**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
**DOI:** https://doi.org/10.5169/seals-46913

# SOMMES DE CARRÉS D'ENTIERS D'UN CORPS $p$-ADIQUE

par Claude MOSER

RÉSUMÉ

On se propose de présenter, dans cet article, une étude aussi complète et élémentaire que possible de l'anneau formé par les entiers d'un corps $p$-adique qui sont sommes de carrés d'entiers. Après avoir donné des résultats généraux sur cet anneau, on recherche pour tout $n \geqslant 1$ quels sont les entiers qui sont sommes de $n$ carrés d'entiers, et si un entier est somme de $n$ carrés, on cherche à le représenter comme tel.

## 1. INTRODUCTION

Le premier intérêt de ce travail est de constituer une étape préliminaire pour l'étude des sommes de carrés d'entiers d'un corps de nombres: on sait qu'une condition nécessaire et suffisante pour qu'un élément totalement positif $a$ d'un corps de nombres $K$ soit somme de $n$ carrés dans $K$, est que $a$ soit somme de $n$ carrés dans chaque complété $p$-adique de $K$; c'est là une application directe du principe de Hasse [1], [4]. Ce principe n'est plus applicable en général lorsqu'il s'agit de représenter un entier comme somme de carrés d'entiers. Il n'en demeure pas moins qu'une condition nécessaire pour qu'un entier $a$ d'un corps de nombres $K$ soit somme de $n$ carrés d'entiers de $K$, est évidemment que $a$ soit somme de $n$ carrés d'entiers dans chaque complété $p$-adique de $K$. Signalons d'ailleurs que la condition est suffisante pour $n = 4$ si le discriminant de $K/\mathbf{Q}$ est impair, cf. [5].

Le second intérêt réside dans le caractère élémentaire de la démarche utilisée: si on peut considérer, en écho aux méthodes générales de C. Riehm sur la représentation d'une forme quadratique par une autre [6], que notre problème est un cas particulier de celui de la représentation entière d'une forme du type $aX^2$ par une forme $X_1^2 + \ldots + X_n^2$, la recherche explicite d'une telle représentation utilise en fait les calculs que nous faisons.

On conçoit que l'essentiel des difficultés réside dans le comportement des corps dyadiques, c'est-à-dire les extensions finies de $\mathbf{Q}_2$, et que les résul

tats dépendent étroitement de la ramification et de l'extension résiduelle du corps $K$ considéré. Mais ces facteurs ne suffisent pas: intervient aussi la propriété pour $-1$ d'être « plus ou moins loin » d'être un carré dans $K$. C'est pourquoi nous utilisons constamment la notion de défaut quadratique introduite par O. T. O'Meara [4].

Nous avons cru intéressant d'étayer les démonstrations de quelques exemples numériques simples qui permettent au lecteur de se rendre compte du caractère effectif de la méthode utilisée.

### 1.1. *Notations générales et rappels*

$K$ désignera un corps $p$-adique, d'anneau des entiers $A$; on notera:

| | |
|---|---|
| $\mathfrak{P}$ | l'idéal maximal de $A$; |
| $\pi$ | une uniformisante de $A$ (choisie une fois pour toutes); |
| $\dot{K}$ | le groupe multiplicatif de $K$; |
| $v : \dot{K} \to \mathbf{Z}$ | la valuation normalisée de $K$; |
| $U$ | le groupe des unités de $A$; |
| $\overline{K}$ | le corps résiduel de $K$; |
| $f$ | le degré résiduel $[\overline{K}:\mathbf{F}_p]$; |
| $e$ | l'indice de ramification absolu de $K$ sur $\mathbf{Q}_p$; |
| $d$ | la partie entière de $e/2$; |
| $A_2$ | le sous-anneau de $A$ formé des sommes de carrés d'éléments de $A$; |
| $V$ | le groupe des unités de $A_2$; |
| $V_n$ | l'ensemble des unités de $A_2$ qui sont sommes de $n$ carrés d'éléments de $A$ (pour $n \geqslant 1$); |
| $s(A)$ | la « stufe » de $A$, c'est-à-dire le plus petit entier $n$ tel que $-1 \in V_n$; |
| $t(A)$ | le plus petit entier $n$ tel que tout élément de $A_2$ soit somme de $n$ carrés d'éléments de $A$. |

