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: 5. RÉSULTATS PROPRES AU CAS p = 2 ET e PAIR
DOI: https://doi.org/10.5169/seals-46913

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 12.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

5. Résultats propres au cas $p = 2$ et e pair

5.1. *Théorème*

Si e est pair, toute unité de A_2 est somme de deux carrés dans A, c'est-à-dire qu'on a $V = V_2$. De plus on a $t(A) = 3$.

La première assertion de ce théorème résulte de la proposition (3.1.) puisque $\delta(u) \geqslant e$ équivaut à $\delta(u) \geqslant e+1$. Soit $u \in U$, et soit $n \in \mathbf{N}$ tel que $x = u\pi^n$ appartienne à A_2. Si $n \geqslant e$, $1-x$ est somme de deux carrés dans A. On a $s(A) = 2$, donc x est somme de trois carrés dans A. Si $n < e$, alors n est pair (cf. proposition 3.1.): si on pose $n = 2m$ et $u = a^2 + b\pi^{\delta(u)}$ avec $a, b \in U$ on obtient: $x = (a\pi^m)^2 + b\pi^{\delta(u)+2m}$; ce résultat implique $\delta(u) + 2m \geqslant e+1$. Pour tout $z \in U$, on a:

$$x = (z + a\pi^m)^2 - (z^2 - b\pi^{2m+\delta(u)} + 2az\pi^m).$$

On en conclut que $z^2 - b\pi^{2m+\delta(u)} + 2az\pi^m$ est somme de deux carrés d'entiers, donc que x est somme de trois carrés dans A. On a ainsi montré que $t(A) \leqslant 3$. L'égalité $t(A) = 3$ résultera des propositions qui suivent et qui concernent respectivement les cas $\delta(-1) = 2e$, (5.2.), $\delta(-1) < 2e$, (5.3.) et $\delta(-1) > 2e$, (5.4.).

5.2. *Proposition*

On suppose e pair et $\delta(-1) = 2e$. Alors:

1. *Pour qu'un entier soit somme de deux carrés dans A, il faut que sa valuation soit paire;*

2. *Soit $u \in U$ tel que $\delta(u) < e$ $(u \notin V)$; le plus petit entier pair $2k$ tel que $u\pi^{2k}$ appartienne à A_2 est $e+1-\delta(u)$; le plus petit entier pair $2l$ tel que $u\pi^{2l}$ soit somme de deux carrés dans A est $2(e-\delta(u))$.*

L'assertion 1. résulte du fait que l'extension $K(i)/K(i^2=-1)$ est non ramifiée et de la proposition (1.2.): un élément de $\dot{K}$ est somme de deux carrés dans K si et seulement si c'est une norme de $K(i)$, c'est-à-dire un élément de $U.\dot{K}^2$.

2. La première assertion est un corollaire de la proposition (3.1.). Soit 2^l le plus petit naturel tel que $u\pi^{2l}$ soit somme de deux carrés d'entiers. Il existe $a, b, c, d \in U$ tels que:

$$u\pi^{2l} = a^2 + b^2 = (c\pi^l)^2 + d\pi^{2l+\delta(u)}.$$

Ce qui donne:

$$-1 = a^{-2}\{(b+c\pi^l)^2 - d\pi^{2l+\delta(u)} - 2bc\pi^l\}.$$

La dernière assertion de la proposition (1.3.2.) permet d'affirmer que $2l + \delta(u) \geqslant e+l$, c'est-à-dire $l \geqslant e-\delta(u)$. Reste à prouver que $u\pi^{2(e-\delta(u))}$ est somme de deux carrés d'entiers. Si on pose $2 = \varepsilon\pi^e$ et $-1 = v^2 + w\pi^{2e}$ avec $\varepsilon, v, w \in U$, on a pour tout $x \in U$:

$$u\pi^{2(e-\delta(u))} = (x+c\pi^{e-\delta(u)})^2 + v^2x^2 + d\pi^{2e-\delta(u)} - 2cx\pi^{e-\delta(u)} + x^2w\pi^{2e}.$$

On applique le lemme de Hensel (1.1.) au polynôme

$$f(X) = w\pi^{\delta(u)}X^2 - \varepsilon cX + d$$

en construisant la suite dont le premier terme est $d\varepsilon^{-1}c^{-1}$. Il existe donc $u' \in U$ tel que $f(u') = 0$ et on a

$$u\pi^{2(e-\delta(u))} = (u'+c\pi^{e-\delta(u)})^2 + v^2u'^2.$$

5.2.1. *Exemple numérique.* L'exemple le plus simple dans ce cas est celui du corps $\mathbf{Q}_2(\sqrt{3})$ pour lequel on a les propriétés suivantes:

