Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 20 (1974)
Heft: 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: SOMMES DE CARRÉS D'ENTIERS D'UN CORPS
Autor: Moser, Claude
Kapitel: 4. RÉSULTATS PROPRES AU CAS p = 2 ET e IMPAIR
DOI: https://doi.org/10.5169/seals-46913

Ceci montre l'existence d'un isomorphisme entre le groupe V/U_{2d+1} et le groupe U^2/U^2_{d+1}. La proposition sera alors une conséquence du lemme de Herbrand:

Lemme de Herbrand. Soit $\varphi : G \to G'$ un homomorphisme de groupes et soit H un sous-groupe de G.

1. *Les deux assertions suivantes sont équivalentes :*

a) *le sous-groupe H est d'indice fini dans G ;*

b) *les indices $(\varphi(G) : \varphi(H))$ et $(\mathrm{Ker}\,\varphi = H \cap \mathrm{Ker}\,\varphi)$ sont finis.*

2. *Si les assertions ci-dessus sont vraies, alors :*

$$(G:H) = (\varphi(G) : \varphi(H)) \,.\, (\mathrm{Ker}\,\varphi : H \cap \mathrm{Ker}\,\varphi) \,.$$

Pour une démonstration, voir [4] § 63.

Appliquons ce lemme au groupe U, à son sous-groupe U_{d+1} et à l'homomorphisme $\varphi : U \to U^2$ $(x \mapsto x^2)$; puisque -1 appartient à U_{d+1}, on a l'égalité

$$(U : U_{d+1}) = (U^2 : U^2_{d+1})$$

et les égalités:

$$(U : U_{2d+1}) = (U : U_{d+1})\,(U_{d+1} : U_{2d+1}) = (U : V)\,(V : U_{2d+1}) \,.$$

On en conclut:

$$(U : V) = (U_{d+1} : U_{2d+1}) = 2^{df} \,.$$

4. Résultats propres au cas $p = 2$ et e impair

4.1. *Théorème*

Supposons e impair et soit $u \in U$. Alors :

1. *Si $\delta(u) > e$, u est somme de deux carrés dans A ;*

2. *Si $\delta(u) = e$, il existe $a, b \in U$ tels que $u = a^2 + 2b$; avec ces notations, les trois assertions suivantes sont équivalentes :*

a) *l'unité u est somme de deux carrés dans A $(u \in V_2)$;*

b) *la trace absolue de (b/a^2) appartient à $2\mathbf{Z}_2$;*

c) *il existe $c \in U$ tel que $b = a^2(c^2 - c)$.*

De plus :

3. *Si f est pair on a $s(A) = 2$, $V = V_3$ et $t(A) = 3$;*

4. *Si f est impair on a $s(A) = 4$, $V = V_4$ et $t(A) = 4$; pour que u appartienne à V_4 mais non à V_3, il faut et il suffit que $-u$ soit un carré dans A.*

La première assertion est une répétition de la seconde assertion de la proposition (3.1.). Avant d'examiner les assertions suivantes faisons quelques remarques. Tout d'abord -1 n'est pas un carré dans K puisqu'on a $\delta(-1) = e$ en vertu de la dernière assertion de la proposition (1.3.2.).

Ensuite remarquons que si v est une unité de $\mathbf{Q}_2(i)$ ($i^2 = -1$), alors $N_{\mathbf{Q}_2(i)/\mathbf{Q}_2}(v) \in 1 + 4\mathbf{Z}_2$. En effet, une base d'entiers de $\mathbf{Q}_2(i)$ est $\{1, i\}$ et si $v = \alpha + i\beta$, alors $N_{\mathbf{Q}_2(i)/\mathbf{Q}_2}(v) = \alpha^2 + \beta^2$, l'un et l'un seulement des nombres α, β étant une unité de $\mathbf{Z}_2$.

Signalons que relativement à l'extension résiduelle $\overline{K}/\mathbf{F}_2$ la trace $tr : \overline{K} \to \mathbf{F}_2$ est un homomorphisme surjectif de groupes additifs dont le noyau est $\{u \mid \exists y \in \overline{K},\ u = y^2 - y\}$ (cf. [2] page 8, prop. 9). Ceci étant dit, soit u une unité de A dont le défaut quadratique est e. Si on a $u = a^2 + 2b$ et si u est somme de deux carrés d'entiers, alors la norme de u est, dans l'extension $K/\mathbf{Q}_2$, la norme d'une unité de $\mathbf{Q}_2(i)$.