1.1.1. *Lemme de Hensel. Soit $\varphi(X)$ un polynôme à coefficients dans $A$. Soit $a_0 \in A$ tel que $v(\varphi(a_0))$ soit strictement supérieur à $2v(\varphi'(a_0))$. Alors la suite $\{a_n\}_{n\in\mathbf{N}}$ définie par :*

$$a_{n+1} = a_n - \varphi(a_n)(\varphi'(a_n))^{-1}$$

*converge dans $A$ vers un zéro de $\varphi(X)$. De plus si $a$ est la limite de cette suite on a les inégalités :*

$$v(a - a_0) \geqslant v(\varphi(a_0)) - 2v(\varphi'(a_0)) > 1 .$$

Pour une démonstration voir [3].

## 1.2. *Extensions cycliques de corps locaux*

1.2.1. *Proposition. Soit L une extension finie et cyclique d'un corps local K et soit* $N_{K/L} : \dot{L} \to \dot{K}$ *l'application norme. On a les égalités :*

$$(\dot{K} : N_{L/K}(\dot{L})) = [L : K],$$
$$(U(K) : N_{L/K}(U(L))) = e(L/K).$$

Pour une démonstration voir [7], ou [4] pour le cas particulier d'une extension de degré 2.

1.2.2. *Proposition. Soit p un nombre premier. Pour tout* $n \geqslant 1$ *il existe une extension non ramifiée (unique à isomorphisme près) de degré n de* $\mathbf{Q}_p$. *Cette extension peut etre décrite comme étant le corps de décomposition sur* $\mathbf{Q}_p$ *du polynôme* $X^{p^n} - X$. *Elle est cyclique.*

Pour une démonstration voir également [4] et [7].

## 1.3. *Le défaut quadratique (cas dyadique, p=2)*

Dans tout ce paragraphe on considère des corps dyadiques, c'est-à-dire des extensions finies du corps $\mathbf{Q}_2$, complété 2-adique du corps des rationnels. La notion de défaut quadratique et les résultats qui la concernent sont dus à O'Meara (cf. [4]).

1.3.1. *Définition. Soit u une unité de A qui n'est pas un carré dans A. On appelle défaut quadratique de u, et on note* $\delta(u)$, *le plus grand entier n tel que la congruence*

$$u \equiv x^2 \pmod{\mathfrak{P}^n}$$

*ait une solution dans A. (Si u est un carré dans A, on convient de poser* $\delta(u) = +\infty$).

1.3.2. *Proposition. Soit u une unité de A.*

1. *Pour que u soit un carré dans A, il faut et il suffit que la congruence* $u \equiv x^2 \pmod{4\mathfrak{P}}$ *ait une solution dans A ; (autrement dit la condition* $\delta(u) \geqslant 2e + 1$ *équivaut à la condition* $\delta(u) = +\infty$).

2. *Si u satisfait à* $\delta(u) < 2e$, *alors* $\delta(u)$ *est un nombre impair.*

3. *L'extension quadratique* $K(\sqrt{u})/K$ *est non ramifiée si et seulement si on a* $\delta(u) = 2e$. *De plus, si deux unités ont pour défaut quadratique 2e, leur produit est un carré.*

4. *Soit $a$ un élément de $A$ tel que $v(a)$ soit impair. Alors $\delta(1+a) = v(a)$.*

Remarquons d'abord que toute unité $u$ a un défaut quadratique car du fait que $\overline{K} = \overline{K}^2$, toute congruence $u \equiv x^2 \pmod{\mathfrak{P}}$ a une solution dans $A$. De plus le défaut quadratique d'une unité $u$ ne dépend que de sa classe modulo les carrés d'unités. Soit $u$ une unité telle que $\delta(u) = m$ et soit $y \in U$. Posons $\delta(uy^2) = n$. A partir des représentations: $u = x^2 + x_1\pi^m$ et $y^2u = z^2 + z_1\pi^n$ on déduit les égalités:

$y^2u = x^2y^2 + x_1y^2\pi^m$, ce qui implique $m \leqslant n$;
$u = (zy^{-1})^2 + z_1y^{-2}\pi^n$, ce qui implique $n \leqslant m$; d'où $m = n$.

