MÉMOIRES DE LA S. M. F.

J.-D. THEROND

Sur deux conjectures de Small

Mémoires de la S. M. F., tome 48 (1976), p. 117-122

<http://www.numdam.org/item?id=MSMF_1976__48__117_0>

Col. sur les Formes quadratiques
Bull. Soc. Math. France
Mémoire 48, 1976, p. 117-122

SUR DEUX CONJECTURES DE SMALL

par

J.-D. THEROND

Soient A un anneau commutatif unitaire, $U(A)$ le groupe de ses éléments inversibles et $G(A)$ le groupe défini en [2, § 7]. Si $A(4)$ désigne le groupe des éléments $z \in A$ tels que $1-4z \in U(A)$ (muni de la loi $z \circ z' = z+z'-4zz'$) il y est montré, si $\alpha : G(A) \to U(A)/U^2(A)$ est définie par $\alpha(z) = \overline{1-4z}$, que le diagramme suivant commute :

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

Dans [3] Small conjecture, si $d > 0$, les résultats suivants

$G(\mathbb{Z}[\sqrt{d}]) \neq \{0\}$ si $d \equiv 3 \pmod 4$ et $G(\mathbb{Z}[\sqrt{d}]) = \{0\}$ si $d \equiv 2$.

On se propose de déterminer $G(A)$ quand A est l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$, quand d est positif (sinon $A(4)$ est nul).

Comme A est intégralement clos, d'après le lemme 6 de [1], l'application α est injective. On cherchera donc $G(A)$ en déterminant $\mathrm{Im}(\alpha)$.

Lemme 1. Si $z \in A(4)$ alors $z \in \mathbb{Z}[\sqrt{d}]$ et $N(1-4z) = 1$.

Preuve. Si $d \not\equiv 1 \pmod 4$ $A = \mathbb{Z}[\sqrt{d}]$. Sinon soit $0 \neq z = a_o + b_o \frac{1+\sqrt{d}}{2} \in A$

$N(1-4z) = N(1-4a_o - 2b_o - 2b_o\sqrt{d}) = (1-4a_o-2b_o)^2 - (2b_o)^2 d = 1+4k$ d'où $N(1-4z) = 1$.

En développant on en déduit $b_o^2 d = (2a_o + b_o)(2a_o + b_o - 1)$ qui est pair, or d est impair donc b_o est pair et $z \in \mathbb{Z}[\sqrt{d}]$.

Soit maintenant $z = a+b\sqrt{d} \in A(4) \subset \mathbb{Z}[\sqrt{d}]$. Alors

$$N(1-4z) = \pm 1 = N(1-4a-4b\sqrt{d}) = 1 + 8(2a^2 - a - 2b^2 d) ;$$

seul $+1$ convient (et le lemme est démontré) et $2a^2 - a = 2b^2 d$.

Ainsi $a = 2^{\alpha+1}a'$, $b = 2^{\beta}b'$, $\alpha \geqslant 0$, $\beta \geqslant 0$, a' et b' impairs et

$$2^{\alpha+1}a'(2^{\alpha+2}a' - 1) = 2^{2\beta+1}b'^2 d \quad .$$

Comme $a'(2^{\alpha+2}a' - 1)$ est impair on obtient, en égalant les puissances de 2

$\alpha+1 = 2(\beta+1)$ si $d = 2d'$ $\qquad$ $\alpha+1 = 2\beta+1$ si $d = d'$ impair

d'où, après simplification par $2^{\alpha+1}$:

$$a'(2^{\alpha+2}a' - 1) = b'^2 d' \quad .$$

Si a_1^2 est le plus grand carré divisant a', $a' = \delta a_1^2$ d'où

$$\delta a_1^2(2^{\alpha+2} a_1^2 \delta - 1) = b'^2 d'$$

où δ et d sont sans facteur carré et où δ et a_1^2 sont premiers avec $2^{\alpha+2} a_1^2\delta - 1$ donc δ divise d' et a_1 divise b'. Ainsi $d' = \delta d_3$ et $b' = a_2 y$ et alors

$$2^{\alpha+2}a_1^2\delta - 1 = d_3 y^2$$

Comme α est positif et y est impair on en déduit $d_3 \equiv 3 \pmod 4$. Si d est impair $d = d' = \delta d_3$ et $\alpha+2 = 2(\beta+1)$; l'équation devient :