On a alors:

$$N_{K/\mathbf{Q}_2}(u) = [N_{K/\mathbf{Q}_2}(a)]^2\,[1 + 2\,Tr_{K/\mathbf{Q}_2}(b/a^2) + 4h] \quad (h \in {}_2\mathbf{Z}).$$

Puisque a est une unité de A, on a $[N_{K/\mathbf{Q}_2}(a)]^2 \in 1 + 8\mathbf{Z}_2$. La deuxième remarque faite ci-dessus permet alors de conclure que $Tr_{K/\mathbf{Q}_2}(b/a^2) \in \mathbf{Z}2_2$.

Maintenant, si l'unité $u = a^2 + 2b$, ($b \in U$), satisfait à $Tr_{K/\mathbf{Q}_2}(b/a^2) \in 2\mathbf{Z}_2$, il existe $c_0 \in \overline{K}$ tel que la classe de (b/a^2) modulo $\mathfrak{P}$ soit $c_0^2 - c_0$. L'application du lemme de Hensel au polynôme $X^2 - X - (b/a^2)$ permet de conclure à l'existence d'une unité c de A telle que $b = a^2(c^2 - c)$.

Enfin, s'il existe $c \in U$ avec $b = a^2(c^2 - c)$ on peut écrire $u = a^2 + 2b$ sous la forme $u = a^2[c^2 + (c-1)^2]$ et $u \in V_2$.

3. Si f est pair, on remarque que K contient une racine primitive cubique j de l'unité. On a $-1 = j^4 + j^2$ et $s(A) = 2$. Si $u \in U$ satisfait à $\delta(u) \geqslant e$ on peut écrire $u = a^2 + 2b$ ($a \in U$, $b \in A$) et $u = (a + b/a)^2 - (b/a)^2 \in V_3$. L'assertion sur $t(A)$ sera démontrée plus loin (cf. Proposition 4.2, remarque).

4. Remarquons que $Tr_{K/\mathbf{Q}_2}(-1) = -ef \notin 2\mathbf{Z}_2$. Par conséquent -1 n'est pas somme de deux carrés dans A, ni même de trois (vérification facile). Donc la forme quadratique $X_1^2 + X_2^2 + X_3^2 + X_4^2$ n'est pas isotrope sur K. On a bien $-1 = 1 + 1 + 4 - 7 \in V_4$, donc $-U^2 \subset V_4/V_3$.

Maintenant soit $u \in V$ tel que u n'appartienne ni à U^2 ni à $-U^2$. Pour toute $v \notin \dot{K}^2$ soit $G(v)$ le sous-groupe de $\dot{K}$ formé par les normes dans l'extension $K(\sqrt{v})/K$. D'après la proposition (1.2.) les groupes $G(u)$ et $G(-1)$ sont d'indice 2 dans $\dot{K}$. Il existe donc $x \in G(u)/G(-1)$; puisque $-1 \notin G(-1)$, il existe $y, v, w, t \in K$ non tous nuls tels que $y^2 - uv^2 = -(w^2+t^2)$. On a $v \neq 0$ et on déduit de là que u est somme de trois carrés dans K. Reste à montrer que u appartient à V_3.

Dans un premier temps remarquons que si u appartient à V/V_2, alors $-u$ appartient à V_2. En effet, quitte à multiplier u par le carré d'une unité on peut supposer que $u = 1 + 2b$ avec $b \in A$ et $Tr_{K/\mathbf{Q}_2}(b) \in 1 + 2\mathbf{Z}_2$; on a alors $-u = 1 - 2(b+1)$ et $Tr_{K/\mathbf{Q}_2}(-(b+1)) = -ef + Tr_{K/\mathbf{Q}_2}(-b) \in 2\mathbf{Z}_2$. Dans un second temps on peut écrire u sous les deux formes