1. Soit $u$ une unité de $A$ telle que $\delta(u) \geqslant 2e + 1$. Quitte à multiplier $u$ par le carré d'une unité, on peut supposer qu'on a:

$$u = 1 + 4\pi b\,, \quad \text{avec} \quad b \in A\,.$$

Dans l'anneau de séries formelles $\mathbf{Q}[[T]]$ l'élément $1 + 4T$ est le carré de l'élément:

$$(1+4T)^{1/2} = 1 + \sum_{n=1}^{\infty} \frac{1}{n!}\left(\frac{1}{2}\right)\left(\frac{1}{2}-1\right)\cdots\left(\frac{1}{2}-n+1\right)4^nT^n\,;$$

on vérifie sans peine que pour tout $n \geqslant 1$ on a:

$$\frac{1}{n!}\left(\frac{1}{2}\right)\left(\frac{1}{2}-1\right)\cdots\left(\frac{1}{2}-n+1\right)4^nT^n = (-1)^{n-1}\binom{2n}{n}T^n\,.$$

[C'est un bon exercice de montrer que le coefficient binomial $\binom{2n}{n}$ est toujours pair, et qu'il est multiple de 4 si et seulement si $n$ n'est pas une puissance de 2]. Maintenant, dans l'espace ultramétrique complet $A$, la série de terme général $a_0 = 1$ et $a_n = (-1)^{n-1}\binom{2n}{n}\pi^nb^n$ $(n \geqslant 1)$ est convergente. On conclut à l'égalité:

$$(CAR.)\ 1 + 4\pi b = \Big\{1 + \sum_{n=1}^{\infty}(-1)^{n-1}\binom{2n}{n}\pi^nb^n\Big\}^2\,.$$

Cette formule rend « explicite » l'extraction de la racine carrée, en ce sens qu'il est possible, pour tout $n \geqslant 0$, de trouver le terme de rang $n$ du développement de Hensel d'une racine carrée de $1 + 4\pi b$.

Réciproquement, si $u$ est un carré d'unité, il est clair que la congruence: $u \equiv x^2 \pmod{4\,\mathfrak{P}}$ a une solution dans $A$.

[Pour une autre démonstration de cette assertion voir [4] pp. 160-163 à qui sont empruntées les démonstrations des assertions 2) à 4).]

2. Il suffit de montrer que si la congruence $u \equiv x^2 \pmod{\mathfrak{P}^{2a}}$ $(a<e)$ a une solution dans $A$, il en est de même de la congruence: $u \equiv x^2 \pmod{\mathfrak{P}^{2a+1}}$. Quitte, encore, à multiplier $u$ par le carré d'une unité, on peut supposer qu'on a $u = 1 + y\pi^{2a}$ avec $y \in A$. Si $y$ n'est pas une unité, il n'y a rien à démontrer. Au contraire si $y$ est une unité, il existe une unité $w$ et un entier $t \in A$ tels que $y = w^2 + \pi t$ et $u = 1 + w^2\pi^{2a} + t\pi^{2a+1}$, c'est-à-dire

$$u = (1+w\pi^a)^2 + t\pi^{2a+1} - 2w\pi^a \equiv (1+w\pi^a)^2 \pmod{\mathfrak{P}^{2a+1}},$$

car on a $v(t\pi^{2a+1} - 2w\pi^a) \geqslant \min\{2a+1, e+a\} \geqslant 2a+1$. On a donc $\delta(u) \geqslant 1 + 2a$.

3. Si $u = y^2 + 4z$ est une unité de $A$ telle que $\delta(u) = 2e$, alors $z$ est une unité et $u$ n'est pas un carré dans $A$. De plus, $\frac{1}{2}(y+\sqrt{u})$ est entier sur $A$. Son polynôme irréductible sur $A$ est $X^2 - yX - z$ dont le discriminant est $u$. C'est dire que $K(\sqrt{u})$ est une extension quadratique non ramifiée de $K$.