$$(2^{\beta+1}a_1)^2\delta - 1 = d_3 y^2 \ .$$

Si d est pair $d = 2d' = 2\delta d_3$, $\alpha+2 = 2(\beta+1)+1$; l'équation devient :

$$(2^{\beta+1}a_1)^2 2\delta - 1 = d_3 y^2 \ .$$

Ainsi dans chaque cas, si $d = d_o d_3$ et $x = 2^{\beta+1}a_1$ (qui est pair) on a

$$d_o x^2 - d_3 y^2 = 1 \qquad d_o d_3 = d \ , \ d_3 \equiv 3 \pmod 4 \ .$$

Comme $a = 2^{\alpha+1}a' = 2^{\alpha+1}a_1^2\delta$ on en déduit

si $d = 2d'$ (d'où $\alpha+1 = 2(\beta+1)$) $\quad a = \dfrac{(2^{\beta+1}a_1)^2\, 2\delta}{2} = \dfrac{x^2}{2} d_o$

si $d = d'$ (d'où $\alpha+1 = 2\beta+1$) $\quad a = \dfrac{(2^{\beta+1}a_1)^2\delta}{2} = \dfrac{x^2}{2} d_o$

Et $b = 2^\beta b' = 2^\beta a_1 y = \dfrac{(2^{\beta+1}a_1)y}{2} = \dfrac{xy}{2}$. D'où la condition nécessaire de la

Proposition 1. Soit A l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$, $d > 0$. Un élément non nul z appartient à $A(4)$ si et seulement si

$$z = \frac{x^2}{2} d_o + \frac{xy}{2}\sqrt{d}$$

où $d_o d_3 = d$, $d_3 \equiv 3 \pmod 4$ et $d_o x^2 - d_3 y^2 = 1$ avec x pair.

Démonstration de la réciproque. Soit z vérifiant les hypothèses. Alors $1-4z = 1-2d_o x^2 + 2xy\sqrt{d}$ d'où

$$N(1-4z) = (1-2d_o x^2)^2 - 4dx^2y^2 = 1-4(d_o x^2 - d_o x^2(d_o x^2 - d_3 y^2)) = 1$$

donc $1-4z \in U(A)$ d'où $z \in A(4)$, c.q.f.d.

D'après le lemme 1, $A(4) \subset \mathbb{Z}[\sqrt{d}]$ donc $1-4z = \pm \varepsilon^n$ pour tout $z \in A(4)$ où ε est l'unité fondamentale de $\mathbb{Z}[\sqrt{d}]$ (c'est le cube de celle de A si celle de A n'appartient pas à $\mathbb{Z}[\sqrt{d}]$).

Lemme 2. Soit $0 \neq z = \dfrac{x^2}{2} d_o + \dfrac{xy}{2}\sqrt{d} \in A(4)$. On a $\alpha(z) = \overline{\pm\varepsilon}$ si et seulement si $d_o \neq 1$ et $d_o \neq -d$.

Preuve. $1-4z = 1-2(d_o x^2 + xy\sqrt{d}) = 1-(d_o x^2 - d_3 y^2) - d_o x^2 - d_3 y^2 - 2xy\sqrt{d}$ d'où

$$1-4z = -(d_o x^2 + d_3 y^2 + 2xy\sqrt{d}) \quad .$$

Si $d_o > 0$ (donc d_3 aussi) alors $1-4z = -(x\sqrt{d_o} + y\sqrt{d_3})^2$ et si $d < 0$ $1-4z = (x\sqrt{|d_o|} + y\sqrt{|d_3|})^2$. Donc, comme $\alpha(z) = \overline{\pm \varepsilon}$ est équivalent à $\alpha(z) \neq \overline{\pm 1}$, on doit avoir $x\sqrt{d_o} + y\sqrt{d_3} \notin \mathbb{Z}[\sqrt{d}]$ et $x\sqrt{|d_o|} + y\sqrt{|d_3|} \notin \mathbb{Z}[\sqrt{d}]$ c'est-à-dire, puisque $d_3 \equiv 3 \pmod 4$, $d_o \neq 1$ et $d_o \neq -d$. La réciproque est évidente.

Lemme 3. Soit $\varepsilon = \eta + \zeta\sqrt{d}$ l'unité fondamentale de $\mathbb{Z}[\sqrt{d}]$. On a $\overline{-1} \in \mathrm{Im}(\alpha)$ si et seulement si $d \equiv 3 \pmod 4$ et ζ est impair.

