

MÉMOIRES DE LA S. M. F.

ARTIBANO MICALI

J.-D. THÉRON

Sur les groupes $A(n)$

Mémoires de la S. M. F., tome 48 (1976), p. 75-87

<http://www.numdam.org/item?id=MSMF_1976__48__75_0>

© Mémoires de la S. M. F., 1976, tous droits réservés.

L'accès aux archives de la revue « Mémoires de la S. M. F. » (<http://smf.emath.fr/Publications/Memoires/Presentation.html>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

SUR LES GROUPEs A(n)

par

A. MICALI et J.-D. THEROND

Les groupes $A(n)$ sont directement issus de la théorie des formes quadratiques et de celle des algèbres de Clifford. En effet, le groupe $G(A)$, qui est lié aux groupes $A(2)$ et $A(4)$ intervient (cf. [6]) dans la classification des algèbres de Clifford.

Nous nous intéressons à des propriétés concernant essentiellement les groupes $A(n)$ et à des phénomènes de nature cohomologique qui s'y rattachent. Nous déterminons, en dernière partie, des groupes $A(n)$ pour certains anneaux d'entiers de corps de nombres.

Tout anneau est commutatif à élément unité et $U(A)$ désigne le groupe multiplicatif des éléments inversibles de l'anneau A . De plus, Ann désigne la catégorie des anneaux et Ab celle des groupes abéliens.

1. Préliminaires. Le groupe $G(A)$

Soient A un anneau, $n \geq 0$ un entier et $A(n) = \{a \mid a \in A, 1-n a \in U(A)\}$. La loi de composition $a \tilde{+} b = a + b - n a b$ pour a et b parcourant A , munit $A(n)$ d'une structure de groupe abélien et on définit ainsi un foncteur covariant $.(n) : \text{Ann} \rightarrow \text{Ab}$.

Pour tout anneau A , on notera $\text{Ip}(A)$ le groupe des idempotents de A muni de la loi de groupe abélien donnée par $e \tilde{+} e' = e + e' - 2 e e'$, e et e' parcourant $\text{Ip}(A)$. On définit aussi, de la sorte, un foncteur noté Ip défini dans Ann à valeurs dans Ab. Voyons comment le groupe des idempotents de l'anneau A est lié aux groupes $A(n)$. Pour cela, on remarque que l'application $\phi : A(2) \rightarrow A(4)$ définie par $x \mapsto x - x^2$ est un morphisme de groupes abéliens dont le noyau est $\text{Ip}(A)$. Si l'on désigne par $\mathcal{G}(A)$ son conoyau, on a la suite exacte de groupes abéliens $0 \rightarrow \text{Ip}(A) \rightarrow A(2) \xrightarrow{\phi} A(4) \rightarrow \mathcal{G}(A) \rightarrow 0$.

Exemples 1.1. Pour tout anneau A , $A(0) = A^+$, le groupe abélien additif sous-jacent à l'anneau A .

1.2. Si A est un anneau de Boole, $\text{Ip}(A) = A(2)$, donc $A(4) \xrightarrow{\sim} \mathcal{G}(A)$ est un isomorphisme de groupes abéliens.

1.3. Pour tout anneau A , l'application $A(n) \rightarrow U(A)$ définie par $a \mapsto 1 - n a$ est

un morphisme de groupes abéliens, car quels que soient a et b dans $A(n)$, $1 - n(a \tilde{+} b) = (1 - na)(1 - nb)$. Si n n'est pas diviseur de zéro dans A , ce morphisme est injectif. De plus, si n est inversible dans A , c'est un isomorphisme, l'isomorphisme réciproque $A(n) \leftarrow U(A)$ étant défini par $\frac{1}{n}(1 - a) \leftarrow a$.

1.4. Considérons le sous-groupe $U^2(A) = \{a^2 \mid a \in U(A)\}$ de $U(A)$, pour un anneau A donné, et soit $\phi : A(4) \rightarrow U(A)$ le morphisme défini par $a \mapsto 1 - 4a$. Si $x \in \text{Im}(A(2) \rightarrow A(4))$, il existe un élément $a \in A(2)$ tel que $x = a - a^2$, donc $\phi(x) = 1 - 4x = (1 - 2a)^2 \in U^2(A)$. Par passage aux quotients, il existe un unique morphisme de groupes abéliens $\bar{\phi} : G(A) \dashrightarrow U(A)/U^2(A)$ rendant commutatif le diagramme

$$\begin{array}{ccc} A(4) & \xrightarrow{\phi} & U(A) \\ \downarrow & & \downarrow \\ G(A) & \dashrightarrow \bar{\phi} & U(A)/U^2(A) \end{array},$$

où les flèches verticales sont canoniques. Si 2 est inversible dans A , le morphisme $\bar{\phi} : G(A) \xrightarrow{\sim} U(A)/U^2(A)$ est un isomorphisme de groupes abéliens.

1.5. Soit $\mathcal{Q}(A)$ le groupe des extensions quadratiques de l'anneau A (cf. [2], Ch. IV, § 3). Si A est un anneau local, on sait (cf. [7]) que toute extension quadratique de A s'écrit sous la forme $A[x]$ avec $x^2 - x + a = 0$, où $a \in A$ et $1 - 4a$ est inversible dans A . L'application $\mathcal{Q}(A) \rightarrow G(A)$ définie par $A[x] \mapsto \bar{a}$ est alors un isomorphisme de groupes abéliens.

On remarque, finalement, que G est un foncteur covariant défini dans la catégorie Ann à valeurs dans la catégorie Ab.

2. Les morphismes $\phi : A(m) \rightarrow A(n)$

On se pose ici le problème de savoir si pour un anneau A donné et pour deux entiers $m, n \geq 0$ donnés, il existe toujours un morphisme non trivial de groupes abéliens $\phi : A(m) \rightarrow A(n)$, i. e., tel que $\phi(x + y - mxy) = \phi(x) + \phi(y) - n\phi(x)\phi(y)$ pour x et y parcourant $A(m)$. Dans un premier temps, nous chercherons les solutions continues de cette équation fonctionnelle.

Supposons donc que $\phi : R \rightarrow R$ soit une fonction continue et différentiable vérifiant l'équation fonctionnelle $\phi(x + y - mxy) = \phi(x) + \phi(y) - n\phi(x)\phi(y)$ quels que soient x et y dans R . On voit donc que pour tout $x \in R$ et pour $h > 0$, $\phi(x + (1 - mx)h) - \phi(x) = (1 - n\phi(x))\phi(h)$ et si l'on remplace h par $\frac{1}{1-mx}$, on a $\phi(x + h) - \phi(x) = (1 - n\phi(x))\phi(\frac{h}{1-mx})$. En divisant par h et en passant à la limite pour $h \rightarrow 0$, on a $\phi'(x) = \frac{1-n\phi(x)}{1-mx} \phi'(0)$.