Réciproquement, soit $u$ une unité non carrée de $A$ telle que $K(\sqrt{u})$ soit non ramifiée sur $K$. Quitte à multiplier $u$ par le carré d'une unité, ce qui ne change pas l'extension $K(\sqrt{u})$, on peut supposer qu'on a $u = 1 + \pi^a b$ avec $a = \delta(u)$ et $b \in U$. Posons $c = -1 + \sqrt{u}$ et désignons par $\hat{v} : (K(\sqrt{u})) \to \mathbf{Z}$ la valuation normalisée de $K(\sqrt{u})$. Puisque l'extension $K(\sqrt{u})/K$ est non ramifiée, $\hat{v}$ coïncide avec $v$ sur $K$. Si on avait $\hat{v}(c) < e$ on aurait $a = 2\hat{v}(c) < 2e$, ce qui est impossible d'après l'assertion 2. ci-dessus. Par conséquent on a $\hat{v}(c) \geqslant e$ et $a \geqslant 2e$. Ceci implique $a = 2e$ puisque $u$ n'est pas un carré dans $A$.

La dernière partie de 3. résulte de l'unicité de l'extension non ramifiée de degré 2 de $K$.

4. Si $a \in A$ est de valuation impaire $v(a) < 2e$, il est clair qu'on a $\delta(1+a) \geqslant v(a)$. Raisonnons par l'absurde et supposons qu'existe $b \in A$ tel que $1 + a$ soit congru à $(1+b)^2$ modulo $\mathfrak{p}^{1+v(a)}$. On aurait $v(b(b+2)) = v(a)$. L'hypothèse $v(b) \geqslant e$ implique $v(a) \geqslant 2e$ tandis que l'hypothèse $v(b) < e$ implique $v(a) = 2v(b)$. Ces deux hypothèses contredisent la définition de $a$. Par conséquent, on a $\delta(1+a) \leqslant v(a)$.

## 2. Etude du cas $p$ impair

Cette étude se résume à l'énoncé et à la démonstration du théorème suivant:

### 2.1. *Théorème*

*Si $p$ est impair, tout entier de $K$ est somme de carrés d'entiers ($A = A_2$); plus précisément :*

1. *Pour qu'un entier de $K$ soit un carré, il faut que sa valuation normalisée soit un nombre pair. Un entier $x = u\pi^{2n}$ de valuation $2n$ est un carré dans $A$ si et seulement si la classe de $u$ dans $\bar{K}$ est un carré.*

2. *Si $p$ est congru à* 1 modulo 4, $-1$ *est un carré et tout entier est somme de deux carrés d'entiers,* ($s(A) = 1$, $t(A) = 2$).

3. *Si $p$ est congru à* $-1$ modulo 4, *on a $s(A) = 1$ et $t(A) = 2$ (resp. $s(A) = 2$ et $t(A) = 3$) si $f$ est pair (resp. impair). Si $f$ est impair, les entiers de valuation paire sont somme de deux carrés d'entiers tandis que les entiers de valuation impaire sont somme de trois carrés d'entiers et pas moins.*

En vue de la démonstration de ce théorème, rappelons quelques propriétés des corps finis:

### 2.2. *Lemme*

*Soit $p$ un nombre premier impair et soit $\mathbf{F}_p$ le corps à $p$ éléments.*

1. *Si $p$ est congru à* 1 modulo 4, *alors* $-1$ *est un carré dans $\mathbf{F}_p$ ; si $p$ est congru à* $-1$ modulo 4, $-1$ *n'est pas un carré dans $\mathbf{F}_p$, mais est somme de deux carrés dans $\mathbf{F}_p$.*

2. *Soit $k$ une extension finie de $\mathbf{F}_p$. Si $p$ est congru à* $-1$ modulo 4 *alors* $-1$ *est un carré dans $k$ si et seulement si $k/\mathbf{F}_p$ est de degré pair.*

Le groupe multiplicatif $\dot{\mathbf{F}}_p$ du corps $\mathbf{F}_p$ est cyclique d'ordre $p-1$. Il admet un seul sous-groupe d'ordre $\dfrac{p-1}{2}$. Or l'endomorphisme ($x \mapsto x^2$, $\dot{\mathbf{F}}_p \to \dot{\mathbf{F}}_p$) a pour noyau $\{-1, +1\}$. Il en résulte que le groupe des carrés de $\dot{\mathbf{F}}_p$ est l'unique sous-groupe d'ordre $\dfrac{p-1}{2}$ de $\dot{\mathbf{F}}_p$. Un élément est un carré si et seulement si son ordre divise $\dfrac{p-1}{2}$. Puisque l'ordre de $-1$ est 2, $-1$ est

un carré si et seulement si $\frac{p-1}{2}$ est pair. Il suffit de montrer que si $a \in \mathbf{F}_p$ n'est pas un carré il est somme de deux carrés. Pour cela considérons $A = \{ x \mid \exists y, x = y^2 \}$ et $B(a) = \{ x \mid \exists y, x = a - y^2 \}$. Ces deux sous-ensembles de $\mathbf{F}_p$ ont pour cardinal $\frac{p+1}{2}$. Puisque Card $\mathbf{F}_p = p$ on a $A \cap B(a) \neq \varnothing$, ce qui prouve que $a$ est somme de deux carrés dans $\mathbf{F}_p$.

