h^+$.

La conjugaison complexe sur A définit une involution toujours notée σ sur $K_1(A;\mathbf{Z}/p)$ qui s'écrit

$$K_1(A;\mathbf{Z}/p) = K_1^-(A;\mathbf{Z}/p) \oplus K_1^+(A;\mathbf{Z}/p)$$

avec $K_1^{\pm}(A;\mathbf{Z}/p) = \ker(\sigma \mp \mathrm{id})$. Par ailleurs,

$$A^\times/(p) \cong \mu_p \times \{\pm 1\} \times (\mathbf{Z}/p)^{(p-3)/2}$$

où $\mu_p = \{\exp(2ik\pi/p),\ 0 \leq k \leq p-1\}$. En particulier, $(A^\times/(p))^- \cong \mu_p$. L'extension (†) p. 20 se scinde donc en deux parties dont la partie antisymétrique s'écrit

$$(\dagger^-) \qquad 1 \longrightarrow \mu_p \longrightarrow K_1^-(A;\mathbf{Z}/p) \xrightarrow{\partial} Cl(A)^-_{(p)} \longrightarrow 1.$$

Dans toute la suite de ce texte , on pose

$$d_p^- := \dim_{\mathbf{Z}/p} Cl(A)^-_{(p)} = \dim_{\mathbf{Z}/p} K_1^-(A;\mathbf{Z}/p) - 1.$$

Rappelons qu'un nombre premier est régulier s'il ne divise pas le nombre de classes h_p : pour un nombre premier régulier, $Cl(A)_{(p)} = Cl(A)^-_{(p)} = 0$.

Proposition 45 *On a $d_p^- = 0$ si et seulement si p est un nombrer premier régulier.*

Preuve : Si p est régulier, l'extension $(\dagger^-)$ se réduit à $K_1^-(A;\mathbf{Z}/p) = \mu_p$. Réciproquement, si $K_1^-(A;\mathbf{Z}/p) = \mu_p$, alors $h^- = 0$ et p ne divise pas h^-. D'après un théorème de Kummer ([24], 5.6), ceci entraîne que p ne divise pas h^+ donc $Cl(A)_{(p)} = 0$, c'est-à-dire p régulier. $\square$

Rappelons 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).

La démarche développée dans les paragraphes qui suivent est celle-ci. L'équation $a^p = b^p + c^p$ permet de construire un élément z de $K_1^-(A; \mathbf{Z}/p)$. La trace de Dennis à coefficients nous permet de montrer que cet élément z n'est pas trivial. L'action du groupe de Galois fournit$(p-1)/2$ éléments de $K_1^-(A; \mathbf{Z}/p)$ construits à partir de z. Grâce à la trace de Dennis, nous minorons la dimension du sous-espace vectoriel de $K_1^-(A; \mathbf{Z}/p)$ engendré par ces $(p-1)/2$ éléments en termes des polynômes de Mirimanoff. On en déduit une minoration de d_p^-.

Au vocabulaire près, le résultat suivant est bien connu.

Proposition 46 *Soient p un nombre premier, A l'anneau $\mathbf{Z}[\zeta_p]$, F le corps $\mathbf{Q}[\zeta_p]$. On suppose que (p, a, b, c) satisfont les hypothèses du premier cas du dernier théorème de Fermat. Pour $1 \leq \ell \leq (p-1)/2$, les éléments*

$$z_\ell = \frac{a - b\zeta^{s^\ell}}{a - b\zeta^{-s^\ell}} \bmod F^{\times(p)}$$

appartiennent alors à $K_1^-(A; \mathbf{Z}/p)$.

Preuve : Sous les hypothèses DTF1, les idéaux fractionnaires principaux $(a - b\zeta^\ell)$, $1 \leq \ell \leq p-1$ 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 $1 \leq \ell \leq p-1$, les éléments $a - b\zeta^\ell \bmod F^{\times(p)}$ appartiennent à $\mathcal{U}(A; \mathbf{Z}/p)$. □

4.2 Emploi du groupe $K_1(A/p; \mathbf{Z}/p)$.

Soit $\varphi : A \to A/p$ la projection canonique. Posons $\lambda = 1 - \varphi(\zeta)$. Alors $A/(p) = \mathbf{Z}/p[\lambda]$ avec $\lambda^{p-1} = 0$. L'anneau A/p est local et $(A/p)^\times = \mathbf{Z}/p^\times + \lambda\mathbf{Z}/p[\lambda]$. On en déduit

$$K_1(A/p; \mathbf{Z}/p) = (A/p)^\times/(p) = (1 + \lambda\mathbf{Z}/p[\lambda], \times).$$

Les modules de différentielles $\Omega^1_{dR}(A)/(p)$, $\Omega^1_{dR}(A/p)$ et $\Omega^1_{dR}(A/p)/(p)$ sont tous trois isomorphes à

$$\mathbf{Z}/p[X]dX/(X-1)^{p-2}dX,$$

donc $\Omega^1_{dR}(A/p) = \mathbf{Z}/p[\lambda]d\lambda$ avec $\lambda^{p-1} = 0$ et $\lambda^{p-2}d\lambda = 0$.