Si $m \neq 0$ et $n \neq 0$, cette équation différentielle nous donne $\phi(x) = \frac{1}{n} (1 - (1-mx)^{\frac{n\phi'(0)}{m}})$; si $m = 0$ et $n \neq 0$, on a $\phi(x) = \frac{1}{n} (1 - e^{-n\phi'(0)x})$; si $m \neq 0$ et $n = 0$, $\phi(x) = -\frac{\phi'(0)}{m} \log(1 - mx)$. Finalement, pour $m = n = 0$, $\phi(x) = \phi'(0)x$.

Supposons que $\phi(x) = \frac{1}{n} (1 - (1 - mx)^{\frac{n\phi'(0)}{m}})$. Le développement de Taylor de $\phi(x)$ au voisinage de l'origine nous donne $\phi(x) = \sum_{k=1}^{\infty} \frac{1}{k!} \phi^{(k)}(0)x^k$, car $\phi(0) = 0$, où $\phi^{(k+1)}(0) = (-1)^k \phi'(0) \prod_{j=1}^k (n\phi'(0) - jm)$, pour tout entier $k \geq 1$.

Supposons qu'il existe un entier k tel que $n\phi'(0) - km = 0$; dans ces conditions, $\phi^{(k+1)}(0) = 0$ et $\phi^{(j)}(0) = 0$ pour tout entier $j \geq k+1$, donc $\phi(x) = \sum_{j=1}^k \frac{1}{j!} \phi^{(j)}(0)x^j$ pour tout x dans R . Mais il n'est pas encore dit que l'application $\phi : A(m) \rightarrow A(n)$ ainsi définie soit un morphisme de groupes abéliens. Pour cela, il suffit que les coefficients $\frac{1}{j!} \phi^{(j)}(0)$ soient des nombres entiers pour $j = 1, \dots, k$.

Nous avons déjà vu que pour tout anneau A , l'application $\phi : A(2) \rightarrow A(4)$ définie par $x \mapsto x - x^2$ est un morphisme de groupes abéliens. D'autre part, nous avons déjà vu que, en général, le morphisme $\phi : A(m) \rightarrow A(n)$ fourni par la formule $\phi(x) = \frac{1}{n} (1 - (1 - mx)^{\frac{n\phi'(0)}{m}})$ pour tout x dans $A(m)$, peut ne pas exister, m et n entiers > 0 quelconques.

Pour tout entier $m > 0$, considérons donc l'application $\phi : A(m) \rightarrow A(m^2)$ définie par $x \mapsto x - \sum_{k=2}^m (-1)^k \binom{m}{k} m^{k-2} x^k$. Il est clair qu'il s'agit d'un morphisme pour les structures de groupes abéliens de $A(m)$ et $A(m^2)$ respectivement (ceci correspond au cas continu dans lequel $n = m^2$ et $\phi'(0) = 1$). Désignons par $Ip_m(A)$ et $G_m(A)$ respectivement le noyau et le conoyau de ϕ . Si $\mu_m(A) = \{a \mid a \in U(A), a^m = 1\}$ désigne le groupe multiplicatif des racines $m^{\text{ièmes}}$ de l'unité, la formule $(1 - mx)^m = 1 - m^2 \phi(x)$ pour tout $x \in A(m)$ nous montre que l'application $Ip_m(A) \rightarrow \mu_m(A)$ définie par $x \mapsto 1 - mx$ est un morphisme de groupes abéliens. On définit de la sorte un morphisme de foncteurs $Ip_m \rightarrow \mu_m$. De plus, le morphisme $Ip_m(A) \rightarrow \mu_m(A)$ est injectif si m n'est pas diviseur de zéro dans A ; c'est un isomorphisme, si m est inversible dans A . Dans ce cas, l'isomorphisme réciproque que $Ip_m(A) \leftarrow \mu_m(A)$ est donné par $\frac{1}{m} (1 - x) \leftarrow x$.

Soient m et n deux entiers ≥ 1 . Pour tout x dans le groupe $A(m)$, on posera $n.x = x \tilde{+} \dots \tilde{+} x$ (n fois).

Lemme 2.1. Soient m et n deux entiers ≥ 1 . Pour tout x dans $A(m)$, on a

$$n.x = \sum_{k=1}^n (-1)^{k+1} \binom{n}{k} m^{k-1} x^k \quad \text{et} \quad 1 - m(n.x) = (1 - mx)^n.$$

La démonstration se fait par récurrence sur n , le cas $n = 1$ étant trivial. D'après l'hypothèse de récurrence on a $n \cdot x = (n-1) \cdot x \tilde{+} x =$

$$= \sum_{k=1}^{n-1} (-1)^{k+1} \binom{n-1}{k} m^{k-1} x^k + x - m x \sum_{k=1}^{n-1} (-1)^{k+1} \binom{n-1}{k} m^{k-1} x^k =$$

$$= \sum_{k=1}^{n-1} (-1)^{k+1} \binom{n-1}{k} m^{k-1} x^k + x - \sum_{k=2}^n (-1)^k \binom{n-1}{k-1} m^{k-1} x^k = \sum_{k=1}^n (-1)^{k+1} \binom{n}{k} m^{k-1} x^k,$$

 pour tout x dans $A(m)$. L'autre formule se démontre aussi par récurrence.

Proposition 2.2. Si $\phi : A(m) \rightarrow A(m^2)$ est le morphisme défini par $x \mapsto x -$

$$- \sum_{k=2}^m (-1)^k \binom{m}{k} m^{k-2} x^k$$
, alors $m \cdot x = m \phi(x)$ pour tout $x \in A(m)$.

Ceci résulte immédiatement du lemme précédant, compte tenu de la définition de ϕ . Il s'ensuit que $(\mathbb{Z}/(m)) \otimes_{\mathbb{Z}} \text{Ip}_m(A) \sim \text{Ip}_m(A)$, donc $\text{Ip}_m(A)$ est muni d'une structure naturelle de $\mathbb{Z}/(m)$ -module. En particulier, le groupe des idempotents de l'anneau A est muni d'une structure naturelle d'espace vectoriel sur le corps $\mathbb{Z}/(2)$.