$$u = \pi^{-2n}(a_1^2+a_2^2+a_3^2) = -(b_1^2+b_2^2)$$

avec $a_1, a_2, a_3, b_1, b_2 \in A$. Si on suppose l'entier n minimum on peut supposer que a_1 est une unité. Si a_2 et a_3 appartiennent à $\mathfrak{P}$ alors $n = 0$ et on a $u \in V_3$. Supposons donc que a_1 et a_2 sont des unités. De l'égalité ci-dessus on déduit la suivante:

$$(a_1 + b_1\pi^n + b_2\pi^n)^2 + a_3^2 + a_2^2 - 2\pi^n(a_1b_1 + a_1b_2 - b_1b_2\pi^n) = 0;$$

si on avait $n \geqslant 1$, l'entier $a_2^2 - 2\pi^n(a_1b_1 + a_1b_2 - b_1b_2\pi^n)$ serait somme de deux carrés d'entiers et la forme $X_1^2 + X_2^2 + X_3^2 + X_4^2$ serait isotrope sur K. Contradiction. On a donc $n = 0$ et $u \in V_3$.

De tout ceci on déduit évidemment: $V = V_4$ et $V_4/V_3 = -U^2$.

4.2. *Proposition*

Soit u une unité de A. On a les résultats suivants :

1. *Le plus petit entier pair $2k$ tel que $u\pi^{2k}$ appartienne à A_2 est* $\max[0, e-\delta(u)]$ *; pour tout entier pair $2l \geqslant \max[0, e-\delta(u)]$, $u\pi^{2l}$ est somme de n carrés dans A si et seulement si u est somme de n carrés dans K ;*

2. *Le plus petit entier impair $2k+1$ tel que $u\pi^{2k+1}$ appartienne à A_2 est e ; pour tout entier impair $2l+1 \geqslant e$, $u\pi^{2l+1}$ est somme de deux ou de trois carrés dans A selon que $u\pi$ est ou n'est pas somme de deux carrés dans K.*

1. Si $\delta(u) \geqslant e$ on a $u \in V$ d'après le théorème (4.1.). Si $\delta(u) < e$ on a $u\pi^{e-\delta(u)} = a^2\pi^{e-\delta(u)} + \pi^e v$ avec $a, v \in U$ et l'assertion initiale résulte de l'assertion 1) de la proposition (3.1.).

a) Le cas f pair : si f est pair, tout élément de A est somme de trois carrés dans K puisque $s(A) = 2$. Si $\delta(u) > e$, on a $u \in V_2$ et il n'y a rien à démontrer. Si $\delta(u) = e$, il suffit de montrer que si u est somme de deux carrés dans K, alors u appartient à V_2. Si u est somme de deux carrés dans K, il existe $v \in \mathbf{N}$, $a, v, x \in U$, $y \in A$ tels que : $u\pi^{2v} = a^2\pi^{2v} + 2v\pi^{2v} = x^2 + y^2$; si on avait $v > 0$, y serait une unité et on aurait :

$$-1 = x^{-2}\{(y + ay^{-1}\pi^v)^2 - 2a\pi^v - 2a^2\pi^{2v} - 2\pi^v v\}$$

ce qui impliquerait $\delta(-1) > e$. Contradiction puisque $\delta(-1) = e$ d'après la dernière assertion de la proposition (1.3.2.). On a donc $v = 0$ et $u \in V_2$. Enfin, dans le cas où $\delta(u) < e$, on peut écrire de manière analogue

$$u = a^2 + v\pi^{\delta(u)} \quad \text{avec} \quad a, v \in U ;$$

si u est somme de deux carrés dans K, soit v le plus petit entier tel que $u\pi^{2v}$ soit somme de deux carrés dans A. Il existe $x, y \in U$ tels que $u\pi^{2v} = x^2 + y^2$, et on obtient :

$$-1 = x^{-2}\{-y + a\pi^v)^2 - v\pi^{2v+\delta(u)} - 2\pi^v(ay - a^2\pi^v\} ;$$

puisque $\delta(-1) = e$, on a bien $2v + \delta(u) = e$.