Par commodité, $o(\lambda^j)$ désigne un élément indéterminé de $\lambda^{j+1}\mathbf{Z}/p[\lambda]$. Soit p un nombre premier impair et soient x et y deux éléments de $(\mathbf{Z}/p)^\times$ tels que $x - y = 1$. Soint les éléments $w = x - y(1-\lambda)$ et $\sigma(w) = x - y(1-\lambda)^{-1}$ de $(A/p)^\times$ et soit $z' = z'(x)$ l'élément de $K_1^-(A/p;\mathbf{Z}/p)$ défini par $z' = w/\sigma(w) \bmod (A/p)^{\times(p)}$.

Proposition 47 *Si p est un nombre premier impair et si $x \in \mathbf{Z}/p \setminus \{0, 1, 1/2\}$, alors l'élément $z'(x)$ ci-dessus de $K_1^-(A/p;\mathbf{Z}/p)$ n'est pas colinéaire à l'élément $1-\lambda$.*

Preuve : Calculons les traces $D_1^{(p)}(z'(x))$ et $D_1^{(p)}(1-\lambda)$. On a

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

Puisque $w = 1 + y\lambda$, $w^{-1} = \sum_{k\geq 0}(-1)^k y^k \lambda^k$, $dw = yd\lambda$ et

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

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

$$d\sigma(w) = -y\sum_{k\geq 1} k\lambda^{k-1}d\lambda$$

et par suite

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

Ces expressions de $w^{-1}dw$ et $\sigma(w)^{-1}d\sigma(w)$ conduisent à

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

Par ailleurs $D_1^{(p)}(1-\lambda) = -(1-\lambda)^{-1}d\lambda = -\sum_{k\geq 0}\lambda^k d\lambda$. 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 $y \in (\mathbf{Z}/p)^\times$ est solution de l'équation $2X^2 + 3X + 1 = 0$ dans $\mathbf{Z}/p[X]$. 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. $\square$

Proposition 48 *On suppose que (p, a, b, c) satisfait DTF1 avec $p > 3$. Alors, $d_p^- \geq 1$.*

Preuve : Désignons par $\varphi_1 : K_1(A; \mathbf{Z}/p) \to K_1(A/p; \mathbf{Z}/p)$ l'application induite par φ en K-théorie à coefficients. L'élément

$$z = \frac{a - b\zeta}{a - b\zeta^{-1}} \text{ mod } F^{\times(n)}$$

de $K_1^-(A; \mathbf{Z}/p)$ est tel que

$$\varphi_1(z) = \frac{x - y(1-\lambda)}{x - y(1-\lambda)^{-1}} \text{ mod } (A/p)^{\times(p)}$$

avec $x = \overline{a}/\overline{c}$ et $y = x - 1$. On a nécessairement $x \neq 0$. Si $x = 1/2$, l'élément

$$z_1 = \frac{a - c\zeta}{a - c\zeta^{-1}} \text{ mod } F^{\times(n)}$$

est tel que $\varphi_1(z_1) = z'(x_1)$ avec $x_1 = \overline{c}/\overline{b}$. 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. $\square$

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

Corollaire 49 *(Kummer, 1847)*
Soit p un nombre premier régulier. Alors le premier cas du dernier théorème de Fermat est satisfait pour p.

4.3 Emploi du groupe $K_1(R; \mathbf{Z}/p)$.

Dans tout ce paragraphe, x et y désignent deux éléments de $(\mathbf{Z}/p)^\times$ tels que $x - y = 1$.

