MÉMOIRES DE LA S. M. F.

ARTIBANO MICALI
J.-D. THÉROND

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>

Col. sur les Formes Quadratiques (1975, Montpellier)
Bull. Soc. Math. France
Mémoire 48, 1976, p. 75-87

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, $n \geqslant 0$ 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 $.(n) : \underline{Ann} \to \underline{Ab}$.

Pour tout anneau A, on notera $Ip(A)$ 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 $Ip(A)$. 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 $\phi : A(2) \to A(4)$ définie par $x \mapsto x - x^2$ est un morphisme de groupes abéliens dont le noyau est $Ip(A)$. Si l'on désigne par $G(A)$ son conoyau, on a la suite exacte de groupes abéliens $0 \to Ip(A) \to A(2) \xrightarrow{\phi} A(4) \to G(A) \to 0$.

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, $Ip(A) = A(2)$, donc $A(4) \tilde{\to} G(A)$ est un isomorphisme de groupes abéliens.

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

un morphisme de groupes abéliens, car quels que soient a et b dans $A(n)$, $1 - n(a \dot{+} b) = (1 - n\,a)(1 - n\,b)$. 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 $\frac{1}{n}(1 - a) \leftarrow\!\shortmid a$.

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 $\phi : A(4) \to U(A)$ le morphisme défini par $a \mapsto 1 - 4a$. Si $x \in \mathrm{Im}(A(2) \to A(4))$, il existe un élément $a \in A(2)$ tel que $x = a - a^2$, donc $\phi(x) = 1 - 4\,x = (1 - 2\,a)^2 \in U^2(A)$. Par passage aux quotients, il existe un unique morphisme de groupes abéliens $\overline{\phi} : G(A) \dashrightarrow U(A)/U^2(A)$ rendant commutatif le diagramme

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

où les flèches verticales sont canoniques. Si 2 est inversible dans A, le morphisme $\overline{\phi} : G(A) \xrightarrow{\sim} U(A)/U^2(A)$ 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 $1 - 4\,a$ est inversible dans A. L'application $\mathcal{Q}(A) \to G(A)$ définie par $A[x] \mapsto \overline{a}$ 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 $\phi : A(m) \to A(n)$

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

Supposons donc que $\phi : \mathbb{R} \to \mathbb{R}$ soit une fonction continue et différentiable vérifiant l'équation fonctionnelle $\phi(x + y - m\,x\,y) = \phi(x) + \phi(y) - n\,\phi(x)\,\phi(y)$ quels que soient x et y dans $\mathbb{R}$. On voit donc que pour tout $x \in \mathbb{R}$ et pour $h > 0$, $\phi(x + (1 - m\,x)\,h) - \phi(x) = (1 - n\,\phi(x))\,\phi(h)$ 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 $h \to 0$, 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 $\phi(x) = \frac{1}{n}(1 - (1-m\,x)^{\frac{n\,\phi'(0)}{m}})$; 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 $n = 0$, $\phi(x) = -\frac{\phi'(0)}{m}\log(1 - m\,x)$. Finalement, pour $m = n = 0$, $\phi(x) = \phi'(0)x$.

Supposons que $\phi(x) = \frac{1}{n}(1 - (1 - m\,x)^{\frac{n\,\phi'(0)}{m}})$. 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 $\phi^{(k+1)}(0) = (-1)^k\,\phi'(0)\prod_{j=1}^{k}(n\,\phi'(0) - j\,m)$, pour tout entier $k \geqslant 1$. Supposons qu'il existe un entier k tel que $n\,\phi'(0) - k\,m = 0$; dans ces conditions, $\phi^{(k+1)}(0) = 0$ et $\phi^{(j)}(0) = 0$ pour tout entier $j \geqslant k+1$, donc $\phi(x) = \sum_{j=1}^{k} \frac{1}{j!}\phi^{(j)}(0)\,x^j$ pour tout x dans $\mathbb{R}$. Mais il n'est pas encore dit que l'application $\phi : A(m) \to A(n)$ 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 $j = 1,\ldots,k$.