Preuve. D'après la démontration précédente, si $\alpha(z) = \overline{-1}$ alors $d_o = 1$. Donc $d = d_o d_3 = d_3 \equiv 3 \pmod 4$ et comme $z \in A(4)$ l'équation $x^2 - dy^2 = 1$ a une solution avec x pair. Comme $d \equiv 3$, $N(\varepsilon) = \eta^2 - \zeta^2 d = +1$ et $\eta\zeta$ est pair. Le développement de $x + y\sqrt{d} = (\eta + \zeta\sqrt{d})^n$ donne alors

$$x \equiv \eta^n + \zeta^n d^{n/2} \equiv 1 \pmod 2 \qquad \text{si } n \text{ est pair}$$

$$x \equiv \eta^n \equiv \eta \pmod 2 \qquad \text{si } n \text{ est impair.}$$

Donc x pair exige η pair donc ζ impair. Réciproquement si $d \equiv 3 \pmod 4$ et ζ impair, l'équation $x^2 - dy^2 = 1$ a une solution avec $x = \eta$ pair. Ainsi $z = \frac{\eta^2}{2} + \frac{\eta\zeta}{2}\sqrt{d} \in A(4)$ et $\alpha(z) = \overline{-1}$.

Lemme 4. Si $N(\varepsilon) = -1$ alors $G(A) = \{0\}$.

Preuve. Comme $N(\varepsilon) = -1$ implique $d \not\equiv 3 \pmod 4$, du lemme 3 on déduit $G(A) \subset \mathbb{Z}/2\,\mathbb{Z}$. Si $0 \neq z \in G(A)$, comme $1-4z = \pm \varepsilon^n$, d'après le lemme 1 on obtient $1 = N(1-4z) = N(\pm \varepsilon^n) = N(\varepsilon^n) = (N(\varepsilon))^n = (-1)^n$ ainsi $n = 2m$ donc $\alpha(z) = \overline{1}$ ou $\overline{-1}$ mais ce dernier cas est impossible car $d \not\equiv 3$.

Théorème 1. Soit A l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$, $d > 0$.

Si $d \equiv 3 \pmod 4$ alors $G(A) \simeq \mathbb{Z}/2\,\mathbb{Z}$

Si $d \not\equiv 3 \pmod 4$ alors $G(A) \simeq \{0\}$ ou $\mathbb{Z}/2\,\mathbb{Z}$

et dans ce cas $G(A)$ n'est pas nul si et seulement si les propositions suivantes, qui sont équivalentes, sont vérifiées :

(a) il existe une décomposition de d en $d_o d_3$ avec $d_o \neq 1$, $d_o \neq -d$, $d_3 \equiv 3 \pmod 4$ telle que l'équation $d_o x^2 - d_3 y^2 = 1$ ait une solution ;

(b) l'unité fondamentale $\varepsilon = \eta + \zeta\sqrt{d}$ de $\mathbb{Z}[\sqrt{d}]$ vérifie $\zeta \equiv 0 \pmod 4$.

Démonstration. 1) Cas où $d \not\equiv 3 \pmod 4$. Si $G(A) \neq \{0\}$, d'après le lemme 3 et le lemme 2 la condition (a) est vérifiée avec x pair ; mais s'il y a une solution comme $d_3 \equiv 3 \pmod 4$ et $d_0 \not\equiv 1 \pmod 4$, obligatoirement x est pair. D'où (a).

Réciproquement si (a) est vérifiée x est pair d'où

$z = \frac{x^2}{2} d_0 + \frac{xy}{2}\sqrt{d} \in A(4)$ et $\alpha(z) = \overline{\pm\varepsilon}$ donc $G(A)$ n'est pas nul.

(a) $\Rightarrow$ (b) Si (a) est vérifiée il existe $0 \neq z \in G(A)$ tel que

$$1-4z = -(d_0x^2 + d_3y^2 + 2xy\sqrt{d}) = -\varepsilon = -(\eta + \zeta\sqrt{d}) \quad \text{si } d_0 \text{ est positif}$$

et $$1-4z = +(|d_0|x^2 + |d_3|y^2 + 2xy\sqrt{d}) = \varepsilon = \eta + \zeta\sqrt{d} \quad \text{si } d_0 \text{ est négatif}$$

donc, comme x est pair, $\zeta = \pm\, 2xy \equiv 0 \pmod 4$.