L'action du groupe de Galois $G = Gal(F/\mathbf{Q})$ sur $\Omega^1_{dR}(A)/(p) = \mathbf{Z}/p[\lambda]d\lambda$ est peu lisible car $g\lambda = 1 - (1-\lambda)^s$. C'est pourquoi nous introduisons les anneaux $R' = \mathbf{Z}[X]/(X^p - 1) = \mathbf{Z}[t]$ et $R = R'/p$ avec $t = X \text{ mod } (X^p - 1)$. Le groupe G opère sur R' par $gt = t^s$ (où g est un générateur de G et $(s, p) = 1$). Remarquons que l'involution $\sigma = g^{(p-1)/2}$ est telle que $\sigma(t) = t^{-1}$.

On a $R = \mathbf{Z}/p[1-t]$ avec $(1-t)^p = 0$. L'anneau R est local, $R^\times = (\mathbf{Z}/p)^\times \oplus (1-t)\mathbf{Z}/p[1-t]$ et

$$K_1(R; \mathbf{Z}/p) = (1 + (1-t)\mathbf{Z}/p[1-t], \times).$$

Les modules de différentielles de Kähler $\Omega^1_{dR}(R')$, $\Omega^1_{dR}(R')/(p)$, $\Omega^1_{dR}(R)$ et $\Omega^1_{dR}(R)/(p)$ sont tous quatre isomorphes à

$$\mathbf{Z}/p[X]dX/(X-1)^p dX.$$

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

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

et

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

conduisent à la décomposition commode suivante.

Proposition 50 *Posons* $f_0^- = t^{-1}dt$, *et pour* $1 \leq \ell \leq (p-1)/2$, $f_\ell^\pm = \left(t^{s^\ell} \mp t^{-s^\ell}\right) t^{-1}dt$.

On a alors

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

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

De plus, en désignant par g *un générateur du groupe de Galois* $G = Gal(F/\mathbf{Q})$ *et en notant* σ *l'involution* $g^{(p-1)/2}$, *on a les relations* $g(f_0^-) = sf_0^-$, $g(f_\ell^\pm) = sf^\pm_{\ell+1}$, $1 \leq \ell < (p-1)/2$, $g(f^\pm_{(p-1)/2}) = f_1^\pm$
et $\sigma(f_0^-) = -f_0^-$, $\sigma(f_\ell^\pm) = \pm f_\ell^\pm$ $(1 \leq \ell \leq (p-1)/2$.

Définition 51 *Pour* $x \in \mathbf{Z}/p \setminus \{0, 1\}$, *on pose* $y = x - 1$ *et pour* $1 \leq k \leq (p-1)/2$, *on introduit les éléments*

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

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

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

Proposition 52 *Dans la base* $(f_0^-, \cdots, f_{(p-1)/2}^-)$ *de* $\Omega_{dR}^-(R)$*, la trace de Dennis de* $z_1(x)$ *s'écrit*

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

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

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

conduit à

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

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

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

On transforme cette quantité en écrivant

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

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 $\Omega_{dR}^-(R)$, 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 $\sigma(v_1(x))^{-1}d\sigma(v_1(x))$ 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 ainsi

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

d'où finalement

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

$\square$

Définition 53 *On note $V(x)$ le sous-espace vectoriel de $K_1^-(R;\mathbf{Z})$ engendré par l'orbite de $z_1(x)$ sous l'action du groupe de Galois G, c'est-à-dire*

$$V(x) = Vect_{\mathbf{Z}/p}(z_k(x),\ 1 \leq k \leq (p-1)/2).$$

Proposition 54 *Soit $C = C(x)$ la matrice circulante d'ordre $(p-1)/2$ à coefficients dans $\mathbf{Z}/p$*

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

Alors

$$\dim_{\mathbf{Z}/p} V(x) \geq rg(C(x)).$$

Preuve : à une constante près, les composantes de $D_1^{(p)}(z_1(x))$ dans la base $(f_0^-, f_1^-, \cdots, f_{(p-1)/2}^-)$ de $\Omega_{dR}^-(R)$ sont $(2, \alpha_1, \cdots, \alpha_{(p-1)/2})$. Puisque $z_k(x) = g^k(z_1(x))$, compte tenu de l'action de g sur les vecteurs de base $(f_0^-, f_1^-, \cdots, f_{(p-1)/2}^-)$, on en déduit que la matrice des composantes respectives de $D_1^{(p)}(z_1(x))$, $D_1^{(p)}(z_2(x))$, $\cdots$, $D_1^{(p)}(z_{(p-1)/2}(x))$ a le même rang que la matrice

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

Puisque $\sum_{k=1}^{(p-1)/2} \alpha_k = -1$, le rang de cette matrice est celui de 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 55 *Les polynômes de Mirimanoff $M_k(X) \in \mathbf{Z}/p[X]$ sont définis pour $1 \leq k \leq p-1$ par*

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

Pour $t \in \mathbf{Z}/p$, on pose

$$r_p(t) = \#\{k \mid 1 \leq k \leq (p-1)/2,\ M_{2k+1}(t) \neq 0\}\cdot$$

C'est le nombre de polynômes de Mirimanoff $M_j(X)$ non nuls en la valeur t et d'indice j impair.