3. Le groupe $\mathcal{P}_n(A)$

Soient A un anneau, $n \geq 1$ un nombre entier et $\mathcal{P}_n(A)$ l'ensemble des couples (P, α) , où P est un A -module projectif de type fini et de rang 1 et $\alpha : P^{\otimes n} \xrightarrow{\sim} A$ est un isomorphisme de A -module. De plus, on dira que deux éléments (P, α) et (P', α') de $\mathcal{P}_n(A)$ sont égaux, et on écrit $(P, \alpha) = (P', \alpha')$, si, et seulement si, il existe un isomorphisme de A -modules $f : P \xrightarrow{\sim} P'$ rendant commutatif le diagramme :

$$\begin{array}{ccc} P^{\otimes n} & \xrightarrow{f^{\otimes n}} & P'^{\otimes n} \\ \alpha \searrow & & \swarrow \alpha' \\ & A & \end{array}$$

On munit alors $\mathcal{P}_n(A)$ d'une structure de groupe abélien en posant $(P, \alpha) + (P', \alpha') = (P \otimes P', \alpha * \alpha')$, où $\alpha * \alpha' : (P \otimes P')^{\otimes n} \xrightarrow{\sim} P^{\otimes n} \otimes P'^{\otimes n} \xrightarrow{\sim} A \otimes A \xrightarrow{\mu} A$ est l'isomorphisme composé évident, $\mu : A \otimes A \rightarrow A$ étant la multiplication de l'anneau A . L'élément neutre de $\mathcal{P}_n(A)$ est le couple (A, μ) où $\mu : A^{\otimes n} \rightarrow A$ est la multiplication de A et l'opposé de (P, α) est $(P, \alpha) + \dots + (P, \alpha)$ ($n-1$ fois), que l'on notera $(n-1)(P, \alpha)$. En effet, $n(P, \alpha) = (P^{\otimes n}, \alpha^{*n}) = (A, \mu)$. On remarque que $\mathcal{P}_1(A)$ est le groupe trivial et que $\mathcal{P}_n(A)$ dépend fonctoriellement de A , pour tout entier $n \geq 1$. Nous allons donner une interprétation cohomologique pour $\mathcal{P}_n(A)$ analogue à celle donnée dans [7] (cf. § 3.2.) pour $\mathcal{P}_2(A)$. Notre démarche sera néanmoins différente de celle utilisée dans [7] et pour ce faire, établissons tout d'abord le résultat suivant (cf. [5], Proposition 2.4.15, pour le cas $n = 2$).

Proposition 3.1. Pour tout anneau A et tout entier $n \geq 1$, on a la suite exacte de groupes abéliens $0 \rightarrow \mu_n(A) \rightarrow U(A) \xrightarrow{n} U(A) \rightarrow \mathcal{P}_n(A) \rightarrow \text{Pic}(A) \xrightarrow{n} \text{Pic}(A)$, où n désigne l'élévation à la puissance n , $\mathcal{P}_n(A) \rightarrow \text{Pic}(A)$ est le morphisme qui à la classe de (P, α) associe la classe de P dans $\text{Pic}(A)$ et $U(A) \rightarrow \mathcal{P}_n(A)$ est le morphisme défini par $a \mapsto (A, a \mu)$.

Ici $\text{Pic}(A)$ désigne le groupe de Picard de l'anneau A . Il est évident que la flèche composée $U(A) \rightarrow \mathcal{P}_n(A) \rightarrow \text{Pic}(A)$ est nulle. Si $(P, \alpha) \in \mathcal{P}_n(A)$ a une image nulle dans $\text{Pic}(A)$, alors P est un A -module libre de rang 1, disons $P = Ae$, et si l'on pose $a = \alpha(e^{\otimes n})$, alors $a \in U(A)$ et $a \mapsto (P, \alpha)$. Ainsi, la suite ci-dessus est exacte. D'autre part, la flèche composée $\mathcal{P}_n(A) \rightarrow \text{Pic}(A) \xrightarrow{n} \text{Pic}(A)$ est nulle et soit P un A -module projectif de type fini et de rang 1 tel que $P^{\otimes n}$ soit isomorphe à A . Choisissons un isomorphisme particulier $\alpha : P^{\otimes n} \xrightarrow{\sim} A$; alors $(P, \alpha) \in \mathcal{P}_n(A)$ et il s'envoie sur P par le morphisme $\mathcal{P}_n(A) \rightarrow \text{Pic}(A)$. Ceci nous dit que la suite $\mathcal{P}_n(A) \rightarrow \text{Pic}(A) \xrightarrow{n} \text{Pic}(A)$ est exacte. Montrons finalement que la suite $U(A) \xrightarrow{n} U(A) \rightarrow \mathcal{P}_n(A)$ est exacte. En effet, la flèche composée est nulle et si $a \in U(A)$ a une image nulle dans $\mathcal{P}_n(A)$, cela signifie qu'il existe un isomorphisme de A -modules $Ae \rightarrow Ae$, $e \mapsto be$, où $b \in U(A)$, rendant commutatif le diagramme

$$\begin{array}{ccc} A e^{\otimes n} & \xrightarrow{\quad \sim \quad} & A e^{\otimes n} \\ & \searrow a\mu & \swarrow \mu \\ & A & \end{array}$$

soit encore $a = b^n$. Cela achève la démonstration de la proposition.

Corollaire 3.2. Pour tout anneau A et pour tout entier $n \geq 2$ on a la suite exacte de groupes abéliens

$$0 \rightarrow U(A)/U^n(A) \rightarrow \mathcal{P}_n(A) \rightarrow \text{Pic}_n(A) \rightarrow 0,$$

où $\text{Pic}_n(A)$ est le noyau du morphisme $\text{Pic}(A) \xrightarrow{n} \text{Pic}(A)$, élévation à la puissance n . En particulier, si $\text{Pic}_n(A) = 0$, (c'est le cas si $\text{Pic}(A)$ est sans $\mathbb{Z}$ -torsion), il existe un morphisme de groupes abéliens $U(A)/U^n(A) \xrightarrow{\sim} \mathcal{P}_n(A)$.

Considérons sur Ann la topologie f. p. p. f. -fidèlement plate de présentation finie- que nous noterons $\mathcal{X}$ (cf. [1] pour les différentes notions concernant les topologies de Grothendieck). Comme sous ces conditions, les faisceaux engendrés par les préfaisceaux U et U^n coïncident et sont égaux à U , la suite exacte de préfaisceaux $0 \rightarrow \mu_n \rightarrow U \rightarrow U^n \rightarrow 0$ nous donne la suite exacte de faisceaux $0 \rightarrow \mu_n \rightarrow U \xrightarrow{n} U \rightarrow 0$. Si l'on passe en cohomologie, on a la suite exacte longue de groupes abéliens $0 \rightarrow \mu_n(A) \rightarrow U(A) \xrightarrow{n} U(A) \rightarrow H^1(\mathcal{X}, A, \mu_n) \rightarrow H^1(\mathcal{X}, A, U) \xrightarrow{n} H^1(\mathcal{X}, A, U) \rightarrow H^2(\mathcal{X}, A, \mu_n) \rightarrow \dots$; or, on sait (cf. [1]) qu'il existe un isomor-

phisme de groupes abéliens $H^1(\mathcal{X}, A, U) \sim \text{Pic}(A)$, donc d'après la proposition 3.1., on déduit un isomorphisme de groupes abéliens $\mathcal{P}_n(A) \sim H^1(\mathcal{X}, A, \mu_n)$. On a donc démontré le résultat suivant :

Théorème 3.3. Si $\mathcal{X}$ est la topologie f. p. p. f. sur la catégorie $\underline{\text{Ann}}$, pour tout anneau A on a un isomorphisme de groupes abéliens $\mathcal{P}_n(A) \sim H^1(\mathcal{X}, A, \mu_n)$.