b) Le cas f impair : la proposition est vraie pour $n = 1$. En ce qui concerne le cas $n = 2$, elle se démontre comme dans a). Si u appartient à $V_3 \backslash V_2$, il n'y a rien à démontrer. Si $u \in U \backslash V$ est somme de trois carrés dans K, soit $2v$ le plus petit entier pair tel que $u\pi^{2v}$ soit somme de trois carrés dans A. Il existe $x \in U$, $y, z \in A$ tels que $u\pi^{2v} = x^2 + y^2 + z^2$ et on a :

$$-1 = x^{-2}\{(y + z + a\pi^v)^2 - v\pi^{2v+\delta(u)} - 2yz - 2a\pi^v(y + z + a\pi^v)\} .$$

Si $yz \in \mathfrak{P}$, on a immédiatement $2v + \delta(u) = e$ puisque $v > 0$.
Si $yz \in U$, on a nécessairement $2v + \delta(u) \geqslant e$ et on peut écrire :

$$-1 = x^{-2}\{(y + a\pi^v)^2 + z^2 - v\pi^{2v+\delta(u)} - 2a^2\pi^{2v} - 2ay\pi^v\} .$$

Si on avait $\delta(u) + 2v > e$, on aurait $z^2 - v\pi^{2v+\delta(u)} - 2a^2\pi^{2v} - 2ay\pi^v \in V_2$ et -1 serait somme de trois carrés dans A. Contradiction.

Enfin, si u n'est pas somme de trois carrés dans K, on a $u \in -U^2$ et u est somme de quatre carrés et pas moins dans A.

2. La première assertion résulte de la proposition (3.1.). De plus $u\pi$ est somme de trois carrés dans K quelle que soit la parité de f, car $-u\pi$ n'est pas un carré.

Si f est pair, il existe $v \in U$ tel que $u\pi^e = 2v$, et on a $u\pi^e = (v+1)^2 - (1+v^2)$, somme de trois carrés dans A. De plus si $u\pi$ est somme de deux carrés dans K et si $2l+1$ est le plus petit entier impair tel que $u\pi^{2l+1}$ soit somme de deux carrés dans A, il existe deux unités a, b de A telles que $a^2 + b^2 = u\pi^{2l+1}$. On a alors $-1 = a^{-2}\{b^2 + u\pi^{2l+1}\}$ et on conclut que $2l+1 = e$.

Si f est impair, soit $2l+1$ le plus petit entier impair tel que $u\pi^{2l+1}$ soit somme de trois carrés dans A. Il existe $x \in A$, $y, z \in U$ tels que $u\pi^{2l+1} = x^2 + y^2 + z^2$, ce qui donne

$$-1 = y^{-2}\{z^2 - u\pi^{2l+1} + x^2\};$$

puisque $s(A) = 4$, on a $2l+1 \leqslant e$ d'après le théorème (4.1.). Par ailleurs on a $2l+1 \geqslant e$ d'après la proposition (3.1.). Donc $2l+1 = e$. Enfin, si $u\pi$ est somme de deux carrés dans K, on raisonne comme dans le cas f pair.

Remarque: Il est clair d'après ce qui précède que $t(A) = 4$ si f est impair. Par ailleurs, si f est pair on a $V_3 \neq V_2$, ce qui montre que $t(A) = 3$. En effet, l'application trace de $\overline{K}$ dans $\mathbf{F}_2$ est surjective: il existe $u \in U$ tel que la trace de la classe de u soit 1 dans $\mathbf{F}_2$. Alors $1 + 2u \in V_3/V_2$.

4.3. *Exemple numérique*

1. Prenons d'abord l'exemple du corps $K = \mathbf{Q}_2(\sqrt[3]{6})$. C'est une extension totalement ramifiée de degré 3 de $\mathbf{Q}_2$ dont une uniformisante π est précisément $\sqrt[3]{6}$. Remarquons qu'on a les égalités:

$$(U : V) = 2 \quad et \quad (V : V_2) = 2 = (V_2 : U^2).$$

Un système de représentants de U modulo V est $\{+1, 1+\sqrt[3]{6}\}$.
Un système de représentants de V modulo V_2 est $\{1, -1\}$.
Un système de représentants de V_2 modulo U^2 est $\{1, 1+2\sqrt[3]{6}\}$.