Proposition 56 *Soient x et y deux éléments de $(\mathbf{Z}/p)^\times$ tels que $x - y = 1$. Les valeurs propres de la matrice $C(x)$ sont $M_{2k+1}(x/y)$, $1 \leq k \leq (p-1)/2$. Le rang de la matrice $C(x)$ est $r_p(x/y)$.*

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

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

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 $r_p(x/y)$. $\square$

En résumé, nous avons montré :

Théorème 57 *Soient x et y deux éléments de $(\mathbf{Z}/p)^\times$ tels que $x-y=1$. Alors*

$$\dim_{\mathbf{Z}/p} V(x) \geq r_p(x/y).$$

Remarque 58. Posons

$$r_p = min\{r_p(t),\ t \in \mathbf{Z}/p \setminus \{0,1,1/2\}\}.$$

Alors, pour tout $x \in \mathbf{Z}/p \setminus \{0,1,1/2\}$, on a

$$(p-1)/2 \geq \dim_{\mathbf{Z}/p} V(x) \geq r_p.$$

4.4 Lien avec les dérivées logarithmiques de Kummer.

Soit toujours A l'anneau des entiers du corps cyclotomique $F = \mathbf{Q}[\zeta_p]$ avec p premier impair. On pose $\lambda = 1-\zeta$. Identifions $K_1(A/p;\mathbf{Z}/p)$ au groupe multiplicatif $(1+\lambda\mathbf{Z}/p[\lambda],\times)$. 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 $K_1(A/p;\mathbf{Z}/p)$ encore noté z. Pour $1 \leq k \leq p-2$, 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

$$\ell_k : (K_1(A/p;\mathbf{Z}/p),\times) \to (\mathbf{Z}/p,+)$$

est un morphisme de groupes.

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

Mirimanoff a montré (*cf.* [20], VII ou [9]) que pour $1 \leq k \leq (p-3)/2$, 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 à coefficients et les dérivées logarithmiques de Kummer. Soient

$$z_k(x) = \frac{x-yt^{s^k}}{x-yt^{s^{-k}}} \bmod (R)^{\times(p)}$$

les éléments de $K_1(R;\mathbf{Z}/p)$ introduits à la définition 51. Soit $C(x) \in \mathrm{Mat}_{(p-1)/2}(\mathbf{Z}/p)$ la matrice des coordonnées de $D_1^{(p)}(z_1(x))$, $D_1^{(p)}(z_2(x))$, ..., $D_1^{(p)}(z_{(p-1)/2}(x))$ dans la base de $\Omega^-_{dR}(R)$ décrite dans la proposition 50. Alors, à une constante près, la matrice $C(x)$ a pour valeurs propres les dérivées logarithmiques de Kummer $\ell_{2k+1}(x-y\zeta)$.

Signalons un autre lien entre les $\ell_{2k+1}(x-y\zeta)$ et la trace de Dennis. Le développement limité à l'ordre 2 de $D_1^{(p)}(z'(x))$ effectué à la proposition 47 peut être précisé. On obtient

$$D_1^{(p)}(z'(x)) = \sum_{k=0}^{p-3} \gamma_k(x)\lambda^k d\lambda$$

avec $\gamma_0(x) = 2y$ et

$$\gamma_k(x) = (-1)^k y^{k+1} + (k+1)y + \sum_{j=1}^{k} j y^2 (1+y)^{k-j}.$$

Introduisons les vecteurs colonnes $\ell(x)$ et $D(x)$ de $(\mathbf{Z}/p)^{(p-1)/2}$ définis par $\ell(x) = (\ell_{2k+1}(z'(x)))_{1\leq k\leq (p-1)/2}$ et $D(x) = (\gamma_{2k}(x))_{0\leq k\leq (p-3)/2}$. Pour $p \leq 13$, on *constate* qu'il existe une matrice triangulaire $A \in \mathbf{GL}_{(p-1)/2}(\mathbf{Z}/p)$ telle que $\ell(x) = AD(x)$ pour tout $x \in (\mathbf{Z}/p)^\times$, ce qui montre qu'il est équivalent de connaître la trace de Dennis à coefficients ou les dérivées logarithmiques de Kummer. Il serait intéressant de savoir si cette observation se généralise à tout nombre premier.