Il est clair que pour les anneaux A dans lesquels n est inversible, on a un isomorphisme de groupes abéliens $H^1(\mathcal{X}, A, \text{Ip}_n) \cong H^1(\mathcal{X}, A, \mu_n)$, pour tout entier $i \geq 0$, mais en général, on ne sait pas interpréter les groupes $H^1(\mathcal{X}, A, \text{Ip}_n)$ pour $n \geq 3$. Par contre, si $\mathcal{Q}(A)$ est le groupe des extensions quadratiques de A et si $\mathcal{X}$ est la topologie f. p. p. f. sur $\underline{\text{Ann}}$, il existe un isomorphisme de groupes abéliens $\mathcal{Q}(A) \sim H^1(\mathcal{X}, A, \text{Ip})$ (cf. [7], § 3.1., théorème 1). Ceci nous permet de donner une interprétation cohomologique du groupe $G(A)$ dans le cas d'un anneau local A . Mais, en général, $G(A)$ est un sous-groupe du groupe $\mathcal{Q}(A)$ des extensions quadratiques de A (cf. [9]). En effet, pour tout anneau A , il existe une suite exacte de groupes abéliens $0 \rightarrow \text{Ip}(A) \rightarrow A(2) \rightarrow A(4) \rightarrow G(A) \rightarrow 0$, où $A(2) \rightarrow A(4)$ est le morphisme de groupes abéliens défini par $x \mapsto x - x^2$. Or, quitte à étendre l'anneau A , on peut toujours supposer que l'équation $x - x^2 = a$, où $a \in A$, soit résoluble dans A . Ceci nous dit que, en tant que faisceau, G est trivial, ce qui nous donne la suite exacte de faisceaux $0 \rightarrow \text{Ip} \rightarrow .(2) \rightarrow .(4) \rightarrow 0$. En passant en cohomologie, pour la topologie f. p. p. f., on a pour tout anneau A la suite exacte longue de groupes abéliens $0 \rightarrow \text{Ip}(A) \rightarrow A(2) \rightarrow A(4) \rightarrow H^1(\mathcal{X}, A, \text{Ip}) \rightarrow H^1(\mathcal{X}, A, .(2)) \rightarrow H^1(\mathcal{X}, A, .(4)) \rightarrow H^2(\mathcal{X}, A, \text{Ip}) \rightarrow \dots$, d'où la suite exacte $0 \rightarrow G(A) \rightarrow \mathcal{Q}(A) \rightarrow H^1(\mathcal{X}, A, .(2)) \rightarrow H^1(\mathcal{X}, A, .(4)) \rightarrow H^2(\mathcal{X}, A, \text{Ip}) \rightarrow \dots$. En particulier, si A est un anneau local, ceci nous donne la suite exacte de groupes abéliens $0 \rightarrow H^1(\mathcal{X}, A, .(2)) \rightarrow H^1(\mathcal{X}, A, .(4)) \rightarrow H^2(\mathcal{X}, A, \text{Ip}) \rightarrow \dots$. Si A est un anneau (non nécessairement local) dans lequel $2 = 0$, on a l'isomorphisme de groupes abéliens $G(A) \cong \mathcal{Q}(A)$; mais cet isomorphisme peut être établi directement sans passer par des considérations cohomologiques.

Exemple 3.4. On a vu plus haut que si n est inversible dans un anneau A , pour tout A -algèbre commutative à élément unité $A \rightarrow B$ on a, pour tout $i \geq 0$, $H^i(B/A, \text{Ip}_n) \sim H^i(B/A, \mu_n)$ (cohomologie d'Amitsur). Par contre, on peut avoir un tel isomorphisme sans que n soit inversible dans A . En effet, on remarque que si n est impair, l'unique racine $n^{\text{ième}}$ de l'unité dans $\mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{Z}[i]$ est $1 \otimes 1$; alors que si n est pair il peut y avoir plusieurs racines $n^{\text{ièmes}}$ de l'unité. Par exemple, pour $n = 2$, les racines carrées de l'unité dans $\mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{Z}[i]$ sont $\pm 1 \otimes 1$, $\pm i \otimes i$; si $n = 4$, les racines sont $\pm 1 \otimes 1$, $\pm i \otimes 1$, $\pm 1 \otimes i$, $\pm i \otimes i$. Mais, dans tous les cas, pour n pair, les seules cocycles sont $1 \otimes 1$ et $-i \otimes i$.

et parmi ces deux cocycles, $1 \otimes 1$ est l'unique cobord. Ceci nous montre que $H^1(\mathbb{Z}[i]/\mathbb{Z}, \mu_n) = 0$ si n est impair et $H^1(\mathbb{Z}[i]/\mathbb{Z}, \mu_n) = \mathbb{Z}/(2)$ si n est pair. En ce qui concerne Ip_n , il est facile de voir que l'unique solution de l'équation $x - \sum_{k=2}^n (-1)^k \binom{n}{k} n^{k-2} x^k = 0$ dans l'anneau intègre $\mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{Z}[i]$ est $x = 0$. Il s'ensuit que $H^1(\mathbb{Z}[i]/\mathbb{Z}, Ip_n) = 0$.

4. Quelques déterminations de groupes $A(n)$

On s'intéressera à l'anneau A des entiers d'un corps de nombres algébriques K . Si K possède s plongements réels et $2t$ plongements complexes, sa dimension sur $\mathbb{Q}$ est $m = s + 2t$ et, d'après le théorème de Dirichlet, $U(A)$ est isomorphe à $H \times \mathbb{Z}^r$ où $r = s + t - 1$ et où H est le sous-groupe (cyclique d'ordre pair) des racines de l'unité de K .

Lemme 4.1. Soit $\zeta \neq 1$, une racine de l'unité d'un corps de nombres K dont l'anneau des entiers est A . Si $z \in A$ on a $1 - nz = -1$ si et seulement si $n = 2$ et $z = 1$ et, pour tout $n \geq 2$, si $\zeta \notin R$, alors $1 - nz \neq \zeta$.

Si $1 - nz = -1$, $2 = nz$ d'où, si N désigne la norme pour l'extension K de $\mathbb{Q}$, $2^m = N(2) = N(nz) = n^m N(z)$ où, comme z est entier algébrique, $N(z) \in \mathbb{Z}$. Donc $n = 2$, d'où $z = 1$. La réciproque est évidente.