a) On a $-1 = 3-4 = 27-28 = (3\sqrt{3})^2 + (2\sqrt{-7})^2$

b) Une uniformisante de ce corps est $\pi = 3 + \sqrt{3}$ dont le polynôme irréductible sur $\mathbf{Q}_2$ est X^2-6X+6. Avec les notations de (1.1.) on a $(U:V) = 2$ et un représentant de la classe non triviale de U modulo V est par exemple $1+\pi$. Pour cette unité on a $\delta(1+\pi) = 1$ et on peut écrire les relations suivantes:

$$u\pi^2 = (1+\pi)\pi^2 = 1+\pi^2-(1-\pi^3) = (1-\pi)^2-(1-2\pi-\pi^3)$$

avec $\pi^3 = 30\pi - 36$. On en déduit

$$(1+\pi)\pi^2 = (2\sqrt{3})^2 - [37-32\pi] = (2-\sqrt{3})^2 + (59-32\sqrt{3}).$$

Or, on constate facilement que $59 - 32\sqrt{3} = (2+8\sqrt{3})^2 - 135$, c'est-à-dire en définitive

$$(1+\pi)\pi^2 = (2-\sqrt{3})^2 + (2+8\sqrt{3})^2 + (3\sqrt{-15})^2.$$

Ceci étant, utilisons les notations de la démonstration de 5.2.: on a: $-1 = v^2 + \pi^{2e}w$ avec $v = \sqrt{3}$ et $w = -(3(1-\pi))^{-2}$ et $2 = \varepsilon\pi^e$ avec $[3(\pi-1)]^{-1}$.

Le polynôme $f(X)$ considéré en 5.2. est donc:

$$f(X) = -\pi(3(1-\pi))^{-2}X^2 - (3(\pi-1))^{-1}X + 1.$$

En effectuant le changement de variable $X_1 = -(3(\pi-1))^{-1} X$ on obtient $f(X) = \varphi(X_1) = -\pi X_1^2 + X_1 + 1$ dont le discriminant est

$$1 + 4\pi = 13 + 4\sqrt{3} = (1+2\sqrt{3})^2 = (-5+2\pi)^2 .$$

La racine de ce polynôme qui est une unité est:

$$x_1 = 1 - \pi[3(\pi-1)]^{-1} .$$

La racine de $f(X)$ qui est une unité est

$$x = 3 - 2\pi .$$

En fin de compte, on obtient pour $\pi^4(1+\pi)$ la représentation comme somme de deux carrés d'entiers:

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

5.3. *Proposition*

On suppose e pair et $\delta(-1) < 2e$. Soit u une unité de A.

1. *Si u est somme de deux carrés dans K on a les propriétés suivantes :*

a) *le plus petit entier impair $2k+1$ tel que $u\pi^{2k+1}$ appartienne à A_2 est $e+1$;*

b) *si π est somme de deux carrés dans K, le plus petit entier impair $2l+1$ tel que $u\pi^{2l+1}$ soit somme de deux carrés dans A est $\delta(-1)$;*

c) *si π n'est pas somme de deux carrés dans K, $u\pi^{2m+1}$ est somme de trois carrés dans A et pas moins quel que soit le nombre impair $2m+1 \geqslant e+1$;*

d) *le plus petit entier pair $2n$ tel que $u\pi^{2n}$ appartienne à A_2 est* $\max[0, e+1-\delta(u)]$ *;*

e) *si $\delta(-1) + \delta(u) < 2e$, le plus petit entier pair $2r$ tel que $u\pi^{2r}$ soit somme de deux carrés dans A est $\delta(-1) - \delta(u)$; si au contraire $\delta(-1) + \delta(u) \geqslant 2e$, le plus petit entier pair $2s$ tel que $u\pi^{2s}$ soit somme de deux carrés dans A est* $2\max[0, e-\delta(u)]$.

2. *Si u n'est pas somme de deux carrés dans K, on a les propriétés suivantes :*

f) *le plus petit entier k tel que $u\pi^k$ appartienne à A_2 est e ;*

g) *si π est somme de deux carrés dans K, alors pour tout $l \geqslant e$, $u\pi^l$ est somme de trois carrés dans A, mais non de deux ;*

h) *si π n'est pas somme de deux carrés dans K, le plus petit entier impair $2m+1$ tel que $u\pi^{2m+1}$ soit somme de deux carrés dans A est $\delta(-1)$; pour tout entier pair $2n \geqslant e$, $u\pi^{2n}$ est somme de trois carrés dans A mais non de deux.*