4.5 Application au premier cas du dernier théorème de Fermat.

Supposons que (p,a,b,c) satisfont aux hypothèses DTF1. Notons $\overline{a}$, $\overline{b}$ et $\overline{c}$ les classes respectives de a, b et c dans $\mathbf{Z}/p$. Introduisons le sous-espace vectoriel $V(p,a,b,c)$ de $K_1^-(A;\mathbf{Z}/p)$ 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

$$V(p,a,b,c) = \mathrm{Vect}_{\mathbf{Z}/p}(z_k,\ 1\leq k\leq (p-1)/2).$$

Proposition 59 *On pose $x = \overline{a}/\overline{c}$ et $y = 1 - x = \overline{b}/\overline{c}$. Avec les notations de la section précédente, on a*

$$1 \geq \dim_{\mathbf{Z}/p} V(x) - \dim_{\mathbf{Z}/p} V(p,a,b,c) \geq 0.$$

Preuve : soient $\varphi : A \to A/p$ la surjection canonique et $\psi : R \to A/p$ le morphisme d'anneaux défini par $\psi(t) = 1-\lambda$. On désigne par $\varphi_1 : K_1(A;\mathbf{Z}/p)$ et $\psi_1 : K_1(R;\mathbf{Z}/p) \to K_1(A/p;\mathbf{Z}/p)$ les applications induites en K-théorie à coefficients. Dans $K_1(A;\mathbf{Z}/p)$, 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 $\psi_1(V(x))$. On vérifie aisément que ψ_1 est surjective de noyau de dimension 1. On en déduit l'inégalité proposée. $\square$

Théorème 60 *Soient (p,a,b,c) des entiers satisfaisant aux hypothèses DTF1. Alors, on a les inégalités*

$$d_p^- \geq r_p(\overline{a}/\overline{c}) - 2 \geq r_p - 2.$$

Preuve : D'après le théorème 50 et la proposition ci-dessus, on a les inégalités

$$d_p^- \geq \dim_{\mathbf{Z}/p} K_1^-(A;\mathbf{Z}/p) - 1 \geq \dim_{\mathbf{Z}/p} V(p,a,b,c) - 1 \geq \\ \dim_{\mathbf{Z}/p} V(\overline{a}/\overline{c}) - 2 \geq r_p(\overline{a}/\overline{c}) - 2 \geq r_p - 2.$$

Remarque 61. A 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 $V(\overline{a}/\overline{c})$. 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 $f_i(\eta) \cong (-1)^{i-1} y M_{i-1}(\overline{a}/\overline{c}) \bmod p$ et la minoration $d_p \geq r_p - 2$ 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 $p \geq 2^{d_p+3} - 2d_p - 3$, où $d_p = \dim_{\mathbf{Z}/p} Cl(A)_{(p)}$. On peut aussi exploiter l'inégalité $d_p^- \geq r_p - 2$ en procédant comme suit.

Proposition 62 *Soit p un nombre premier. On a*

$$d_p^- < \frac{p+3}{4}$$

PREUVE : LA quantité $p^{d_p^-}$ divise h^-. D'après [16] et [18], on a

$$h^- \le 2p\left(\frac{p}{24}\right)^{\frac{p-1}{4}}.$$

On en déduit

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

Le second membre de cette inégalité est négatif pour $p \ge 2$.

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

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

Soulignons que le calcul numérique de r_p est assez rapide, ce qui ne semble pas être le cas pour d_p ou d_p^-. Pour $p < 1000$, un calcul sur ordinateur montre qu'on a toujours l'inégalité $r_p > (p+11)/4$ (le nombre maximal de valeurs nulles pour $M_{2k+1}(t)$ est 7).

4.6 Lien avec les nombres de Bernoulli.

L'inégalité $d_p^- \ge r_p - 2$ proposée au théorème 60 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 $B_k \in \mathbf{Q}$ sont définis par

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

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

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

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

$$(\mathcal{K}) \qquad B_{p-(2k+1)} M_{2k+1}(x) \cong 0 \mod p \quad (1 \le k \le (p-3)/2).$$

Il est clair que si x est solution des congruences de Kummer, on a l'inégalité

$$r_p(x) \leq i(p).$$

Par ailleurs, Kummer a montré que si (p, a, b, c) satisfont aux hypothèses DTF1, alors $x = \overline{a}/\overline{c}$ satisfait les congruences $(\mathcal{K})$ (*cf.* [20], VII ou [9]). On en déduit $r_p \leq i(p)$. Cette inégalité est conditionnelle à l'existence d'une solution à DTF1. L'inégalité $i(p) \leq d_p^-$, indépendante d'une éventuelle solution à DTF1, résulte d'un théorème de Ribet [21].