(b) $\Rightarrow$ (a) Si $\zeta \equiv 0 \pmod 4$ alors $N(\varepsilon) = \eta^2 - \zeta^2 d \equiv \eta^2 \pmod{16}$ donc $N(\varepsilon) = 1$ d'où $\eta = \pm 1 \pmod 8$. Ainsi une valeur $z = \frac{1 \mp (\eta + \zeta\sqrt{d})}{4}$ appartient à $\mathbb{Z}[\sqrt{d}]$. Et comme $1-4z = \pm\varepsilon$, $\alpha(z) \neq \overline{1}$ donc $G(A)$ n'est pas nul et (a) est vérifiée.

2) Cas où $d \equiv 3 \pmod 4$ (donc $d_0 \equiv 1 \pmod 4$). Si (a) est vérifiée avec x impair l'équation $-d_3x^2 - (-d_0)y^2 = 1$ (où $-d_0 \equiv 3$) a une solution avec x pair (la valeur y de $d_0x^2 - d_3y^2 = 1$). Ici encore (a) et (b) sont équivalents. Ainsi, d'après la condition (b) ($\zeta \equiv 0 \pmod 4$) et le lemme 3 ($\zeta \equiv 1$ ou $3 \pmod 4$) $\overline{1}$ et $\overline{\pm\varepsilon}$ ne peuvent, compte tenu du lemme 2, appartenir simultanément à $\mathrm{Im}(\alpha)$. Donc dans ces trois cas $G(A) \simeq \mathbb{Z}/2\,\mathbb{Z}$. Comme le cas $\zeta \equiv 2 \pmod 4$ est exclu (car $\eta^2 - \zeta^2 d = 1$ impliquerait $4d \equiv 0 \pmod 8$) le théorème est démontré.

Corollaire. Si $N(\varepsilon) = -1$, alors $G(A)$ est nul et, si d est impair, la réciproque est vraie.

Preuve. La condition est nécessaire (c'est le lemme 4). Réciproquement si $G(A) = \{0\}$ alors $d \not\equiv 3 \pmod 4$ donc $d \equiv 1 \pmod 4$ et d'après le théorème 1 on a $\zeta \not\equiv 0 \pmod 4$. Si ζ est impair, η est pair donc $N(\varepsilon) = \eta^2 - \zeta^2 d \equiv -1 \pmod 4$ donc $N(\varepsilon) = -1$. Si $\zeta \equiv 2 \pmod 4$, $N(\varepsilon) \equiv 1-4d \pmod 8$. Si $N(\varepsilon) = 1$ alors $4d \equiv 0 \pmod 8$ impossible car d impair et si $N(\varepsilon) = -1$ alors $2 \equiv 4d \pmod 8$ impossible. Ce cas est donc exclu.

Comme $N(5 + 2\sqrt{6}) = +1$, la réciproque est fausse pour d pair.

Remarque 1. Le théorème 1 démontre la conjecture de Small pour $d \equiv 3 \pmod 4$. Il infirme celle pour $d \equiv 2 \pmod 4$ car $G(\mathbb{Z}[\sqrt{d}]) \simeq \mathbb{Z}/2\,\mathbb{Z}$ pour $d = 14, 46, 62, 94$ et 138 car les cinq expressions suivantes, qui fournissent explicitement des valeurs de z telles que $\alpha(z) = \overline{-\varepsilon}$, valent 1 :

$$2.2^2 - 7.1^2 = 2.78^2 - 23.23^2 = 2.4^2 - 31.1^2 = 2.732^2 - 47.151^2 =$$
$$= 6.2^2 - 23.1^2 = 1 \ .$$

Remarque 2. La comparaison du théorème 1 avec le théorème 1 de [5] montre que le cardinal de $G(A)$ est plus petit ou égal à celui de $Q_{fs}(A)$ groupe des extensions quadratiques séparables libres de A. En est-il ainsi pour tout anneau A ?

Notons (A,a,b) l'extension quadratique séparable libre $B = A \oplus Ax$ où $x^2 = ax + b$ et $a^2 + 4b \in U(A)$ et $[A,a,b]$ sa classe d'isomorphisme. Comme d'après [4] la loi sur $Q_{fs}(A)$ est

$$[A,a,b]\,[A,c,d] = [A,ac,a^2d + c^2b + 4bd]$$

les éléments $[A,1,b]$ forment un sous-groupe de $Q_{fs}(A)$.