1. L'assertion a) résulte de la proposition (3.1.). En ce qui concerne b), si π est somme de deux carrés dans K, il en est de même de $u\pi^{2j+1}$ pour tout naturel j. Si $2l+1$ est le plus petit entier impair tel que $u\pi^{2l+1}$ soit somme de deux carrés dans A, il existe $a \in U$, $b \in A$ tels que $u\pi^{2l+1} = a^2 + b^2$, et on a $-1 = a^{-2}\{b^2 - u\pi^{2l+1}\}$; on en conclut que $2l+1 = \delta(-1)$ à l'aide de la proposition (1.4.). Si π n'est pas somme de deux carrés dans K, il en est de même de $u\pi^{2j+1}$ pour tout naturel j. On applique le théorème 5.1. Ceci démontre c). d) Si $\delta(u) \geqslant e$ on a $u \in V$ et il n'y a rien à démontrer. Si $\delta(u) < e$ on peut écrire $u = a^2 + b\pi^{\delta(u)}$. Si $2n$ est le plus petit entier pair cherché on a $2n + \delta(u) = e+1$ d'après la proposition (3.1.). e) Si on a $\delta(u) \geqslant e$, c'est-à-dire $u \in V$, il n'y a rien à démontrer. On supposera donc $\delta(u) < e$. Si $2n$ est l'entier minimum cherché il existe $a, b, c, d \in U$ tels que: $u = a^2 + b\pi^{\delta(u)} = (c^2+d^2)\pi^{-2n}$ et on a:

$$-1 = c^{-2}\{(d+a\pi^n)^2 - b\pi^{\delta(u)+2n} - 2ad\pi^n - 2a^2\pi^{2n}\};$$

Si $\delta(u) + 2n < e+n$, on a $\delta(u) + 2n = \delta(-1)$ avec l'inégalité $\delta(-1) + \delta(u) < 2e$.

Si $\delta(u) + 2n \geqslant e+n$, on a $e+n \leqslant \delta(-1)$, donc $2n \geqslant 2(e-\delta(u))$ et $\delta(-1) + \delta(u) \geqslant 2e$. Il suffit donc de montrer que $u\pi^{2(e-\delta(u))}$ est somme de deux carrés d'entiers. Or pour tout $y \in U$ on a:

$$\begin{cases} u\pi^{2(e-\delta(u))} = (y+a\pi^{e-\delta(u)})^2 - y^2 + b\pi^{2e-\delta(u)} - 2ay\pi^{e-\delta(u)} \\ -1 = v^2 + w\pi^{\delta(-1)} \text{ (pour un } v \text{ et un } w \in U). \end{cases}$$

de là:

$$\begin{aligned} u\pi^{2(e-\delta(u))} &= (y+a\pi^{e-\delta(u)})^2 + v^2y^2 + wy^2\pi^{\delta(-1)} \\ &\quad - 2ay\pi^{e-\delta(u)} + b\pi^{2e-\delta(u)}. \end{aligned}$$

Pour que $u\pi^{2(e-\delta(u))}$ soit somme de deux carrés dans A il suffit que le polynôme $f(Y) = w\pi^{\delta(-1)+\delta(u)-2e}Y^2 - 2\pi^{-e}aY + b$ ait un zéro $y \in U$. Mais on peut supposer $\delta(u) + \delta(-1) > 2e$ car si $\delta(-1) + \delta(u) = 2$ on a évidemment $2n = 2(e-\delta(u))$. Cela étant, le lemme de Hensel s'applique à $f(Y)$ et prouve que ce polynôme admet un zéro y congru à $b\pi^e/2a$ modulo $\mathfrak{P}$.

2. L'assertion f) est encore un corollaire de la proposition (3.1.). Si π est somme de deux carrés dans K, quel que soit $j \in \mathbf{N}$, $u\pi^j$ n'est pas somme de deux carrés dans K. On applique le théorème (5.1.) pour terminer la démonstration de g). h) Si π n'est pas somme de deux carrés dans K, alors $u\pi^{2j+1}$ est somme de deux carrés dans K puisque $(\dot{K} : N_{K(i)/K}(\dot{K}(i))) = 2$. Si $2m+1$ est l'entier impair minimum cherché il existe $a, b, c, d \in U$ tels que

$$c^2 + d^2 = a^2\pi^{2m+1} + b\pi^{2m+1+\delta(u)}$$

et on a $-1 = c^{-2}\{d^2 - a^2\pi^{2m+1} - b\pi^{2m+1+\delta(u)}\}$ et $\delta(-1) = 2m+1$. La dernière assertion se démontre comme l'assertion c) ci-dessus.