Bibliographie

[1], Artin E. & Tate J., *Class field theory*, Benjamin, New-York, 1967.

[2] Bass H., *Algebraic K-theory*, Benjamin, New-York, 1968.

[3] Bass H., Milnor J. & Serre J.-P., Solution of the congruence subgroup problem for SL_n $(n \geq 3)$ and Sp_{2n} $(n \geq 2)$, *Publ. Math. Inst. Hautes Études Sci.*, **33**, 1967, pp. 59-37.

[4] Berrick J., Interwiners 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 ang. Math.*, **274-276**, 1975, pp. 21-26.

[7] Connes A., Non-commutative differential geometry, *Publ. Math. Inst. Hautes Études Sci.*, **62**, 1985, pp. 257-360.

[8] Goodwillie T.-G., Relative algebraic K-theory and cyclic homology, *Ann. of Math.*, **124**, 1986, pp. 347-402.

[9] Granville A., The Kummer-Wieferich-Skula approach to the first case of Fermat's last theorem, Proceedings of the 3^{rd} conference of the Canadian Number theory Association, August 18-25 1991, *Advances in Number theory*, ed. F.-Q. Gouveâ & N. Yui, Clarendon Press, Oxford, 1993.

[10] Igusa K., What happens to Hatcher and Wagoner's formula for $\pi_0 C/M$ when the first Postnikov invariant of M is trivial ?, *Lectures Notes in Math.*, **1046**, New-York, Springer Verlag, 1984, pp. 104-72.

[11] Karoubi M., Homologie cyclique et K-théorie, *Astérisque*, **149**, Soc. Math. France, 1987.

[12], Karoubi M. & Lambre T., Quelques classes caractéristiques en théorie des nombres, *C. R. Acad. Sci. Paris*, t. 330, Série I, 2000.

[13] Karoubi M. & Villamayor O., K-théorie algébrique et K-théorie topologique I, *Math. Scand.*, **28**, 1971, pp. 265-307.

[14] Lambre T., Quelques exemples de lemme de première perturbation en homologie cyclique, *Comm. Algebra*, **23**, 1995, pp. 525-541.

[15] Larsen M., Lindenstrauss A., Cyclic homology of Dedekind domains, *K-theory*, **6**, 1992, pp. 301-334.

[16] Lepistö T., On the growth of the first factor of the class number of the prime cyclotomic field, *Ann. Acad. Sci. Fennicae*, Série A, I, **577**, 1974, Helsinski (21 pages).

[17] Loday J.-L., *Cyclic Homology*, Springer Verlag, Berlin, 1992.

[18] Metsänkylä T., Class numbers and μ-invariants of cyclotomic fields, *Proc. Amer. Math. Soc.*, **43**, 2, 1974, pp. 299-300.

[19] Neisendorfer J., Primary homotopy theory, *Memoirs Am. Math. Soc.*, **232**, 1980.

[20] Ribenboim P., *13 lectures on Fermat's Last Theorem*, Springer, Berlin, 1974.

[21], Ribet K., A modular construction of unamified p-extensions of $\mathbf{Q}(\mu_p)$, *Invent. Math.*, **34**, 1976, pp. 151-162.

[22] Serre J.-P., *Corps locaux*, Hermann, 1968.

[23] Wagoner J.-B., Delooping classifying spaces in algebraic K-theory, *Topology*, **1972**, 11, pp. 349-370.

[24] Washington L., *Introduction to cyclotomic Fields*, GTM 83, Springer, Berlin, 1982 .

[25] Weibel Ch., Nil K-theory maps to cyclic homology,*Trans. Am. Math. Soc.*, **303**, 1987, pp. 541-558.

[26] Weibel Ch., *An introduction to homological algebra*, Cambridge Studies in advanced mathematics, **38**, Cambrigde, 1994.

[27] Wodzicki M., Excision in cyclic homology and in rational algebraic K-theory, *Ann. Math.*, **129**, 1989, pp. 591-639.

[28] Yamamoto Y., On unramified Galois extensions of quadratic number fields, *Osaka J. Math.*, **7**, 1970, pp. 57-76.