Nous avons déjà vu que pour tout anneau A, l'application $\phi : A(2) \to A(4)$ 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 $\phi : A(m) \to A(n)$ fourni par la formule $\phi(x) = \frac{1}{n}(1 - (1 - m\,x)^{\frac{n\,\phi'(0)}{m}})$ 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 $\phi : A(m) \to A(m^2)$ 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 $(1 - m\,x)^m = 1 - m^2\,\phi(x)$ pour tout $x \in A(m)$ nous montre que l'application $Ip_m(A) \to \mu_m(A)$ définie par $x \mapsto 1 - m\,x$ est un morphisme de groupes abéliens. On définit de la sorte un morphisme de foncteurs $Ip_m \to \mu_m$. De plus, le morphisme $Ip_m(A) \to \mu_m(A)$ 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 $Ip_m(A) \leftarrow \mu_m(A)$ est donné par $\frac{1}{m}(1 - x) \leftarrow\!\shortmid x$.

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

Lemme 2.1. Soient m et n deux entiers $\geqslant 1$. Pour tout x dans $A(m)$, on a $n.x = \sum_{k=1}^{n}(-1)^{k+1}\binom{n}{k}m^{k-1}x^k$ et $1 - m(n.x) = (1 - m\,x)^n$.

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

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

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

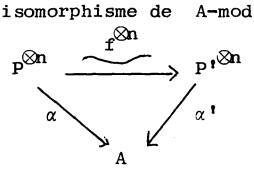
pour tout x dans $A(m)$. L'autre formule se démontre aussi par récurrence.

Proposition 2.2. Si $\phi : A(m) \to A(m^2)$ est le morphisme défini par $x \mapsto x - \sum_{k=2}^{m} (-1)^k \binom{m}{k} m^{k-2} x^k$, alors $m.x = m\,\phi(x)$ pour tout $x \in A(m)$.

Ceci résulte immédiatement du lemme précédant, compte tenu de la définition de ϕ. Il s'ensuit que $\mathbb{Z}/(m) \otimes_{\mathbb{Z}} Ip_m(A) \simeq Ip_m(A)$, donc $Ip_m(A)$ 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 $\mathcal{P}_n(A)$

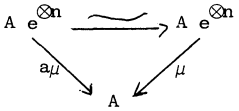
Soient A un anneau, $n \geqslant 1$ un nombre entier et $\mathcal{P}_n(A)$ l'ensemble des couples (P,α), où P est un A-module projectif de type fini et de rang 1 et $\alpha : P^{\otimes n} \xrightarrow{\sim} A$ est un isomorphisme de A-module. De plus, on dira que deux éléments (P,α) et (P',α') de $\mathcal{P}_n(A)$ 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 :



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 $\alpha * \alpha' : (P \otimes P')^{\otimes n} \xrightarrow{\sim} P^{\otimes n} \otimes P'^{\otimes n} \xrightarrow{\alpha \otimes \alpha'} A \otimes A \xrightarrow{\mu} A$ est l'isomorphisme composé évident, $\mu : A \otimes A \to A$ étant la multiplication de l'anneau A. L'élément neutre de $\mathcal{P}_n(A)$ est le couple (A,μ) où $\mu : A^{\otimes n} \to A$ est la multiplication de A et l'opposé de (P,α) est $(P,\alpha) + \ldots + (P,\alpha)$ $(n-1$ 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 $n \geqslant 1$. 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 $n \geqslant 1$, on a la suite exacte de groupes abéliens $0 \to \mu_n(A) \to U(A) \xrightarrow{n} U(A) \to \mathcal{P}_n(A) \to \mathrm{Pic}(A) \xrightarrow{n} \mathrm{Pic}(A)$, où $\xrightarrow{n}$ désigne l'élévation à la puissance n, $\mathcal{P}_n(A) \to \mathrm{Pic}(A)$ est le morphisme qui à la classe de (P,α) associe la classe de P dans Pic(A) et $U(A) \to \mathcal{P}_n(A)$ est le morphisme défini par $a \mapsto (A, a\mu)$.

Ici Pic(A) désigne le groupe de Picard de l'anneau A. Il est évident que la flèche composée $U(A) \to \mathcal{P}_n(A) \to \mathrm{Pic}(A)$ est nulle. Si $(P,\alpha) \in \mathcal{P}_n(A)$ a une image nulle dans 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 $\mathcal{P}_n(A) \to \mathrm{Pic}(A) \xrightarrow{n} \mathrm{Pic}(A)$ 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 $\mathcal{P}_n(A) \to \mathrm{Pic}(A)$. Ceci nous dit que la suite $\mathcal{P}_n(A) \to \mathrm{Pic}(A) \xrightarrow{n} \mathrm{Pic}(A)$ est exacte. Montrons finalement que la suite $U(A) \xrightarrow{n} U(A) \to \mathcal{P}_n(A)$ 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 $Ae \to Ae$, $e \mapsto be$, où $b \in U(A)$, rendant commutatif le diagramme



