SÉMINAIRE DE THÉORIE DES NOMBRES DE BORDEAUX

JACQUES MARTINET

Sommes de carrés

Séminaire de théorie des nombres de Bordeaux (1970-1971), exp. n° 24, p. 1-9

<http://www.numdam.org/item?id=STNB_1970-1971____A24_0>

SOMMES DE CARRES

par

Jacques MARTINET

-:-:-:-

§. I. - GENERALITES SUR LES FORMES QUADRATIQUES

On supposera toujours que l'on travaille sur un corps qui n'est pas de caractéristique 2 ; les formes quadratiques que nous considérons sont toujours supposées non dégénérées.

Soit $Q(X_1, \ldots, X_n)$ une forme quadratique sur un corps K. On dit que Q représente $a \in K^*$ s'il existe $x_1, \ldots, x_n \in K$ tels que $Q(x_1, \ldots, x_n) = a$. On dit que Q représente 0 s'il existe $x_1, \ldots, x_n \in K$, non tous nuls, vérifiant $Q(x_1, \ldots, x_n) = 0$. On montre que si une forme Q représente 0, elle représente alors tout élément de K^* (voir par exemple J. P. Serre, cours d'arithmétique [8]).

Il résulte de cette propriété qu'une forme $Q = Q(X_1, X_2, \ldots, X_n)$ représente un élément $a \in K^*$ si et seulement si la forme $Q_a = Q(X_1, \ldots, X_n) - a X_o^2$ représente 0 ; en effet, si Q_a représente 0, il existe $x_o, x_1, \ldots, x_n \in K$, non tous nuls, avec $Q_a(x_o, x_1, \ldots, x_n) = 0$. Si $x_o \neq 0$, alors $a = Q(\frac{x_1}{x_o}, \ldots, \frac{x_n}{x_o})$. Si $x_o = 0$, alors Q représente 0, donc tout élément de K^*, et en particulier a.

Nous utiliserons aussi la remarque suivante : si la forme à quatre variables $Q = X^2 - aY^2 - bZ^2 + abT^2$ (où $a, b \in K^*$) représente 0, alors $X^2 - aY^2 - bZ^2$ représente 0. Cette remarque se rattache à la théorie des algèbres de quaternions. Soit $H = K_{a,b}$ l'algèbre définie par $i^2 = a$, $j^2 = b$, $ij = -ji = k$, d'où $k^2 = -ab$; la forme $X^2 - aY^2 - bZ^2 + abT^2$ est la norme réduite. On sait que H est centrale simple sur K, et est donc soit un corps gauche, soit l'algèbre de matrices $M_2(K)$; Q représente 0 si et seulement si $H \simeq M_2(K)$. Mais cela s'écrit (interprétation par les cocycles) $b \in N_{K(\sqrt{a})/K}[(K(\sqrt{a})^*)]$, ce qui signifie que $X^2 - aY^2 - bZ^2$ représente 0.

PROPOSITION 1. Si, dans K, -1 est somme de trois carrés, alors -1 est somme de deux carrés.

(En fait, on sait depuis Pfister [6] que le nombre minimum supposé fini de carrés nécessaire pour représenter -1 est une puissance de 2).

En effet, si -1 est somme de trois carrés, la forme $X^2 + Y^2 + Z^2 + T^2$ représente 0. La remarque précédente appliquée à $a = b = -1$ montre tout de suite que $X^2 + Y^2 + Z^2$ représente 0, donc que -1 est somme de deux carrés.

Dans la suite du paragraphe, on suppose que K est un corps de nombres. Rappelons que $a \in K^*$ est dit totalement positif (notation $a \gg 0$) si l'image de a dans tous les plongements réels de K est positive ; en particulier, dans un corps totalement imaginaire (i. e. les complétés aux places archimédiennes sont isomorphes au corps des complexes), tout nombre non nul est totalement positif. On dispose pour étudier les formes sur un corps de nombres du

THEOREME DE HASSE-MINKONSKI. Soit K un corps de nombres, et Q une forme quadratique non dégénérée à n variables, définie sur K. Alors, Q représente 0 dans K si et seulement si Q représente 0 dans tous les complétés de K.