Théorème 2. Soient A un anneau commutatif unitaire quelconque et $Q_{fs}(A)$ le groupe des classes d'isomorphisme des extensions quadratiques séparables libres de A. Le groupe $G(A)$ est isomorphe au sous-groupe formé des éléments $[A,1,-z]$ de $Q_{fs}(A)$.

Démonstration. Soient $z \in A(4)$ et $\overline{z} \in G(A)$. Si $\overline{z} = \overline{z'}$, d'après [2], $z' = z - (x^2 - x)(1-4z)$ donc $1-4z' = (1-4z)(1-2x)^2$. Comme z et z' appartiennent à $A(4)$, $u = 1-2x \in U(A)$ et donc $v = \frac{-x}{1-2x} \in A$. Ainsi

$$-z' = -z + (x^2-x)(1-4z) = u^2(v-z-v^2) \qquad \text{et} \quad u(1-2v) = 1$$

donc, d'après le lemme 1 de [4], on a $(A,1,-z) \sim (A,1,-z')$. L'homomorphisme

$$g : G(A) \to Q_{fs}(A)$$
$$\overline{z} \mapsto [A,1,-z]$$

est donc bien défini. Considéré comme application à valeurs dans le sous-groupe des éléments $[A,1,b]$ il est surjectif. L'élément neutre de $Q_{fs}(A)$ étant $[A,1,0]$ si $g(\overline{z}) = [A,1,-z] = [A,1,0]$ d'après le lemme 1 de [4] il existe $u \in U(A)$ et $v \in A$ tels que $1 = u(1-2v)$ et $0 = u^2(v.1-z-v^2)$, donc $z = v-v^2 = 0-(v^2-v)(1-4.0)$ donc $z \sim 0 \in A(4)$ donc $\overline{z} = \overline{0}$ et g est injective.

Elle peut ne pas être surjective : la comparaison entre le théorème 1 et le théorème 1 de [5] montre en effet que pour les trois cas $d \equiv 1$, 2 ou 3 (mod. 4) les plus petites valeurs de d telle que $G(A)$ soit un sous-groupe strict de $Q_{fs}(A)$ sont respectivement $d = 5$, 6 et 39 (les unités fondamentales étant $\frac{1+\sqrt{5}}{2}$, $5+2\sqrt{6}$ et $25+4\sqrt{39}$). Dans le cas où $d \equiv 1$ (mod. 4), si $\varepsilon \in \mathbb{Z}[\sqrt{d}]$ alors $G(A) \sim Q_{fs}(A)$ (car ζ pair implique $\zeta \equiv 0$ (mod. 4)) et si $\varepsilon \notin \mathbb{Z}[\sqrt{d}]$, $G(A) \sim Q_{fs}(A)$ si et seulement si $N(\varepsilon) = 1$ (car, $\eta+\zeta\sqrt{d}$ désignant ε^3, $N(\varepsilon) = 1$ implique $\zeta \equiv 0$ (mod. 4) et $N(\varepsilon) = -1$ implique ζ impair).

Comme $Q_{fs}(A)$ est un sous-groupe de $Q(A)$ (cf. [3], théorème 2), on déduit du théorème 2 le corollaire suivant :

Théorème 3. Soit A un anneau commutatif unitaire. Le groupe $G(A)$ est un sous-groupe du groupe $Q(A)$ des extensions quadratiques de A.

BIBLIOGRAPHIE

[1] A. MICALI et P. REVOY - Algèbres de Clifford séparables, Secrétariat des Mathématiques, Université de Montpellier, 1969 ; M.R.46,198 b(1973).

[2] A. MICALI et O. VILLAMAYOR - Sur les algèbres de Clifford, Ann. Sc. Ecole Norm. Sup. 4è. I (1968), 271-304.

[3] C. SMALL - The group of quadratic extensions. J. of Pure and Applied Algebra 2 (1972) 83-105.

[4] K. KITAMURA - On the free quadratic extension of a commutative ring. Osaka J. Math. 10 (1973), 15-20.

[5] J.-D. THEROND - Le groupe des extensions quadratiques séparables libres de l'anneau des entiers de $Q(\sqrt{d})$, C.R.Acad. Sc. Paris. Série A, 281 (1975), 939-942.

Institut de Mathématiques
Université des Sciences et
Techniques du Languedoc

34060 MONTPELLIER CEDEX

FRANCE