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

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

$$0 \to U(A)/U^n(A) \to \mathcal{P}_n(A) \to \mathrm{Pic}_n(A) \to 0 \quad ,$$

où $\mathrm{Pic}_n(A)$ est le noyau du morphisme $\mathrm{Pic}(A) \xrightarrow{n} \mathrm{Pic}(A)$, élévation à la puissance n. En particulier, si $\mathrm{Pic}_n(A) = 0$, (c'est le cas si 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 $\mathfrak{X}$ (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 $0 \to \mu_n \to U \to U^n \to 0$ nous donne la suite exacte de faisceaux $0 \to \mu_n \to U \xrightarrow{n} U \to 0$. Si l'on passe en cohomologie, on a la suite exacte longue de groupes abéliens $0 \to \mu_n(A) \to U(A) \xrightarrow{n} U(A) \to H^1(\mathfrak{X}, A, \mu_n) \to H^1(\mathfrak{X}, A, U) \xrightarrow{n} \xrightarrow{n} H^1(\mathfrak{X}, A, U) \to H^2(\mathfrak{X}, A, \mu_n) \to \ldots$; or, on sait (cf. [1]) qu'il existe un isomor-

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

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

Il est clair que pour les anneaux A dans lesquels n est inversible, on a un isomorphisme de groupes abéliens $H^i(\mathfrak{X},A,Ip_n) \xrightarrow{\sim} H^i(\mathfrak{X},A,\mu_n)$, pour tout entier $i \geqslant 0$, mais en général, on ne sait pas interpréter les groupes $H^1(\mathfrak{X},A,Ip_n)$ pour $n \geqslant 3$. Par contre, si $\mathcal{Q}(A)$ est le groupe des extensions quadratiques de A et si $\mathfrak{X}$ est la topologie f. p. p. f. sur Ann, il existe un isomorphisme de groupes abéliens $\mathcal{Q}(A) \simeq H^1(\mathfrak{X},A,Ip)$ (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 $0 \to Ip(A) \to A(2) \to A(4) \to G(A) \to 0$, où $A(2) \to A(4)$ 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 $0 \to Ip \to .(2) \to .(4) \to 0$. En passant en cohomologie, pour la topologie f. p. p. f., on a pour tout anneau A la suite exacte longue de groupes abéliens $0 \to Ip(A) \to A(2) \to A(4) \to H^1(\mathfrak{X},A,Ip) \to$ $\to H^1(\mathfrak{X},A,.(2)) \to H^1(\mathfrak{X},A,.(4)) \to H^2(\mathfrak{X},A,Ip) \to \ldots$, d'où la suite exacte $0 \to$ $\to G(A) \to \mathcal{Q}(A) \to H^1(\mathfrak{X},A,.(2)) \to H^1(\mathfrak{X},A,.(4)) \to H^2(\mathfrak{X},A,Ip) \to \ldots$. En particulier, si A est un anneau local, ceci nous donne la suite exacte de groupes abéliens $0 \to H^1(\mathfrak{X},A,.(2)) \to H^1(\mathfrak{X},A,.(4)) \to H^2(\mathfrak{X},A,Ip) \to \ldots$ Si A est un anneau (non nécessairement local) dans lequel $2 = 0$, on a l'isomorphisme de groupes abéliens $G(A) \xrightarrow{\sim} \mathcal{Q}(A)$; 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 $A \to B$ on a, pour tout $i \geqslant 0$, $H^i(B/A,Ip_n) \simeq H^i(B/A,\mu_n)$ (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 $n^{ième}$ de l'unité dans $Z[i] \otimes_Z Z[i]$ est $1 \otimes 1$; alors que si n est pair il peut y avoir plusieurs racines $n^{ièmes}$ de l'unité. Par exemple, pour $n = 2$, les racines carrées de l'unité dans $Z[i] \otimes_Z Z[i]$ 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 $1-n\,z = -1$ si et seulement si $n = 2$ et $z = 1$ et, pour tout $n \geqslant 2$, si $\zeta \notin \mathbb{R}$, alors $1-nz \neq \zeta$.*

Si $1-n\,z = -1$, $2 = n\,z$ d'où, si N désigne la norme pour l'extension K de $\mathbb{Q}$, $2^m = N(2) = N(n\,z) = n^m N(z)$ 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 $z = \dfrac{1-\zeta}{n} \in \mathbb{Q}(\zeta_h)$ d'où, si N' désigne la norme de l'extension $\mathbb{Q}(\zeta_h)$ de $\mathbb{Q}$ et ϕ l'indicateur d'Euler,