5.3.1. *Exemple numérique.* Le polynôme $X^4 - 2X + 2 \in \mathbf{Z}_2[X]$ est un polynôme d'Eisenstein, donc irréductible sur $\mathbf{Z}_2$. Si π est une racine de ce polynôme dans une clôture algébrique de $\mathbf{Q}_2$, alors $K = \mathbf{Q}_2(\pi)$ est une extension totalement ramifiée de degré 4 de $\mathbf{Q}_2$ dont π est une uniformisante. Dans l'anneau A des entiers de K on a:

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

Ceci implique que $\delta(-1) = 5$. Avec les notations de la proposition ci-dessus on a: $v = 1+\pi^2$, $w = \dfrac{1+\pi}{1-\pi}$ et $\varepsilon = \dfrac{-1}{1-\pi}$. Remarquons que l'unité $1-\pi$ est somme de deux carrés dans K puisque $1 - \pi = \dfrac{\pi^4}{2}$. Un système de représentants de U modulo V est par exemple

$$\{1, 1-\pi, 1-\pi^3, (1-\pi)(1-\pi^3)\}.$$

Remarquons encore, puisque tout élément de V est somme de deux carrés dans A et puisqu'il existe des unités de A qui ne sont pas somme de deux carrés dans K, que $1-\pi^3$ n'est pas somme de deux carrés dans K. Pour simplifier les notations posons $u_1 = 1-\pi$ et $u_2 = 1-\pi^3$. On obtient ainsi: $u_1\pi^5 = \pi^5 - \pi^6 = -2(1+\pi^4)$ qui est somme de deux carrés d'entiers. Ceci illustre les assertions a) et b) de la première partie de la proposition 5.4. car on a $\delta(-1) = e+1 = 5$.

Passons à l'étude de $u_2 = 1-\pi^3$. D'après ce qu'on a dit plus haut u_2 n'est pas somme de deux carrés dans K. Par suite $\pi^e u_2 = \pi^4 - \pi^7$ est somme de trois carrés dans A et pas moins. En effet on obtient $u_2\pi^4 = \pi^4 - \pi^7 = -2 + 2\pi - \pi^7 = 1 + (1 + 2\pi - \pi^7 - 4)$ et on a $1 + 2\pi - \pi^7 - 4 \in V_2$.

5.4. *Proposition*

On suppose e pair et $\delta(-1) = +\infty$, $(-1 \in \dot{K}^2)$. *Soit* $u \in U$. *Alors :*

1. *Le plus petit entier pair* $2k$ *tel que* $u\pi^{2k}$ *appartienne à* A_2 *est* $\max\{0, e+1-\delta(u)\}$; *le plus petit entier pair* $2l$ *tel que* $u\pi^{2l}$ *soit somme de deux carrés dans* A *est* $2\max\{0, e-\delta(u)\}$.

2. *Le plus petit entier impair* $2m+1$ *tel que* $u\pi^{2m+1}$ *appartienne à* A_2 *est* $e+1$ *; le plus petit entier impair* $2n+1$ *tel que* $u\pi^{2n+1}$ *soit somme de deux carrés dans* A *est* $2e+1$.

On remarque que tout élément de A est somme de deux carrés dans K. Ceci étant, la première assertion de 1) résulte de la proposition (3.1.) et la seconde se démontre comme la dernière assertion de la proposition (5.3.). 2) La première assertion résulte encore de la proposition (3.1.). En ce qui concerne la dernière assertion il existe $(a, b) \in U \times A$ tel que: $-1 = (a^{-1}b)^2 - a^{-2}u\pi^{2n+1}$.

La proposition (1.4.) permet d'affirmer que $2n+1 \geqslant 2e+1$ et que $2e+1$ convient.

5.4.1. *Exemple numérique.* Le polynôme $X^6 - 2X^3 + 4X + 2$ est un polynôme d'Eisenstein. Si π est une racine de ce polynôme dans une clôture algébrique de $\mathbf{Q}_2$, le corps $K = \mathbf{Q}_2(\pi)$ est totalement ramifié sur $\mathbf{Q}_2$ et admet π pour uniformisante. De plus dans l'anneau A des entiers de K on a l'égalité:

$$-1 = (1-\pi^3)^2 + 4\pi\,,$$

c'est-à-dire que -1 est un carré dans K. On a par ailleurs $(U : V) = 8$ et un système de représentants de U modulo V est par exemple:

$$\{1, 1+\pi, 1+\pi^3, 1+\pi^5, (1+\pi)(1+\pi^3), (1+\pi)(1+\pi^5), (1+\pi^3)(1+\pi^5), (1+\pi)(1+\pi^3)(1+\pi^5)\}\,.$$

A titre d'exemple, on a:

$$(1+\pi^3)\pi^{e+1-\delta(1+\pi^3)} = (1+\pi^3)\pi^4 = (1+\pi^4) - (1-\pi^7)$$
$$= (1+\pi^2)^2 - (1+2\pi-2\pi^2-2\pi^4)$$

cet entier est somme de trois carrés de A et pas moins. Par contre, on a: $(1+\pi^3)\pi^6 = \pi^6+\pi^9 = -[1-\pi^3]^2 + (-1-4\pi)$, qui est somme de deux carrés de A.