Par ailleurs, si K' est une extension d'un corps p-adique $\mathbb{Q}_p$, on montre qu'une forme ayant $n \geq 5$ variables représente toujours 0. On a donc

le résultat supplémentaire suivant :

COMPLEMENT AU THEOREME DE HASSE-MINKONSKI. Une forme ayant au moins cinq variables représente 0 si et seulement si elle représente 0 dans tous les complétés réels de K .

Application aux sommes de carrés

PROPOSITION 2. Soit K un corps de nombres, $a \in K^*$. Les conditions suivantes sont équivalentes :

1) a est somme de carrés ;
2) a est somme de quatre carrés ;
3) a est totalement positif.

En effet, dire que a est somme de n carrés, avec $n \geq 4$, revient à dire que la forme quadratique à n+1 variables $aX_o^2 - X_1^2 - \ldots - X_n^2$ représente 0 dans K ; comme $n+1 \geq 5$, on regarde ce qui se passe aux places réelles, d'où le résultat.

PROPOSITION 3. Soit K un corps de nombres. Les conditions suivantes sont équivalentes :

1) -1 est somme de carrés ;
2) -1 est somme de quatre carrés ;
3) K est totalement imaginaire.

En effet, $-1 >> 0 \Leftrightarrow$ K totalement imaginaire.

§. II. - DEUX OU QUATRE CARRES ? REDUCTION AU CAS LOCAL

Si -1 est un carré dans K , il n'y a rien de plus à dire. Si on écarte ce cas, -1 est somme de deux ou quatre carrés. Problème : caractériser chacune de ces possibilités.

En fait, la réponse est connue des spécialistes depuis certainement longtemps, bien que la littérature soit muette à ce sujet, si bien que certains ont publié des réponses partielles (Chowla, Moser).

THEOREME 4. Soit K un corps de nombres totalement imaginiare, dans lequel -1 n'est pas un carré. Pour tout idéal premier $\mathfrak{p}$ de K, notons $e_{\mathfrak{p}}$ son indice de ramification absolu (si $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, $\mathfrak{p}^{e_{\mathfrak{p}}} | p\,O_K$, $\mathfrak{p}^{e_{\mathfrak{p}}+1} \nmid p\,O_K$, O_K désignant l'anneau des entiers de K) et $f_{\mathfrak{p}}$ son degré résiduel ($O_K/\mathfrak{p}$ est de degré $f_{\mathfrak{p}}$ sur $\mathbb{Z}/p\mathbb{Z}$).

Alors, -1 est somme de deux carrés dans K si et seulement si pour tout idéal $\mathfrak{p}$ au-dessus de 2, l'un des entiers $e_{\mathfrak{p}}$ ou $f_{\mathfrak{p}}$ est pair.

Par ailleurs, dire que -1 est somme de deux carrés dans K revient à dire que pour toute place v de K, -1 est somme de deux carrés dans le complété K_v de K en v. Cette condition est vérifiée pour les places v archimédiennes, car K_v est alors isomorphe au corps des complexes, et aussi pour les places finies $\mathfrak{p}$ au-dessus d'un nombre premier impair p : en effet, -1 est alors somme de deux carrés dans $\mathbb{Z}/p\mathbb{Z}$, donc aussi dans $\mathbb{Q}_p$ (lemme de Hensel), et donc aussi dans $K_{\mathfrak{p}}$ qui contient $\mathbb{Q}_p$ (variante : si $K' = K(i)$, avec $i^2 = -1$, -1 est somme de deux carrés dans K si et seulement si -1 est une norme dans K'/K ; cette condition se localise (théorème des normes de Hasse), et est vérifiée aux places impaires de K, car les extensions locales déduites de K'/K étant non ramifiées, toute unité est une norme). Comme le produit $e_{\mathfrak{p}}\,f_{\mathfrak{p}}$ est le degré local, on est ramené à prouver le

THEOREME 4 bis. Soit K une extension de degré fini du corps 2-adique $\mathbb{Q}_2$. Alors, -1 est somme de deux carrés dans K si et seulement si K est une extension de degré pair de $\mathbb{Q}_2$.

