SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

CLAUDE MOSER

Sommes de carrés d'entiers d'un corps dyadique

Séminaire de théorie des nombres de Grenoble, tome 2 (1972-1973), exp. n° 4, p. 1-16

<http://www.numdam.org/item?id=STNG_1972-1973__2__A4_0>

Claude MOSER

15 mars 1973

SOMMES DE CARRES D'ENTIERS D'UN CORPS DYADIQUE

Soient p un nombre premier, K un corps p-adique (extension finie de $\mathbb{Q}_p$) et A l'anneau des entiers de K. Le but de cet exposé est l'étude de la décomposition des entiers de K en sommes de carrés dans A. Cette étude se veut élémentaire et utilise essentiellement une forme faible du lemme de Hensel et la notion de défaut quadratique d'une unité dans le cas $p = 2$. Le cas p impair ne présente aucune difficulté et n'est cité que pour mémoire. Par contre, les résultats concernant le cas $p = 2$ sont assez "dispersés" puisqu'ils dépendent de trois paramètres de K : l'indice de ramification absolu $e = e(K/\mathbb{Q}_2)$, le degré résiduel $f = f(K/\mathbb{Q}_2)$ et le défaut quadratique de -1 dans K.

1. NOTATIONS GENERALES ET RAPPELS.

Etant donné le corps p-adique K dont l'anneau des entiers est A on notera :

- $\mathfrak{p}$ l'idéal maximal de A ;
- π une uniformisante de A (choisie une fois pour toutes) ;
- $\mathcal{U}$ le groupe des unités de A ;
- $\bar{K}$ le corps résiduel de K ;
- f le degré résiduel $[\bar{K}:\mathbb{F}_p]$;
- e l'indice de ramification absolue de K sur $\mathbb{Q}_p$;
- 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 ;

$V_n (n \geq 1)$ l'ensemble des unités de A_2 qui sont somme de n carrés d'éléments de A ;

$s(A)$ la "stufe" de A, c'est-à-dire le plus petit 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. Lemme de Hensel.

Soit $v : \dot{K} \to Z$ la valuation normalisée de K et soit $f(X)$ un polynôme à coefficients dans A. Soit $a_o \in A$ tel que $v(f(a_o))$ soit strictement supérieur à $2v(f'(a_o))$. Alors la suite $\{a_n\}_{n \in \mathbb{N}}$ définie par :

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

converge vers un zéro de f dans A. De plus, si a est la limite de cette suite on a les inégalités :

$$v(a-a_o) \geq v(f(a_o)) - 2v(f'(a_o)) > 1 .$$

■ Démonstration dans S. LANG, Algebraic Numbers, Addison Wesley. ■

1.2. Proposition.

Soit L une extension finie et cyclique de K et soit $N_{L/K} : \dot{L} \to \dot{K}$ l'application norme. On a les égalités :

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

$$(U : N_{L/K} U_L) = e(L/K) .$$

■ Voir J.P. SERRE, Corps locaux, Hermann. ■

Dans la suite de ce paragraphe, on suppose $p = 2$.

1.3. Définition du défaut quadratique.

Soit u une unité de A qui n'est pas un carré dans K ; on appelle défaut quadratique de u, et on note $\delta(u)$, le plus petit entier n tel que la congruence :

$$u \equiv x^2 \pmod{p^n}$$

ait une solution dans A . (Soit u une unité qui est un carré dans K ; on convient de poser $\delta(u) = +\infty$).

Cette notion est empruntée à O.T.O'MEARA, ainsi que les résultats suivants :

1.4. Proposition.

Soit u une unité de A .

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

2) L'extension quadratique $K(\sqrt{u})/K$ est non ramifiée si et seulement si $\delta(u) = 2e$.

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

4) Soit α un élément de A dont la valuation normalisée est un nombre impair $v(\alpha)$ inférieur à 2e . On a $\delta(1+\alpha) = v(\alpha)$.