On a évidemment $1 + 2\sqrt[3]{6} = 1 + (\sqrt[3]{6})^4 - 4\sqrt[3]{6}$. Considérons maintenant l'unité $1 + \sqrt[3]{6}$. Cette unité a pour défaut quadratique 1, de même que son opposé. On en déduit que le plus petit entier pair tel que $\pi^{2k}(1+\pi)$ soit somme de carrés dans A est $2k = 2$. De plus $\pi^{2k}(1+\pi)$ et $-\pi^{2k}(1+\pi)$ sont tels que l'un est somme de deux carrés dans A et pas moins et l'autre somme de trois carrés et pas moins. Effectivement on a les égalités:

$$-\pi^2(1+\pi) = -\pi^2 - 6 = 9\pi^2 - 7 + 1 - 10\pi^2.$$

Dans $\mathbf{Z}_2$, l'une des racines carrées de -7 est de la forme $1 + 4a$ et on a:

$$\begin{aligned} -\pi^2(1+\pi) &= (1+4a-3\pi)^2 - 6\pi - 12a\pi + 1 - 10\pi^2 \\ &= (1+4a-3\pi)^2 + (\pi^4+1-2\pi^2) - 12\pi - 12a\pi - 8\pi^2 \\ -\pi^2(1+\pi) &= (1+4a-3\pi)^2 + (1-\pi^2)^2 - 12\pi - 12a\pi - 8\pi^2 . \end{aligned}$$

Ceci permet d'affirmer que $-\pi^2(1+\pi)$ est somme de deux carrés dans A et que $\pi^2(1+\pi)$ est somme de trois carrés et pas moins. Une représentation s'obtient par exemple à partir de l'égalité.

$$\pi^2(1+\pi) = \pi^2 + 6 = (\pi+2)^2 + 2(1-4\pi) .$$

Ceci étant, le plus petit entier impair tel que $(1+\pi)\,\pi^{2k+1}$ appartienne à A_2 est $e = 3$. Mais $\pi^3(1+\pi) = 6(1+\pi) = (-6)\big(-(1+\pi)\big)$. Or dans $\mathbf{Z}_2$, $-6 = 1 - 7$ est somme de deux carrés et on vient de voir que $-(1+\pi)$ est somme de deux carrés dans K. Par conséquent $6(1+\pi)$ est somme de deux carrés dans A. De façon « semi-explicite » on peut écrire $-(1+\pi) = c^2 + d^2$ avec πc et πd dans A tels que $\pi c \equiv \pi d \equiv 1 \bmod \mathfrak{P}$. On a alors:

$$6(1+\pi) = [1+(1+4a)^2] \cdot [c^2+d^2] = (c+d+4ad)^2 + (c-d-4ad)^2$$

et chacun des termes figurant entre parenthèses est un entier de K.

2. Pour obtenir un exemple où f est pair, considérons maintenant le corps $K = \mathbf{Q}_2(\sqrt[3]{6}, j)$ où j est une racine cubique de l'unité. Une uniformisante est encore $\sqrt[3]{6}$. Mais dans ce corps $1 + \sqrt[3]{6}$ est somme de deux carrés. Une unité qui est somme de trois carrés et pas moins est par exemple $1 + 2(j+\sqrt[3]{6})$ puisqu'on a

$$Tr_{K/\mathbf{Q}_2}(j+\sqrt[3]{6}) = 3\, Tr_{\mathbf{Q}_2(j)/\mathbf{Q}_2}(j) = -3 .$$

On a d'ailleurs:

$$\begin{aligned} 1 + 2(j+\sqrt[3]{6}) &= (j^2-\sqrt[3]{6})^2 + j^2(j+\sqrt[3]{6})^2 + j^4(j+\sqrt[3]{6})^2 \\ &= (j^2-\sqrt[3]{6})^2 + (j^2+j\sqrt[3]{6})^2 + (1+j^2\sqrt[3]{6})^2 . \end{aligned}$$

Remarquons enfin qu'on a $(U : V) = 4$ dans ce cas et qu'un système de représentants de U modulo V est par exemple:

$$\{1, 1+\sqrt[3]{6}, 1+j\sqrt[3]{6}, 1+j^2\sqrt[3]{6}\} .$$