La deuxième assertion résulte de ce que pour tout $n \geqslant 1$, $\mathbf{F}_p$ admet une extension de degré $n$ unique (à isomorphisme près) (cf. par exemple [2] ou [8]). Ceci étant, si $p$ est congru à $-1$ modulo 4 l'unique extension de degré 2 de $\mathbf{F}_p$ est $\mathbf{F}_p(\sqrt{-1})$.

Démontrons maintenant le théorème 2.1:

1. La première assertion est évidente. Soit $u$ une unité de $A$. Si la classe de $u$ modulo $\mathfrak{P}$ n'est pas un carré, a fortiori $u$ n'est pas un carré dans $A$. Si au contraire la classe de $u$ est un carré dans $\overline{K}$, il existe une unité $b$ de $A$ telle que l'on ait $u - b^2 \in \mathfrak{P}$. On peut alors appliquer au polynôme $X^2 - u$ le lemme de Hensel (1.1.1) et conclure que $u$ est un carré dans $A$.

2 et 3. Remarquons que 2 est une unité de $A$ et que pour tout élément $a$ de $A$ on a l'égalité:

$$(*) \quad a = \left(\frac{a+1}{2}\right)^2 - \left(\frac{a-1}{2}\right)^2 .$$

Si $p$ est congru à 1 modulo 4 ou si le degré résiduel $f = [\overline{K} : \mathbf{F}_p]$ de $K$ est pair, alors $-1$ est un carré dans $\overline{K}$ (cf. lemme 2.2) et la première partie du théorème permet d'affirmer que $-1$ est un carré dans $A$. On conclut facilement en utilisant (*) que tout élément de $A$ est somme de deux carrés dans $A$.

Enfin, si $p$ est congru à $-1$ modulo 4 et si le degré résiduel de $K$ est impair, $-1$ est somme de deux carrés dans $\overline{K}$. Il existe donc deux unités $u$ et $z$ de $A$ telles que $-1 - u^2 - z^2 \in \mathfrak{P}$. On applique alors le lemme de Hensel au polynôme $X^2 + 1 + u^2$ pour conclure qu'il existe une unité de de $A$ telle que $1 + u^2 + w^2 = 0$. Alors toute unité de $A$ est somme de deux carrés d'éléments de $A$ puisque toute unité est soit un carré soit l'opposé d'un carré. Pour terminer remarquons que les éléments de $K$ qui sont somme de deux carrés dans $K$ sont les normes des éléments de $K(\sqrt{-1})$. L'égalité $[\dot{K} : N(K(\sqrt{-1}))\cdot] = 2$ implique qu'aucun élément de valuation impaire n'est somme de deux carrés dans $K$. Enfin tout élément de valuation impaire de $A$ est somme de trois carrés dans $A$ en vertu de l'égalité (*).

## 3. Etude du cas $p = 2$. Résultats généraux

Ce paragraphe regroupe quelques résultats valables pour tous les corps dyadiques.

### 3.1. *Proposition*

*Soit $u$ une unité de $A$, anneau des entiers du corps dyadique $K$ (extension finie de $\mathbf{Q}_2$).*

1. *Le plus petit entier impair $2k+1$ tel que $u\pi^{2k+1}$ soit somme de carrés d'entiers est $2d+1$ ; ($d$ est la partie entière de $e/2$).*

2. *Pour que $u$ soit somme de carrés d'entiers ($u \in V$), il faut et il suffit qu'on ait $\delta(u) \geqslant e$. De plus, si on a $\delta(u) \geqslant e+1$, alors $u$ est somme de deux carrés d'entiers.*

Remarquons que $-1$ est somme de carrés dans $A$, ce qui permet d'affirmer que $A_2$ est bien un sous-anneau de $A$: dans l'anneau $\mathbf{Z}_2$ des entiers dyadiques, $-7$ est un carré car 2 est une uniformisante et $-7$ est congru à 1 modulo 8. Il en résulte que $-1 = 1+1+4-7$ est somme de quatre carrés dans $A$. Ceci étant:

1. Pour tout élément $a$ de $A$ on a l'égalité $2a = (a+1)^2 - (a^2+1)$; par conséquent $2a$ est somme de carrés dans $A$. Plus précisément, si $b$ est une racine carrée de $-7$ dans $\mathbf{Z}_2$, on a l'égalité obtenue à partir de la propriété de multiplicativité de la norme des quaternions:

$$2a = (1+a)^2 + (1+a)^2 + (1-a)^2 + (2+ab)^2 + (2a-b)^2 .$$

Par ailleurs, il existe une unité $\varepsilon$ de $A$ satisfaisant à $\pi^e = 2\varepsilon$. Dans ces conditions on a bien $u\pi^e \in A_2$ pour toute unité $u$ de $A$. En particulier, on a $u\pi^{2d+1} \in A_2$ pour toute unité $u$ de $A$.

Réciproquement, soit $u$ une unité de $A$, $2k+1$ un entier impair tels qu'on ait $u\pi^{2k+1} \in A_2$; il existe une famille finie $\{a_1, \ldots, a_N\}$ d'éléments de $A$ telle que:

$$u\pi^{2k+1} = \sum_{j=1}^{N} a_j^2 = \left(\sum_{j=1}^{N} a_j\right)^2 - 2 \sum_{1 \leqslant i < j \leqslant N} a_i a_j .$$

Comparons les valuations $\mathfrak{P}$-adiques de chacun des termes écrits ci-dessus; on a $v_K(u\pi^{2k+1}) \geqslant \min\{2v_K(\sum_1^N a_j), e + v_K(\sum_{1 \leqslant i < j \leqslant N} a_j a_j)\}$. On ne peut

avoir $2v_K(\sum_{j=1}^{N} a_j) < e + v_K(\sum_{1\leq i<j\leq N} a_i a_j)$ car $v_K(u\pi^{2k+1})$ est impair. On en conclut que $2k+1 \geqslant e$ et de façon plus précise que $k$ est supérieur ou égal à $d$.

2. Si $u \in U$ est une somme de carrés dans $A$, il existe une famille finie d'éléments de $A$, soit $\{ a_1, ..., a_N \}$, telle que

$$u = \sum_{j=1}^{N} a_j^2 = (\sum_{j=1}^{N} a_j)^2 - 2 \sum_{i<j} a_i a_j ;$$

ceci prouve que $\delta(u)$ est supérieur ou égal à $e$. Réciproquement, si $\delta(u)$ est supérieur ou égal à $e$, il existe une unité $v$ de $A$ et un entier $b$ tels que $u = v^2 + \pi^e b$; or on vient de voir que $\pi^e b$ est somme de carrés dans $A$.

3. Si l'unité $u$ satisfait à $\delta(u) \geqslant e+1$, il existe une unité $v$ de $A$ et un entier $b$ tels qu'on ait:

$$u = v^2 + 2\pi b = \frac{1}{2} v^2 [1 + 1 + 4\pi b v^{-2}] .$$

De l'égalité $(CAR)$ obtenue au paragraphe (1.3.2.) on déduit:

$$u = \frac{1}{2} v^2 \{ 1 + [1 + \sum_{n=1}^{\infty} (-1)^{n-1} \binom{2n}{n} \pi^n b^n v^{-2n}]^2 \} ,$$

$$u = v^2 \{ [1 + \frac{1}{2} \sum_{n=1}^{\infty} (-1)^{n-1} \binom{2n}{n} \pi^n b^n v^{-2n}]^2 + [\frac{1}{2} \sum_{n=1}^{\infty} (-1)^{n-1} \binom{2n}{n} \pi^n b^n v^{-2n}]^2 \} .$$

Alors $u$ est somme de deux carrés dans $A$ puisque pour tout $n \geqslant 1$ $\binom{2n}{n}$ est un nombre pair.