■ Voir O.T. O'MEARA, Introduction to Quadratic Forms, Springer, § 63, page 160. ■

Remarque : La proposition ci-dessus est une formulation, dans le cas d'extensions quadratiques de K , du théorème sur la décomposition d'un idéal dans une extension de Kummer. (cf. HECKE, Vorlesungen über die Theorie der algebraischen Zahlen, (Chelsea), Chap.V paragraphe 39). Si on raisonne en terme de nombre de ramification (J.P. SERRE, Corps locaux) et si on désigne par r(u) le nombre de ramification de l'extension $K(\sqrt{u})/K$ on vérifie sans peine que $\delta(u)$ est égal à $2e+1-r(u)$.

2. ETUDE DU CAS p IMPAIR.

Elle peut se résumer dans le 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.

▪ 1) Remarquons que l'égalité des indices $(U : U^2)$ et $(\dot{\bar{K}} : \dot{\bar{K}}^2) = 2$ est une conséquence immédiate du lemme de Hensel. Par ailleurs, le choix d'une uniformisante de K définit un isomorphisme du groupe $\dot{K}$ sur le groupe produit $\mathbb{Z} \times U$ et par suite un isomorphisme de $\dot{K}/\dot{K}^2$ sur $(\mathbb{Z}/2\mathbb{Z}) \times (U/U^2)$. On en déduit l'assertion.

2) Si p est congru à 1 modulo 4, -1 est un carré dans $\bar{K}$. On utilise alors l'identité

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

et le fait que 2 est une unité de A .

3) Si p est congru à -1 modulo 4 et si f est pair, -1 est un carré dans $\bar{K} = \mathbb{F}_{p^f}$ et on raisonne comme dans 2).

Par contre, si f est impair, -1 n'est pas un carré dans $\bar{K}$, mais est somme de deux carrés dans $\bar{K}$ (Toute forme quadratique binaire sur un corps fini est universelle) ; il en résulte que -1 est somme de deux carrés dans A . Tout entier de valuation paire est soit un carré, soit l'opposé d'un carré, c'est-à-dire une somme de deux carrés d'entiers. Enfin, l'extension

$\mathbb{Q}_p(i)/\mathbb{Q}_p$ $(i^2=-1)$ est non ramifiée. Il en est de même de l'extension $K(i)/K$. Ceci montre qu'aucun élément de valuation impaire de K n'est somme de deux carrés dans K . Enfin, tout entier de valuation impaire est somme de trois carrés d'entiers en vertu de (*) ■

3. ETUDE DU CAS $p = 2$. RESULTATS GENERAUX.

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 $\mathbb{Q}_2$).

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 $\delta(u) \geq e$. De plus, si on a $\delta(u) \geq e+1$, alors u est somme de deux carrés d'entiers.

■ Remarquons tout d'abord qu'on a $-1 \in A_2$. En effet il résulte du lemme de Hensel (1.1) appliqué à X^2+7 dans $\mathbb{Z}_2[X]$, que -7 est un carré dans $\mathbb{Z}_2$, donc que $-1 = 1+1+4-7$ appartient à V_4 (ceci montre que A_2 est bien un sous-anneau de A).

1) On a pour tout entier a : $2a = (a+1)^2 - (a-1)^2$. Par ailleurs il existe une unité ε de A telle que $\pi^e = 2\varepsilon$. Dans ces conditions on a bien $u\pi^e \in A_2$ pour tout $u \in \mathcal{U}$. En particulier, on a bien $u\pi^{2d+1} \in A_2$ pour tout $u \in \mathcal{U}$.

Réciproquement, supposons qu'on ait une égalité du type :

$$u\pi^{2k+1} = \sum_{j=0}^{N} a_j^2 \quad , \quad (a_0, \ldots, a_N \in A) \quad .$$

Alors :

$$u\pi^{2k+1} = (\sum_{0}^{N} a_j)^2 - 2 \sum_{0\le i<j\le N} a_i a_j \quad .$$

La comparaison des valuations de chacun des membres de cette égalité montre qu'on a $2k+1 \ge e$, c'est-à-dire $k \ge d$.