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

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 $\zeta \notin \mathbb{R}$, $|1 - \zeta| < 2$ donc, G désignant le groupe de Galois de $\mathbb{Q}(\zeta_h)$ sur $\mathbb{Q}$:

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

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

$$\theta : A(n) \to U(A) \to H \times \mathbb{Z}^r$$
$$z \mapsto 1-nz = \zeta_h^a \varepsilon_1^{k_1} \dots \varepsilon_r^{k_r} \mapsto (\zeta_h^a, k_1, \dots, k_r) \ ;$$

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

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 $z^o \in A(n)$ est l'opposé de z, $1-nz^o = \zeta_h^{-a} \varepsilon_1^{-k_1} \dots \varepsilon_r^{-k_r}$ et $Z = z' \tilde{+} z^o \in A(n)$ vérifie $1-nZ = (1-nz')(1-nz^o) = \zeta^{b-a}$. Donc, d'après le lemme, $\zeta^{b-a} = \pm 1$ si $n = 2$ et $\zeta^{b-a} = 1$ si $n > 2$. On peut donc définir une application (projection)

$$\theta' : H \times \mathbb{Z}^r \to \mathbb{Z}^r \qquad \text{si } n > 2$$
$$\theta' : H \times \mathbb{Z}^r \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^r \qquad \text{si } n = 2$$

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

Corollaire 4.3. Si K est un corps quadratique imaginaire, $A(2) \simeq \mathbb{Z}/2\mathbb{Z}$ 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 $\alpha \geqslant 1$ 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 $p_1^{\alpha_1} \dots p_\upsilon^{\alpha_\upsilon}$ est la décomposition en produit de facteurs premiers de $n > 2$ et si $A(p_i^{\alpha_i}) \simeq (\mathbb{Z}/2\mathbb{Z})^\gamma \, k_{i1}\mathbb{Z} \times \dots \times k_{ir}\mathbb{Z}$ où $\gamma = 1$ ou 0 suivant que $p_i^{\alpha_i}$ égale 2 ou non, alors $A(n) \simeq k_1\mathbb{Z} \times \dots \times k_r\mathbb{Z}$ où k_i est un multiple du p.p.c.m. de $k_{1j}, \dots, k_{\upsilon j}$.

En effet, l'application $A(n) \to A(p_i^{\alpha_i})$ 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 $i = 1, \dots, \upsilon$, 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 $A(p_i^{\alpha_i}) \simeq (\mathbb{Z}/2\mathbb{Z})^\gamma \, k_i\mathbb{Z}$ alors $A(n) \simeq k\mathbb{Z}$ où k est le p.p.c.m. de $k_1, \dots, k_\upsilon$ 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, $U(A) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ 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 $(1, e_2, \ldots, e_m)$, 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 $z = \dfrac{1 \mp \varepsilon^{\ell}}{n} \in A(n)$; sinon $\varepsilon^{2\ell} \equiv 1 \pmod{n}$ et $z = \dfrac{1 - \varepsilon^{2\ell}}{n} \in A(n)$.

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 $k_{\alpha}' \leqslant p^{\alpha-1} k_1'$ pour tout $p > 2$ et $A(4) \simeq \ell_2 \mathbb{Z}$ implique $A(2^{\beta}) \simeq \ell_{\beta} \mathbb{Z}$ où $\ell_{\beta} \leqslant 2^{\beta-2} \ell_2$. 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 $k_{\alpha}' \leqslant p^{\alpha-1} k_1'$. 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 $k_1, \ldots, k_v$ 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 $n \geqslant 2$. 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 $d \geqslant 0$, 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'appartient à A, d'où le résultat.

Proposition 4.8. Soient A l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$ où $d \geqslant 0$, 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 $A(4) \sim 4\mathbb{Z}$.

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

Si $d \equiv 1 \pmod 4$, $A(4) \sim \alpha\beta\mathbb{Z}$ 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 $A(4) \sim 3\alpha\mathbb{Z}$ où α est défini par $\mathbb{Z}[\sqrt{d}]\ (4) \sim \alpha\mathbb{Z}$. 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 $\mathbb{Z}[\sqrt{d}](4) \sim \mathbb{Z}$. Si d est pair et $N(\varepsilon) = -1$, $1 - \varepsilon^4 \equiv 0 \pmod 4$ et $1 \pm \varepsilon^3 \not\equiv 0 \not\equiv 1 \pm \varepsilon^2$ donc $A(4) \sim 4\mathbb{Z}$. 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 $Z[\sqrt{d}]$ et p un nombre premier impair. Il existe un algorithme fini de détermination de A(p) et $A(p) \sim \rho Z$ ou $3 \rho Z$ suivant si $\varepsilon \in Z[\sqrt{d}]$ ou non où $0 \leqslant \rho \leqslant p-1$ (et même ρ divise $(p-1)/2$ si p divise d).