§. III. - LA METHODE DE LA RAMIFICATION SUPERIEURE (d'après G. Gras [3])

Dans ce paragraphe, K est une extension de $\mathbb{Q}_2$, dont on note e l'indice de ramification, f le degré résiduel, O_K l'anneau des entiers, $\mathfrak{p}_K$ l'idéal maximal (on a donc $2O_K = \mathfrak{p}_K^e$ et $[O_K/\mathfrak{p}_K : \mathbb{Z}_2/2\mathbb{Z}_2] = f$), U_K le groupe des unités, $U_K^{(i)} = \{x \in U_K \mid x-1 \in \mathfrak{p}_K^i\} = 1 + \mathfrak{p}_K^i$. On pose $L = K(i)$, avec $i^2 = -1$, et l'on définit de même O_L, U_L, $U_L^{(i)}$, $\mathfrak{p}_L$. Soit π une uniformisante de L ($\mathfrak{p}_L = \pi O_L$), et soit $\pi' = N_{L/K}(\pi)$ (on a $\mathfrak{p}_K = \pi' O_K$).

On note $\bar{K}$ et $\bar{L}$ les corps résiduels de K et L.

Enfin, $G = \{1, \sigma\}$ désigne le groupe de Galois de L/K (si $L \neq K$), et G_i désigne la suite des groupes de ramification dans G ($\sigma \in G_i \Leftrightarrow \forall x \in O_L$, $x - \sigma x \in \mathfrak{p}_L^i$). Remarquons que si $L = K$, $K \supset Q_2(i)$; par conséquent, lorsque -1 est un carré dans K, $[K : Q_2]$ est pair. On supposera dans la suite $[L : K] = 2$.

L'extension L/K est alors ramifiée, et $\bar{L} = \bar{K}$.

Soit t l'entier vérifiant $G_t = G$, $G_{t+1} = \{1\}$. On vérifie que $1 \leq t \leq e$. Nous posons en outre, $\omega = \frac{2}{\pi'^e}$, $\theta = \frac{\sigma\pi}{\pi}$ et $\varphi = \frac{\theta - 1}{\pi^t}$; alors, $\varphi \in U_L$. On vérifie que $\mathrm{Tr}_{L/K}(\pi^t) = b\pi'^t$, avec $b \in U_L$, et l'on montre que $\bar{b} = \bar{\varphi}^2$ ($\bar{x}$ désigne l'image dans $\bar{K} = \bar{L}$ de $x \in O_L$).

L'étape importante de la démonstration est le

LEMME. <u>Soit</u> $\Omega = -\omega\pi'^{e-t}$. <u>Alors</u>, -1 <u>est somme de deux carrés dans</u> K <u>si et seulement si</u> $X^2 + \bar{b}X + \bar{\Omega}$ <u>a une racine dans</u> $\bar{K}$.

<u>Preuve du lemme</u> - Soit $N_t : U_L^{(t)}/U_L^{(t+1)} \to U_K^{(t)}/U_K^{(t+1)}$ l'application déduite naturellement de la norme. On sait ([7], chapitre V) que $U_K/N(U_L)$ est canoniquement isomorphe à $\mathrm{coker}\ N_t$, et que, en identifiant $U_L^{(t)}/U_L^{(t+1)}$ et $U_K^{(t)}/U_K^{(t+1)}$ à $\bar{K}$, N_t associe à $\bar{U} \in \bar{K}$ l'élément $\bar{b}\bar{U} + \bar{U}^2$ de $\bar{K}$. Alors, comme $-1 = 1 + \Omega \cap t$, $-1 \in N_{L/K}(U_L)$ si et seulement si $X^2 + \bar{b}X + \bar{\Omega}$ a une racine dans $\bar{K}$.