### 3.2. *Théorème*

*Soit T la sous-extension non ramifiée maximale de K et soit B l'anneau des entiers de T. Alors :*

1. *Les anneaux B et $B_2$ coïncident, c'est-à-dire que tout entier de T est somme de carré d'entiers de T.*

2. *L'anneau $A_2$ est un anneau local, nœthérien, de dimension 1 ; son idéal maximal est $\mathfrak{P} \cap A_2$. En tant que B-module, $A_2$ est libre de rang e. En tant que B-algèbre, $A_2$ est égal à $B[\pi^2, 2\pi]$.*

3. *Avec les notations* 1, *on a la double égalité :*

$$(A : A_2) = (U : V) = 2^{df}$$

1. Puisque $B$ est non ramifié sur $\mathbf{Z}_2$, 2 est une uniformisante de $B$; tout élément non nul de $B$ s'écrit donc de façon unique sous la forme $2^n(1+2a)$ avec $n \in \mathbf{N}$ et $a \in B$, et on a dans $B$ : $1+2a = (a+1)^2 + a^2 + a^2 + 4a^2 + (\sqrt{-7})^2 a^2$.

2. L'anneau $A$ est une extension totalement ramifiée de $B$; il en résulte que $\pi$, uniformisante de $A$, est racine d'un polynôme d'Eisenstein à coefficients dans $B$; en d'autres termes, il existe une unité $b_0$ de $B$ et $(e-1)$ éléments $b_1, \ldots, b_{e-1}$ de $B$ tels qu'on ait:

$$\pi^e = 2 \sum_{j=0}^{e-1} b_j \pi^j .$$

Par ailleurs, on sait que $A = B[\pi]$ et que la famille $\{ 1, \pi, \ldots, \pi^{e-1} \}$ est une base du $B$-module $A$. On va montrer que si $e$ est pair, (resp. impair), la famille $\{ 1, 2\pi, \pi^2, \ldots, \pi^{e-2}, 2\pi^{e-1} \}$ (resp. $\{ 1, 2\pi, \pi^2, \ldots, 2\pi^{e-2}, \pi^{e-1} \}$) constitue une base de $A_2$ considéré comme $B$-module. En premier lieu, il est clair que $B$ est un sous-anneau de $A^2$ et que la famille considérée est libre sur $B$.

Remarquons qu'on peut choisir comme système $R$ de représentants non nuls de $A$ modulo $\mathfrak{P}$ un ensemble d'unités de $B$, ces unités étant elles-mêmes des carrés dans $B$. (On a en effet $\overline{K} = \overline{K}^2$ et toute unité de $B$ est congrue à un carré modulo $2B$.) Tout élément $a$ de $A$ admet donc un développement de Hensel de la forme:

$$a = \sum_{j=0}^{\infty} r_j^2 \pi^j \quad (r_j^2 \in R \cup \{ 0 \} \quad \text{pour tout } j \in \mathbf{N}) .$$

En particulier, il résulte de la proposition 3.1.1.) que tout $a \in A_2$ admet un développement de Hensel de la forme:

$$a = \sum_{j=0}^{d} r_{2j}^2 \pi^{2j} + \pi^{1+2d} \sum_{j=0}^{\infty} r_{j+1+2d}^2 \pi^j .$$

Remarquons alors les détails suivants:

a) L'ensemble $A_2$ est un fermé de $A$ pour la topologie $\mathfrak{P}$-adique. Ceci est encore une conséquence de la proposition 3.1.1.).

b) L'ensemble $B[\pi^2, 2\pi]$ est un fermé de $A$ pour la topologie $\mathfrak{P}$-adique.

Or sur $B[\pi^2, 2\pi]$ cette topologie coïncide avec l'unique prolongement à cet espace de la topologie 2-adique de $B$. En particulier $B[\pi^2, 2\pi]$ est un fermé de $A_2$.

Il reste en définitive à prouver que $B[\pi^2, 2\pi]$ est dense dans $A_2$. Pour cela, il suffit de montrer que pour tout $n \in \mathbf{N}$, $\pi^{e+n}$ est combinaison linéaire à coefficients dans $B$ des éléments de la famille considérée plus haut. Faisons la démonstration dans le cas $e$ pair; (dans le cas $e$ impair, la démonstration est analogue):