2) Si $u \in \mathcal{U}$ est somme de carrés d'entiers, on a une égalité du type : $u = (\sum_{0}^{N} a_j)^2 - 2 \sum_{0\le i<j\le n} a_i a_j$, $(a_1,\ldots,a_n \in A)$. On en déduit que $\sum_{0}^{N} a_j$ est une unité de A et que $\delta(u) \ge e$. La réciproque est une conséquence immédiate de 1) et de l'assertion 3) de la proposition (1.4). Supposons maintenant qu'on ait $\delta(u) \ge e+1$. Il existe alors une unité ϵ de A et un entier η tels que : $u = \epsilon^2 + 2\pi\eta = \epsilon^2 + 4\pi\eta - 2\pi\eta$. Il résulte alors de l'assertion 1) de la proposition (1.4) que $\epsilon^2+4\pi\eta$ est le carré d'une unité γ de A. Ceci étant on a :

$$u = \frac{1}{2}(\epsilon^2+\gamma^2) = (\frac{\epsilon+\gamma}{2})^2 + (\frac{\epsilon-\gamma}{2})^2$$

$$\epsilon^2-\gamma^2 = -4\eta\pi \quad .$$

Il suffit de montrer que $\frac{1}{2}(\epsilon+\gamma)$ et $\frac{1}{2}(\epsilon-\gamma)$ sont des entiers. Si ces deux éléments ont même valuation, la deuxième égalité montre que cette valuation est positive. S'ils n'ont pas la même valuation, l'un d'eux est une unité et l'autre est un entier ■

3.2. Proposition.

Soit $\mathcal{U}$ le groupe des unités de A et soit V le groupe des unités de V. Le sous-groupe V de $\mathcal{U}$ est d'indice 2^{df} dans $\mathcal{U}$:

$$(U:V) = 2^{df} \quad .$$

■ Pour tout $n \ge 1$ désignons par $\mathcal{U}_n$ le sous-groupe $1+\mathfrak{p}^n$ de $\mathcal{U}$. On sait que pour tout $n \ge 1$ on a $(U:U_1) = 2^f-1$ et $(U_n:U_{n+1}) = 2^f$ (cf. J.P. SERRE, Corps locaux).

Remarquons ensuite qu'on a l'égalité :

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

(C'est une conséquence immédiate de l'assertion 1) de la proposition (3.1)).

Montrons qu'on a $U^2 \cap U_{2d+1} = U^2_{d+1}$. L'inclusion $U^2_{d+1} \subset U^2 \cap U_{2d+1}$ est évidente. Réciproquement, soit $x \in \mathcal{U}$ 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 $x = 1 + b\pi^{\varepsilon}$ avec $\varepsilon \geq 1$ et $b \in A$. On obtient alors $b^2\pi^{2\varepsilon} = a\pi^{2d+1} - 2b\pi^{\varepsilon}$, ce qui montre que $2\varepsilon \geq 2d+1$, donc $\varepsilon \geq d+1$.

Tout 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 . 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.

Si ces assertions sont vraies on a l'égalité :

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

(Pour une démonstration, voir par exemple O.T. O'MEARA op.cit. §63).

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

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

et les égalités

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

D'où enfin

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

4. RESULTATS PROPRES AU CAS $p = 2$ ET e IMPAIR.

4.1. Théorème.

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

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

2) Si $\delta(u) = e$, il existe $a,b \in \mathcal{U}$ 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 $2\mathbb{Z}_2$;

c) Il existe $c \in \mathcal{U}$ 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.

■ 1) est un corollaire de l'assertion 2) de la proposition (3.1).

2) On sait que l'extension $\bar{K}/\mathbb{F}_2$ est finie et cyclique. Dans cette extension l'application trace : $tr : \bar{K} \to \mathbb{F}_2$ est un homomorphisme surjectif de groupes additifs dont le noyau est l'ensemble $\{y^2-y \mid y \in \bar{K}\}$. Ceci étant, soit u un élément de V_2 : il existe $\alpha \in \mathcal{U}$ et $\beta \in A$ tels que $u = N_{K(i)/K}(\alpha+i\beta)$ ($i^2 = -1$; remarquons au passage que -1 n'est pas un carré dans K en vertu de la dernière assertion de la proposition 1.4 et de l'égalité $-1 = 1-2$). Il en résulte que $N_{K/\mathbb{Q}_2}(u)$ est la norme d'une unité de $\mathbb{Q}_2(i)$ dans l'extension $\mathbb{Q}_2(i)/\mathbb{Q}_2$. On a donc $N_{K/\mathbb{Q}_2}(u) \in 1+4\mathbb{Z}_2$. Par ailleurs, si $u = a^2 + 2b$ dans A on a :

$$N_{K/\mathbb{Q}_2}(u) = (N_{K/\mathbb{Q}_2}(a))^2 [1 + 2\,\mathrm{Tr}_{K/\mathbb{Q}_2}(b/a^2) + 4h] \qquad (h \in \mathbb{Z}_2) .$$