Soit ζ_h un générateur de H , $\zeta = \zeta_h^a$ et $z = \frac{1 - \zeta}{n} \in \mathbb{Q}(\zeta_h)$ d'où, si N' désigne la norme de l'extension $\mathbb{Q}(\zeta_h)$ de $\mathbb{Q}$ et ϕ l'indicateur d'Euler,

$$N(z) = N'_{(K|\mathbb{Q}(\zeta_h))}(z) = N'(z^{m/\phi(h)}) = (N'(z))^{m/\phi(h)}$$

car $[\mathbb{Q}(\zeta_h) : \mathbb{Q}] = \phi(h)$. Or $z \in A$ (c'est-à-dire z est entier algébrique) donc $N(z) \in \mathbb{Z}$ ce qui est alors le cas si et seulement si $N'(z) \in \mathbb{Z}$. Si $\zeta \notin R$, $|1 - \zeta| < 2$ donc, G désignant le groupe de Galois de $\mathbb{Q}(\zeta_h)$ sur $\mathbb{Q}$:

$$|N'(z)| = \left| \prod_{\sigma \in G} \frac{1 - \sigma(\zeta)}{n} \right| \leq \prod_{\sigma \in G} \frac{|1 - \sigma(\zeta)|}{n} < \left(\frac{2}{n}\right)^{\phi(h)} < 1$$

donc $N'(z) \notin \mathbb{Z}$, contrairement à l'hypothèse $z \in A$.

Proposition 4.2. Soient K un corps de nombres de dimension $m = s + 2t$ sur $\mathbb{Q}$, A l'anneau des entiers de K et $r = s + t - 1$.

Si $n > 2$, $A(n)$ est isomorphe à un sous-groupe de $\mathbb{Z}^r$ et $A(2)$ est isomorphe au produit de $\mathbb{Z}/2\mathbb{Z}$ par un sous-groupe de $\mathbb{Z}^r$.

Soit $(\varepsilon_1, \dots, \varepsilon_r)$ un système d'unités fondamentales de $U(A)$; alors pour tout $u \in U(A)$, $u = \zeta_h^a \varepsilon_r^{k_1} \dots \varepsilon_1^{k_r}$. Comme n est régulier, $A(n) \rightarrow U(A)$ est injective, donc il en est de même de l'application composée

$$\theta : A(n) \rightarrow U(A) \rightarrow H \times Z^r$$

$$z \mapsto 1-nz = \zeta_h^a \varepsilon_1^{k_1} \dots \varepsilon_r^{k_r} \mapsto (\zeta_h^a, k_1, \dots, k_r) ;$$

$A(n)$ est donc isomorphe à un sous-groupe de $H \times Z^r$.

Supposons que $z \in A(n)$ et $z' \in A(n)$ vérifient

$$1-nz = \zeta_h^a \varepsilon_1^{k_1} \dots \varepsilon_r^{k_r} \quad \text{et} \quad 1-nz' = \zeta_h^b \varepsilon_1^{k_1} \dots \varepsilon_r^{k_r}.$$

Si $z^0 \in A(n)$ est l'opposé de z , $1-nz^0 = \zeta_h^{-a} \varepsilon_1^{-k_1} \dots \varepsilon_r^{-k_r}$ et $z = z' \tilde{z} z^0 \in A(n)$

vérifie $1-nz = (1-nz')(1-nz^0) = \zeta_h^{b-a}$. Donc, d'après le lemme, $\zeta_h^{b-a} = \pm 1$ si $n=2$ et $\zeta_h^{b-a} = 1$ si $n > 2$. On peut donc définir une application (projection)

$$\theta' : H \times Z^r \rightarrow Z^r \quad \text{si } n > 2$$

$$\theta' : H \times Z^r \rightarrow Z/\mathbb{Z} \times Z^r \quad \text{si } n = 2$$

telle que $\theta' \circ \theta$ soit injective ; ainsi $A(n)$ est isomorphe à un sous-groupe de Z^r (resp. $Z/\mathbb{Z} \times Z^r$) si $n > 2$ (resp. $n = 2$). Mais comme $1 \in A(2)$, si $z \in A(2)$ $z \tilde{z} 1 \in A(2)$ et $1-2z$ et $1-2(z \tilde{z} 1)$ n'ont pas même projection suivant Z^r . D'où le résultat pour $A(2)$.

Corollaire 4.3. Si K est un corps quadratique imaginaire, $A(2) \simeq Z/\mathbb{Z}$ et $A(n) \simeq \{0\}$ si $n > 2$.

En effet $r = 0$. On supposera maintenant $r > 0$ et on remarque que, dans ce cas, $A(n^\alpha)$ est nul pour tout $\alpha \geq 1$ si et seulement si $A(n)$ l'est. En effet, si $0 \neq z \in A(n^\alpha)$, d'après le lemme 4.1., $1-n^\alpha z \in U(A)$ est d'ordre infini, donc $\frac{1}{n^{\alpha+1}} (1-(1-n^\alpha z)^n)$ qui appartient à $A(n^{\alpha+1})$ n'est pas nul.

Théorème 4.4. Soient A l'anneau des entiers d'un corps de nombres K de dimension $m = s + 2t$ sur $\mathbb{Q}$ où $r = s + t - 1 \neq 0$. Si $p_1^{\alpha_1} \dots p_v^{\alpha_v}$ est la décomposition en produit de facteurs premiers de $n > 2$ et si $A(p_i^{\alpha_i}) \simeq (\mathbb{Z}/\mathbb{Z})^\gamma k_{i1} \mathbb{Z} \times \dots \times k_{ir} \mathbb{Z}$ où $\gamma = 1$ ou 0 suivant que $p_i^{\alpha_i}$ égale 2 ou non, alors $A(n) \simeq k_{11} \mathbb{Z} \times \dots \times k_{r1} \mathbb{Z}$ où k_i est un multiple du p.p.c.m. de $k_{1j}, \dots, k_{vj}$.

En effet, l'application $A(n) \rightarrow A(p_i^{\alpha_i})$ définie par $z \mapsto np_i^{\alpha_i} z$ est injective donc $A(n)$ est un sous-groupe de $A(p_i^{\alpha_i})$; ainsi k_{ij} divise k_j pour tout $i = 1, \dots, v$, d'où le résultat.

Théorème 4.5. Soit A l'anneau des entiers d'un corps de nombres K qui soit, un corps quadratique réel, ou un corps cubique irréel, ou un corps biquadratique qui ne soit pas une extension quadratique de $\mathbb{Q}(\sqrt{d})$, $d \in \{-3, -1, 2, 3, 5\}$. Avec les notations précédentes si $A(p_i^{\alpha_i}) \simeq (\mathbb{Z}/\mathbb{Z})^\gamma k_{i1} \mathbb{Z}$ alors $A(n) \simeq k \mathbb{Z}$ où k est le p.p.c.m. de $k_1, \dots, k_v$ ou son double.