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

On écrira k en base p (d'où $k = \sum_{i=0}^{\ell} k_i p^i$, $0 \leqslant k_i < p$) 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, $(\frac{d}{p}) = 0$, 1 ou -1.

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

$$\varepsilon_1^{p^i k_i} = (\varepsilon_1^{p^{i-1}})^{k_i} \equiv (\eta^{p^{i-1}})^{k_i} \equiv \eta^{k_i} \pmod p .$$

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 $\tau_p(k) \leqslant k$. Comme $\eta^p \equiv \eta \pmod p$, de même $\eta^{\tau_p(k)} \equiv \eta^{\tau_p^2(k)} \equiv \eta^{\tau_p^3(k)} \equiv \cdots \pmod p$. La suite d'entiers positifs $k, \tau_p(k), \tau_p^2(k), \tau_p^3(k), \ldots$ étant décroissante, elle est stationnaire ; sa limite $\overline{\tau_p(k)}$ est strictement inférieure à p (car si $k \geqslant p$, $\tau_p(k) < k$) ; on a alors $\varepsilon_1^k \equiv \eta^{\overline{\tau_p(k)}} \pmod p$ où $0 \leqslant \overline{\tau_p(k)} < p$. Si $A(p) \sim \rho Z$, comme $\eta^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$ implique $\frac{1 \pm \varepsilon_1}{p} \in Z[\sqrt{d}]$, on en déduit $\rho Z \supset \frac{p-1}{2} Z$, 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

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

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).

S'il vaut -1, c'est-à-dire si $d^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, $\varepsilon'^{p} \equiv \eta - \zeta\sqrt{d} = \sigma(\varepsilon') \pmod{p}$ 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

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

Mais si $z \in A(p)$, $\varepsilon'^{k} \equiv \pm 1 \pmod{p}$; cela implique $\varepsilon' \equiv \sigma(\varepsilon') \pmod{p}$ 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 $0 \leqslant \overline{\tau'_p}(k) < p$.

Ces trois propositions permettrons 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 $n > 2$, $A(n) \sim k\mathbb{Z}$ si $\varepsilon \in \mathbb{Z}[\sqrt{d}]$ et $A(n) \sim 3k\mathbb{Z}$ si $\varepsilon \notin \mathbb{Z}[\sqrt{d}]$ où, ϕ étant l'indicateur d'Euler, k vérifie les inégalités

$$0 \leqslant k \leqslant 4\phi(n) \text{ si } d \equiv 2 \pmod{4} \text{ et } N(\varepsilon) = -1 \text{ et } n \text{ pair}$$
$$0 \leqslant k \leqslant 2\phi(n) \text{ sinon} .$$

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 $1 \leqslant k \leqslant 4\phi(n)$ (resp. $2\phi(n)$), k est nul et $A(n) \sim \{0\}$.

D'après la proposition 4.8., si $d \equiv 2$ et $N(\varepsilon) = -1$, $A(4) \sim 4\mathbb{Z}$, donc d'après le corollaire 4.6., $A(2^\beta) \sim \ell_\beta \mathbb{Z}$ où $\ell_\beta \leqslant 2^\beta = 2\phi(2^\beta)$. Dans tous les autres cas $\ell_\beta \leqslant 2^{\beta-1} = \phi(2^\beta)$ et, d'après le corollaire 4.6. et la proposition 4.9., si p est premier impair $A(p^\alpha) \sim k_\alpha \mathbb{Z}$ où $k_\alpha \leqslant p^{\alpha-1}(p-1) = \phi(p^\alpha)$. 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,

$$k \leqslant 2\phi(p_1^{\alpha_1}) \ldots \phi(p_\upsilon^{\alpha_\upsilon}) = 2\phi(p_1^{\alpha_1} \ldots p_\upsilon^{\alpha_\upsilon}) = 2\phi(n)$$

et $k \leqslant 4\phi(n)$ 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 Andgewandte 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 $Q(\sqrt{d})$, 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