Les remarques faites au début de la démonstration montrent que la propriété à démontrer est vraie pour $n = 0$. De plus, on a les égalités:

$$\pi^{e+1} = 2\pi \sum_{j=0}^{e-1} b_j \pi^j = 2 \sum_{j=0}^{d-2} b_{2j+1} \pi^{2(j+1)} + 2b_{e-1}\pi^e + 2\pi \sum_{j=0}^{d-1} b_{2j} \pi^{2j};$$

$$\pi^{e+1} = 2b_0 b_{e-1} + \sum_{j=1}^{d-1} (b_{2j-1} + 2b_{e-1}b_{2j})\pi^{2j}$$

$$+ 2\pi \sum_{j=0}^{d-1} (b_{2j} + 2b_{e-1}b_{2j+1})\pi^{2j};$$

$$\pi^{e+2} = 2b_{e-1}\pi^{e+1} + 2b_{e-2}\pi^e + \sum_{j=0}^{e-3} 2b_j \pi^{j+2}.$$

A partir de là on raisonne par récurrence sur $m$ pour évaluer $\pi^{e+2m}$ et $\pi^{e+1+2m}$.

Enfin, puisque $B$ est un anneau de valuation discrète, la $B$-algèbre de type fini $B[\pi^2, 2\pi]$ est un anneau nœthérien; puisque $A$ est un anneau de valuation discrète entier sur $A_2$, l'unique idéal maximal de $A_2$ est $\mathfrak{P} \cap A_2$.

3. L'égalité $(A : A_2) = 2^{df}$ résulte de ce que $\{1, \pi, ..., \pi^{e-1}\}$ est une base de $A$ en tant que $B$-module, tandis qu'une base de $A_2$ comme $B$-module est $\{1, 2\pi, ..., 2\pi^{e-1}\}$ ou $\{1, 2\pi, ..., \pi^{e-1}\}$ selon que $e$ est pair ou impair. Reste à démontrer la dernière égalité.

Pour tout $n \geqslant 1$ soit $U_n$ le sous-groupe $1 + \mathfrak{P}^n$ de $U$. On sait que $(U:U_1) = 2^f - 1$ et que pour tout $n \geqslant 1$ on a $(U_n:U_{n+1}) = 2^f$. (Pour plus de détails, voir [4] ou [5].) Il résulte de la proposition 3.1, 1), qu'on a:

$$V = U^2 \cdot U_{2d+1}.$$

Montrons qu'on a $U^2 \cap U_{2d+1} = U_{d+1}^2$. L'inclusion $U_{d+1}^2 \subset U^2 \cap U_{2d+1}$ est évidente. Réciproquement, soit $x \in U$ tel que $x^2 = 1 + a\pi^{2d+1}$ avec $a \in A$. Quitte à changer $x$ en $-x$ on peut écrire $x$ sous la forme $1 + b\pi^2$ avec $\varepsilon \geqslant 1$ et $b \in A$. On obtient alors $b^2\pi^{2\varepsilon} = a\pi^{2d+1} - 2b\pi^{\varepsilon}$ ce qui implique $2\varepsilon \geqslant 2d+1$ et $\varepsilon \geqslant d+1$.

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 $\alpha$, $\beta$ 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 $\pi$ 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 $\pi c$ et $\pi d$ 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:

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

## 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 $\pi$ 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 $\pi$ 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 $u\pi^{25}$ 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 $\pi$ 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 $\pi$ 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 $\pi$ 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 $\pi$ 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:

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

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 $\pi$ 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 $\pi$ 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 $\pi$ 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 $\pi$ 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 $\pi$ 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 $\pi$ 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 $A$.

## BIBLIOGRAPHIE

[1] HASSE, H. Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen. *Journal de Crelle CLII* (1923).
[2] JOLY, J. R. Equations et variétés algébriques sur un corps fini, chap. 1. *L'Enseignement mathématique XIX* (1973).
[3] LANG, S. *Algebraic Numbers*. Addison Wesley (1964).
[4] O'MEARA, O. T. *Introduction to Quadratic Forms*. Springer (1963).
[5] PETERS, M. Quadratische Formen über Zahlringen. *Acta Arithmetica XXIV* (1973).
[6] RIEHM, C. On the Integral Representation of Quadratic Forms over Local Fields. *American Journal of Mathematics* (1964).
[7] SERRE, J. P. *Corps locaux*. Hermann (1968).
[8] —— *Cours d'arithmétique*. P.U.F. (1970).

*(Reçu le 29 octobre 1974.)*

Claude Moser

Institut de mathématiques pures
Boîte postale 116
F-38402 Saint-Martin-d'Hères