On a respectivement $(s, t) = (2, 0), (1, 1)$ ou $(0, 2)$, donc $r = 1$; et k est, d'après le théorème 4.4., un multiple du p.p.c.m. des k_i . Dans les deux premiers cas, les seules racines de l'unité sont ± 1 (car $s \neq 0$, cf. [3], chap. II, § 3, Ex. 3). Dans le troisième, si $\zeta_h \in A$ comme $\mathbb{Q} \subset \mathbb{Q}(\zeta_h) \subset K$ entraîne que $\phi(h) = [\mathbb{Q}(\zeta_h) : \mathbb{Q}]$ divise $[K : \mathbb{Q}] = 4$, $\phi(h) = 2$ ou 4 . Comme $\phi(h) = 4$ est équivalent à $h = 5, 8, 10$ ou 12 , ce cas est exclu car les corps $\mathbb{Q}(\zeta_5) \simeq \mathbb{Q}(\zeta_{10})$, $\mathbb{Q}(\zeta_8)$ et $\mathbb{Q}(\zeta_{12})$ possèdent un sous-corps quadratique réel $\mathbb{Q}(\zeta_h + \zeta_h^{-1})$ isomorphe respectivement à $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{3})$. Si $\phi(h) = 2$, $h = 3, 4$ ou 6 , donc K est une extension quadratique de $\mathbb{Q}(j) \simeq \mathbb{Q}(\zeta_6) \simeq \mathbb{Q}(\sqrt{-3})$ ou de $\mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$ contrairement à l'hypothèse.

Ainsi, dans les trois cas, $U(A) \simeq \mathbb{Z}/\mathbb{Z} \times \mathbb{Z}$ donc si $z \in A(p_i^{\alpha_i})$, $1 - p_i^{\alpha_i} z = \pm \varepsilon^{k_i}$ où ε est l'unité fondamentale de K , donc $\varepsilon^{k_i} \equiv \pm 1 \pmod{p_i^{\alpha_i}}$ (ce qui signifie, puisque A est un $\mathbb{Z}$ -module libre de base $(1, e_2, \dots, e_m)$, que la première coordonnée est congrue à ± 1 modulo $p_i^{\alpha_i}$ et les autres à 0). Soit $k_i \ell_i = \ell$ le p.p.c.m. des k_i . Alors $\varepsilon^\ell = (\varepsilon^{k_i})^{\ell_i} \equiv (\pm 1)^{\ell_i} \equiv \pm 1 \pmod{p_i^{\alpha_i}}$ pour tout i ; donc, si le signe est toujours le même, $\varepsilon^\ell \equiv \pm 1 \pmod{n}$ et $z = \frac{1 \pm \varepsilon^\ell}{n} \in A(n)$; sinon $\varepsilon^{2\ell} \equiv 1 \pmod{n}$ et $z = \frac{1 - \varepsilon^{2\ell}}{n} \in A(n)$.

Corollaire 4.6. Soit A l'anneau des entiers d'un corps de nombres défini au théorème 4.5. $A(p) \simeq k_1' \mathbb{Z}$ implique $A(p^\alpha) \simeq k_\alpha' \mathbb{Z}$ où $k_\alpha' \leq p^{\alpha-1} k_1'$ pour tout $p > 2$ et $A(4) \simeq \ell_2 \mathbb{Z}$ implique $A(2^\beta) \simeq \ell_\beta \mathbb{Z}$ où $\ell_\beta \leq 2^{\beta-2} \ell_2$. Et il existe un algorithme fini de détermination de $A(n)$ à partir de $A(2)$ ou $A(4)$, si 2 ou 4 divise n , et des $A(p)$ où p est un diviseur premier de n .

Si $A(p) \simeq k_1' \mathbb{Z}$, il existe $z \in A$ tel que $1 - pz = \pm \varepsilon^{k_1'}$ donc $\pm \varepsilon^{p^{\alpha-1} k_1'} = (\pm \varepsilon^{k_1'})^{p^{\alpha-1}} = (1 - pz)^{p^{\alpha-1}} = 1 - p^\alpha z'$ où $z' \in A$ donc $z' \in A(p) \simeq k_\alpha' \mathbb{Z}$ et $k_\alpha' \leq p^{\alpha-1} k_1'$. De même pour $A(2^\beta)$.

L'algorithme est défini par le théorème 4.5. En effet, $A(n) \simeq k \mathbb{Z}$ où k est le p.p.c.m. de $k_1, \dots, k_v$ ou son double, chaque k_j étant majoré par $p_j^{\alpha_j-1} k_j'$. L'algorithme consiste à calculer les puissances successives de ε et de voir la première congrue à ± 1 modulo n . Si ce n'est pas le cas pour aucune (jusqu'au p.p.c.m. ou son double), alors $A(n)$ est nul.

On va montrer maintenant que si A est l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$, il existe un algorithme fini de détermination de $A(n)$. Vu le corollaire 4.3., on suppose d positif et comme $A(1) \simeq U(A)$ est défini par l'unité fondamentale que

l'on sait calculer, on se limitera à $n \geq 2$. Il suffit, d'après le corollaire 4.6., de trouver un algorithme fini pour $A(2)$, $A(4)$ ou $A(p)$ pour tout p premier impair.

On rappelle d'abord que si l'unité fondamentale de A n'appartient pas à $\mathbb{Z}[\sqrt{d}]$ (c'est parfois le cas pour $d \equiv 5 \pmod{8}$) son cube, lui, appartient à $\mathbb{Z}[\sqrt{d}]$.

Proposition 4.7. Soient A l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$ où $d \geq 0$, ε son unité fondamentale, $\eta + \zeta\sqrt{d}$ celle de $\mathbb{Z}[\sqrt{d}]$. Alors $A(2)$ est isomorphe :

- si $d \not\equiv 1 \pmod{4}$ à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ si ζ est pair

$\mathbb{Z}/2\mathbb{Z} \times 2\mathbb{Z}$ si ζ est impair

- si $d \equiv 1 \pmod{4}$ à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ si $\varepsilon \in \mathbb{Z}[\sqrt{d}]$

$\mathbb{Z}/2\mathbb{Z} \times 3\mathbb{Z}$ si $\varepsilon \notin \mathbb{Z}[\sqrt{d}]$.

Dans le premier cas $\varepsilon^2 \equiv \pm 1 \pmod{2}$, donc $\frac{1 \pm \varepsilon^2}{2} \in \mathbb{Z}[\sqrt{d}]$ et, de plus, si ζ est pair $\frac{1 \pm \varepsilon}{2} \in \mathbb{Z}[\sqrt{d}]$ d'où le résultat. Si $d \equiv 1 \pmod{4}$, on a $\mathbb{Z}[\sqrt{d}] \subset A$, et si ζ est pair $z = \frac{1 + (\eta + \zeta\sqrt{d})}{2} \in A$; si ζ est impair, $\eta \pm 1$ l'est; donc z appartient aussi à A , donc, si $\varepsilon \in \mathbb{Z}[\sqrt{d}]$, $A(2)$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. Si $\varepsilon \notin \mathbb{Z}[\sqrt{d}]$, ni $\frac{1 \pm \varepsilon}{2}$, ni $\frac{1 \pm \varepsilon^2}{2}$ n'appartiennent à A , d'où le résultat.