Puisque a est une unité de A on a $(N_{K/\mathbb{Q}_2}(a))^2 \in 1+8\mathbb{Z}_2$ et on en déduit bien $\mathrm{Tr}_{K/\mathbb{Q}_2}(b/a^2) \in 2\mathbb{Z}_2$.

Maintenant, si on a $\mathrm{Tr}_{K/\mathbb{Q}_2}(b/a^2) \in 2\mathbb{Z}_2$, il existe $c_o \in \bar{K}$ tel que la classe de (b/a^2) dans $\bar{K}$ soit $c_o^2-c_o$. L'application du lemme de Hensel au polynôme $X^2 - X - (b/a^2)$ permet d'affirmer l'existence de $c \in \mathcal{U}$ tel que $b = a^2(c^2-c)$.

Enfin, s'il existe $c \in \mathcal{U}$ 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 $-1 = j^2 + j^4$ et $s(A) = 2$. Si $u \in \mathcal{U}$ satisfait à $\delta(u) \geq e$ on peut écrire $u = a^2 + 2b$ $(a \in \mathcal{U}, b \in A)$ et $u = (a+b/a)^2 - (b/a)^2 \in V_3$. L'assertion sur $t(A)$ sera démontrée plus loin.

4) Remarquons que $\mathrm{Tr}_{K/\mathbb{Q}_2}(-1) = -ef \notin 2\mathbb{Z}_2$. 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 $-U^2 \subset V_4 \setminus V_3$.

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 $x \in G(u) \setminus G(-1)$; 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 $V \setminus V_2$, 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 $\mathrm{Tr}_{K/\mathbb{Q}_2}(b) \in 1 + 2\mathbb{Z}_2$; on a alors $-u = 1 - 2(b+1)$ et $\mathrm{Tr}_{K/\mathbb{Q}_2}(-(b+1)) = -ef + \mathrm{Tr}_{K/\mathbb{Q}_2}(-b) \in 2\mathbb{Z}_2$. 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 $n \geq 1$, 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 $V_4 \setminus V_3 = -U^2$ ■

4.2. Proposition.

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

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 $2\ell \geq \max[0,e-\delta(u)]$ $u\pi^{2\ell}$ 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 $2\ell+1 \geq e$ $u\pi^{2\ell+1}$ 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 $\delta(u) \geq e$ 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 $a,v \in \mathcal{U}$ 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 et 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 $\nu \in \mathbb{N}$, $a,v,x \in \mathcal{U}$, $y \in A$ tels que : $u\pi^{2\nu} = a^2\pi^{2\nu} + 2v\pi^{2\nu} = x^2+y^2$; si on avait $\nu > 0$, y serait une unité et on aurait :

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

ce qui impliquerait $\delta(-1) > e$. Contradiction puisque $\delta(-1) = e$ d'après la dernière assertion de la proposition (1.4). On a donc $\nu = 0$ et $u \in V_2$. Enfin, dans le cas où $\delta(u) < e$, on peut écrire de manière analogue

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

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

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

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

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 2ν le plus petit entier pair tel que $u\pi^{2\nu}$ soit somme de trois carrés dans A. Il existe $x \in \mathcal{U}$, $y,z \in A$ tels que $u\pi^{2\nu} = x^2 + y^2 + z^2$ et on a :

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

Si $yz \in \mathfrak{p}$ on a immédiatement $2\nu + \delta(u) = e$ puisque $\nu > 0$.
Si $yz \in \mathcal{U}$ on a nécessairement $2\nu + \delta(u) \geq e$ et on peut écrire :

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

Si on avait $\delta(u) + 2\nu > e$ on aurait $z^2 - v\pi^{2\nu+\delta(u)} - 2a^2\pi^{2\nu} - 2ay\pi^{\nu} \in V_2$ 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 $v \in \mathcal{U}$ 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 $2\ell+1$ est le plus petit entier impair tel que $u\pi^{2\ell+1}$ soit somme de deux carrés dans A il existe deux unités a,b de A telles que $a^2+b^2 = u\pi^{2\ell+1}$. On a alors :
$-1 = a^{-2}\{b^2+u\pi^{2\ell+1}\}$ et on conclut que $2\ell+1 = e$.