Proposition 4.8. Soient A l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$ où $d \geq 0$, ε son unité fondamentale, $\eta + \zeta\sqrt{d}$ celle de $\mathbb{Z}[\sqrt{d}]$.

Si $d \not\equiv 1 \pmod{4}$ et $N(\varepsilon) = -1$, alors $A(4) \simeq 4\mathbb{Z}$.

Si $d \not\equiv 1 \pmod{4}$ et $N(\varepsilon) = 1$, alors $A(4) \simeq 2\mathbb{Z}$ si $\zeta \not\equiv 0 \pmod{4}$ et $A(4) \simeq \mathbb{Z}$ si $\zeta \equiv 0 \pmod{4}$.

Si $d \equiv 1 \pmod{4}$, $A(4) \simeq \alpha\beta\mathbb{Z}$ où $\alpha = 1$ ou 2 suivant que $N(\varepsilon) = +1$ ou -1 et $\beta = 1$ ou 3 suivant que $\varepsilon \in \mathbb{Z}[\sqrt{d}]$ ou non.

Si $\varepsilon \notin \mathbb{Z}[\sqrt{d}]$, ni $\frac{1 \pm \varepsilon}{4}$, ni $\frac{1 \pm \varepsilon^2}{4}$ n'appartiennent à A , donc

$A(4) \simeq 3\alpha\mathbb{Z}$ où α est défini par $\mathbb{Z}[\sqrt{d}](4) \simeq \alpha\mathbb{Z}$. Si d est impair $\eta\zeta$ est pair donc $1 \pm \varepsilon^2 \equiv 1 \pm (\eta^2 + \zeta^2 d) \pmod{4}$ peut être congru à 0 modulo 4. (en choisissant le signe convenable). Si d est pair on a $2\eta\zeta \equiv 0 \pmod{4}$ si, et seulement si, $N(\varepsilon) = +1$ et, dans ce cas,

$$1 - \varepsilon^2 = 1 - (\eta^2 + 2\eta\zeta\sqrt{d} + \zeta^2 d) = 1 - N(\varepsilon) + 2\eta\zeta\sqrt{d} + 2\zeta^2 d \equiv 0 \pmod{4}.$$

Ainsi dans tous ces cas, $\mathbb{Z}[\sqrt{d}](4) \supset 2\mathbb{Z}$. De plus, $1 \pm (\eta + \zeta\sqrt{d}) \equiv 0 \pmod{4}$ si et seulement si $\zeta \equiv 0 \pmod{4}$ et dans ce cas $\mathbb{Z}[\sqrt{d}](4) \simeq \mathbb{Z}$. Si d est pair et $N(\varepsilon) = -1$, $1 - \varepsilon^4 \equiv 0 \pmod{4}$ et $1 \pm \varepsilon^3 \not\equiv 1 \pm \varepsilon^2$ donc $A(4) \simeq 4\mathbb{Z}$. Le cas $d \not\equiv 1$ est terminé. Vue la première remarque et le fait que si $\varepsilon \notin \mathbb{Z}[\sqrt{d}]$,

$\zeta \equiv 0 \pmod{4}$ si et seulement si $N(\varepsilon) = 1$, le cas $d \equiv 1$ l'est aussi.

Proposition 4.9. Soient un entier $d > 1$, A l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$ d'unité fondamentale ε , $\varepsilon' = \eta + \zeta \sqrt{d}$ celle de $\mathbb{Z}[\sqrt{d}]$ et p un nombre premier impair. Il existe un algorithme fini de détermination de $A(p)$ et $A(p) \simeq \rho \mathbb{Z}$ ou $3\rho \mathbb{Z}$ suivant si $\varepsilon \in \mathbb{Z}[\sqrt{d}]$ ou non où $0 \leq \rho \leq p-1$ (et même ρ divise $(p-1)/2$ si p divise d).

Comme $p > 2$, si $\varepsilon^k \notin \mathbb{Z}[\sqrt{d}]$, $\frac{1 \pm \varepsilon^k}{p} \notin A$. Donc si k est le plus petit entier tel que $z = \frac{1 \pm \varepsilon^k}{p} \in \mathbb{Z}[\sqrt{d}]$, alors $A(p) \simeq k\mathbb{Z}$ ou $3k\mathbb{Z}$ suivant si $\varepsilon \in \mathbb{Z}[\sqrt{d}]$ ou non.

On écrira k en base p (d'où $k = \sum_{i=0}^{\ell} k_i p^i$, $0 \leq k_i < p$) et comme

$$\varepsilon^p = (\eta + \zeta \sqrt{d})^p \equiv \eta^p + \zeta^p d^{\frac{p-1}{2}} \sqrt{d} \equiv \eta + \zeta d^{\frac{p-1}{2}} \sqrt{d} \pmod{p}$$

on distinguera les trois cas, donnés par le symbole de Legendre, $\left(\frac{d}{p}\right) = 0, 1$ ou -1 .

S'il est nul, c'est-à-dire si p divise d , alors $\varepsilon^p \equiv \eta \pmod{p}$ donc

$$\varepsilon_1^{p k_i} = (\varepsilon_1^p)^{k_i} \equiv (\eta^p)^{k_i} \equiv \eta^{k_i} \pmod{p}.$$

Si $\tau_p(k)$ est la somme des chiffres de k exprimée en base p , on a

$$\varepsilon_1^k = \prod_{i=0}^{\ell} \varepsilon_1^{p^i k_i} \equiv \prod_{i=0}^{\ell} \eta^{k_i} = \eta^{\tau_p(k)} \pmod{p}$$

où $\tau_p(k) \leq k$. Comme $\eta^p \equiv \eta \pmod{p}$, de même $\eta^{\tau_p(k)} \equiv \eta^{\tau_p^2(k)} \equiv \eta^{\tau_p^3(k)} \equiv \dots$

$\pmod{p}$. La suite d'entiers positifs $k, \tau_p(k), \tau_p^2(k), \tau_p^3(k), \dots$ étant décroissante, elle est stationnaire ; sa limite $\overline{\tau_p(k)}$ est strictement inférieure à p

(car si $k \geq p$, $\tau_p(k) < k$) ; on a alors $\varepsilon_1^k \equiv \eta^{\overline{\tau_p(k)}}$ où $0 \leq \overline{\tau_p(k)} < p$. Si $A(p) \simeq$

$\rho \mathbb{Z}$, comme $\eta^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ implique $\frac{1 \pm \varepsilon_1^k}{p} \in \mathbb{Z}[\sqrt{d}]$, on en déduit

$\rho \mathbb{Z} \supset \frac{p-1}{2} \mathbb{Z}$, donc p divise $\frac{p-1}{2}$ c.q.f.d. Et l'algorithme est la détermination du plus petit diviseur ρ de $\frac{p-1}{2}$ tel que $\eta^{\rho} \equiv \pm 1 \pmod{p}$.

S'il vaut 1, c'est-à-dire si $d^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, alors $\varepsilon^p \equiv \varepsilon' \pmod{p}$ d'où

$$\varepsilon_1^k = \prod_{i=0}^{\ell} (\varepsilon_1^p)^{k_i} \equiv \prod_{i=0}^{\ell} \varepsilon_1^{k_i} = \varepsilon_1^{\tau_p(k)} \equiv \varepsilon_1^{\overline{\tau_p(k)}} \pmod{p}$$

et ρ est le plus petit entier inférieur à p tel que $\varepsilon_1^{\rho} \equiv \pm 1 \pmod{p}$ (c'est 0 si ce n'est jamais vérifié).

Si l'on a -1 , c'est-à-dire si $\frac{p-1}{2} \equiv -1 \pmod{p}$, $\varepsilon^p \equiv \eta - \zeta \sqrt{d} = \sigma(\varepsilon')$ (mod. p) ainsi $\varepsilon^{p^i k_i} \equiv \sigma(\varepsilon')^{p^{i-1} k_i} \equiv \sigma^i(\varepsilon')^{k_i}$ qui est congru à $\varepsilon_1^{k_i}$ ou $\sigma(\varepsilon_1)^{k_i}$ suivant la parité de i . Ainsi, si $\tau_p'(k)$ désigne la valeur absolue de la différence entre la somme des chiffres de rang pair de k et celle de ceux de rang impair et si k' est la plus petite de ces deux sommes

$$\varepsilon^{k_i} \equiv \prod \sigma^i(\varepsilon')^{k_i} = N(\varepsilon')^{k'} \varepsilon^{\tau_p'(k)} \quad \text{ou} \quad N(\varepsilon')^{k'} \sigma(\varepsilon')^{\tau_p'(k)}.$$

Mais si $z \in A(p)$, $\varepsilon^{k_i} \equiv \pm 1 \pmod{p}$; cela implique $\varepsilon' \equiv \sigma(\varepsilon')$ (mod. p) puis

$$\pm 1 \equiv \varepsilon^{\tau_p'(k)} \equiv \varepsilon^{\overline{\tau_p'(k)}} \pmod{p}$$

où $\overline{\tau_p'}$ est la limite définie à partir de τ_p' de la même manière que pour τ_p . L'algorithme est le même que dans ce cas car $0 \leq \overline{\tau_p'(k)} < p$.

Ces trois propositions permettront de démontrer le théorème suivant :

Théorème 4.10. Soient A l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$ où $d > 0$, ε son unité fondamentale, $\eta + \zeta \sqrt{d}$ celle de $\mathbb{Z}[\sqrt{d}]$. Si $n > 2$, $A(n) \simeq k\mathbb{Z}$ si $\varepsilon \in \mathbb{Z}[\sqrt{d}]$ et $A(n) \simeq 3k\mathbb{Z}$ si $\varepsilon \notin \mathbb{Z}[\sqrt{d}]$ où, ϕ étant l'indicateur d'Euler, k vérifie les inégalités

$$\begin{aligned} 0 &\leq k \leq 4\phi(n) \quad \text{si} \quad d \equiv 2 \pmod{4} \quad \text{et} \quad N(\varepsilon) = -1 \quad \text{et} \quad n \text{ pair} \\ 0 &\leq k \leq 2\phi(n) \quad \text{sinon} \end{aligned}$$

C'est la plus petite valeur telle que $(\eta + \zeta \sqrt{d})^k \equiv \pm 1 \pmod{4}$ et si ce n'est jamais le cas pour $1 \leq k \leq 4\phi(n)$ (resp. $2\phi(n)$), k est nul et $A(n) \simeq \{0\}$.

D'après la proposition 4.2., si $d \equiv 2$ et $N(\varepsilon) = -1$, $A(4) \simeq 4\mathbb{Z}$, donc d'après le corollaire 4.6., $A(2^\beta) \simeq \ell_\beta \mathbb{Z}$ où $\ell_\beta \leq 2^\beta = 2\phi(2^\beta)$. Dans tous les autres cas $\ell_\beta \leq 2^{\beta-1} = \phi(2^\beta)$ et, d'après le corollaire 4.6. et la proposition 4.9., si p est premier impair $A(p^\alpha) \simeq k_\alpha \mathbb{Z}$ où $k_\alpha \leq p^{\alpha-1}(p-1) = \phi(p^\alpha)$. Comme le p.p.c.m. de plusieurs nombres est inférieur ou égal à leur produit, on déduit du théorème 4.5. que, dans le second cas,

$$k \leq 2\phi(p_1^{\alpha_1}) \dots \phi(p_v^{\alpha_v}) = 2\phi(p_1^{\alpha_1}) \dots p_v^{\alpha_v} = 2\phi(n)$$

et $k \leq 4\phi(n)$ dans le premier si $n \equiv 0 \pmod{4}$; il en est de même si $n \equiv 2 \pmod{4}$ car la projection de $A(2)$ suivant $\mathbb{Z}/2\mathbb{Z}$ est $\mathbb{Z}$ ou $2\mathbb{Z}$ et $2 = 2\phi(2)$.

BIBLIOGRAPHIE

- [1] M. ARTIN, Grothendieck Topologies, Harvard University, 1962.
- [2] H. BASS, Lectures on topics in algebraic K-theory, Tata Institute of Fundamental Research, Bombay, 1967.
- [3] Z.I. BOREVITCH et I.R. CHAFAREVITCH, Théorie des Nombres, Gauthier-Villars, Paris, 1967.
- [4] A. MICALI et Ph. REVOY, Algèbres de Clifford séparables, Montpellier 1969 (non publié), M.R. 46 (1973), 198 b.
- [5] A. MICALI et Ph. REVOY, Modules quadratiques, livre en préparation.
- [6] A. MICALI et O.E. VILLAMAYOR, Sur les algèbres de Clifford, Ann. Sc. Ec. Normale Sup., 4è série, 1 (1968), 271-304.
- [7] A. MICALI et O.E. VILLAMAYOR, Sur les algèbres de Clifford II, Journal für die Reine und Angewandte Mathematik, 242 (1970), 61-90.
- [8] C. SMALL, The group of quadratic extensions, J. of Pure and Applied Algebra 2 (1972), 83-105.
- [9] J.-D. THEROND, Sur deux conjectures de Small, ce volume, p.103-115.
- [10] J.-D. THEROND, Le groupe des extensions quadratiques séparables libres de l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$, C.R.Acad. Sc. Paris, 281 (1975) 939-943.

Institut de Mathématiques
 Université des Sciences et Techniques
 du Languedoc
 Place E. Bataillon

34060 MONTPELLIER CEDEX

FRANCE