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

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

puisque $s(A) = 4$ on a $2\ell+1 \leq e$ d'après le théorème (4.1). Par ailleurs on a $2\ell+1 \geq e$ d'après la proposition (3.1). Donc $2\ell+1 = e$. 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 $\bar{K}$ dans $\mathbb{F}_2$ est surjective ; il existe $u \in \mathcal{U}$ tel que la trace de la classe de u soit 1 dans $\mathbb{F}_2$. Alors $1+2u \in V_3 \setminus V_2$.

5. RESULTATS 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 $\delta(u) \geq e$ équivaut à $\delta(u) \geq e+1$. Soit $u \in \mathcal{U}$, et soit $n \in \mathbb{N}$ tel que $x = u\pi^n$ appartienne à A_2. Si $n \geq e$, $1-x$ 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 $a,b \in \mathcal{U}$ on obtient : $x = (a\pi^m)^2 + b\pi^{\delta(u)+2m}$; ce résultat implique $\delta(u) + 2m \geq e+1$. Pour tout $z \in \mathcal{U}$, 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'en-

tiers, donc que x est somme de trois carrés dans A. On a ainsi montré que $t(A) \leq 3$. L'égalité $t(A) = 3$ résultera des propositions qui suivent. ∎

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 $u \in \mathcal{U}$ 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 $u\pi^{2\ell}$ 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 $\mathcal{U}.\dot{K}^2$.

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

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

Ce qui donne :

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

La dernière assertion de la proposition (1.4) permet d'affirmer que $2\ell + \delta(u) \geq e+\ell$, c'est-à-dire $\ell \geq e-\delta(u)$. 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 $\varepsilon, v, w \in \mathcal{U}$ on a pour tout $x \in \mathcal{U}$:

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

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

$u' \in \mathcal{U}$ tel que $f(u') = 0$ et on a

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

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 :

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 $2\ell+1$ tel que $u\pi^{2\ell+1}$ 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 $2m+1 \geq e+1$;

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 $\delta(-1) + \delta(u) \geq 2e$, 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 :

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 $\ell \geq e$ $u\pi^\ell$ 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 $2n \geq e$, $u\pi^{2n}$ 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 $2\ell+1$ est le plus petit entier impair tel que $u\pi^{2\ell+1}$ soit somme de deux carrés dans A, il existe $a \in \mathcal{U}$, $b \in A$ tels que $u\pi^{2\ell+1} = a^2+b^2$, et on a $-1 = a^{-2}\{b^2-u\pi^{2\ell+1}\}$; on en conclut que $2\ell+1 = \delta(-1)$ 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 $\delta(u) \geq e$ 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 $\delta(u) \geq e$, 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 $a,b,c,d \in \mathcal{U}$ 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 $\delta(u) + 2n \geq e+n$, on a $e+n \leq \delta(-1)$, donc $2n \geq 2(e-\delta(u))$ et $\delta(-1) + \delta(u) \geq 2e$. Il suffit donc de montrer que $u\pi^{2(e-\delta(u))}$ est somme de deux carrés d'entiers. Or pour tout $y \in \mathcal{U}$ on a :

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

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 $y \in \mathcal{U}$. 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 $j \in \mathbb{N}$, $u\pi^j$ 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 $a,b,c,d \in \mathcal{U}$ 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 ■

5.4. Proposition.

On suppose e pair et $\delta(-1) = +\infty$, $(-1 \in \dot{K}^2)$. Soit $u \in \mathcal{U}$. 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 $u\pi^{2\ell}$ 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 (5.2). 2) La première assertion résulte encore de la proposition (3.1). En ce qui concerne la dernière assertion il existe $(a,b) \in \mathcal{U} \times A$ tel que : $-1 = (a^{-1}b)^2 - a^{-2}u\pi^{2n+1}$.

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