On vérifie que $\bar{\Omega} = 0$ si e est pair. Dans ce cas, -1 est bien somme de deux carrés dans K. Si au contraire e est impair, on trouve $\bar{\Omega} = \bar{\varphi}^2$. La subtitution $X \to \bar{\varphi}X$ transforme alors $X^2 + \bar{b}\bar{X} + \bar{\Omega}$ en $X^2 + X + 1$, et ce polynôme, étant irréductible sur $\mathbb{Z}/2\mathbb{Z}$, a une racine dans K si et seulement si le degré de $\bar{K}$ sur $\mathbb{Z}/2\mathbb{Z}$ est pair.

§. IV. - INVARIANTS LOCAUX ATTACHES A UNE ALGEBRE CENTRALE SIMPLE

Soit K un corps ; une K-algèbre (de dimension finie) A est dite simple si elle ne possède pas d'idéaux bilatères non triviaux. Rappelons qu'une telle algèbre est isomorphe à un anneau de matrice sur un corps gauche D ($A \simeq M_r(D)$) et que le rang de D sur son centre est un carré.

Une K-algèbre est dite centrale si son centre est K . On montre que, si A et B sont centrales simples sur K , $A \otimes_K B$ est centrale simple, et que, pour toute extension L de K , $A_L = A \otimes_K L$ est une L-algèbre centrale simple.

Soit maintenant K un corps local (K est un corps complet pour une valuation discrète, à un corps résiduel $\bar{K}$ fini), O_K son anneau de valuation, M_K l'idéal de O_K , et D un corps gauche de centre K , de rang d^2 sur K . On montre (par exemple [7]) que D possède un sous-corps commutatif maximal L ($[L : K] = d$), non ramifié sur K . Le groupe de Galois G de L/K est cyclique ; soit σ son générateur de Frobenius (si card $\bar{K} = q$, on a $\sigma x \equiv x^q$ modulo M_K pour tout $x \in O_L$). Il existe un élément $e \in D^*$, pour lequel, quel que soit $x \in L$, on a $exe^{-1} = \sigma x$. Les éléments $1, e, \ldots, e^{d-1}$ forment une base de D sur L (indépendance linéaire des automorphismes de L). Comme e^n commute avec tous les éléments de cette base et avec tous les éléments de L , $e^n \in K^*$. De plus, on voit facilement que l'image de e^n dans $K^*/N_{L/K}(L^*)$ ne dépend pas du choix de e . Mais $K^*/N_{K/L}(L^*)$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, lui-même isomorphe au sous-groupe $1/n\mathbb{Z}/\mathbb{Z}$ de $\mathbb{Q}/\mathbb{Z}$. En s'inspirant de ces remarques, on peut associer à toute algèbre centrale simple A sur un corps local, un invariant i(A) à valeurs dans $\mathbb{Q}/\mathbb{Z}$.

Cet invariant jouit des propriétés suivantes :

(i) si A est un corps gauche de centre K , de rang d^2 sur K , $d\,i(A) \equiv 0 \mod \mathbb{Z}$.

(ii) Si $A \simeq M_r(D)$ et $A' \simeq M_{r'}(D')$ sont deux K-algèbres centrales simples, $i(A) = i(A') \Leftrightarrow D \simeq D'$.

(iii) Si A et A' sont deux K-algèbres centrales simples,

$$i(A \otimes_K B) = i(A) + i(B) .$$

(iv) $i(A) = 0 \Leftrightarrow A$ est une algèbre de matrices sur K .

(v) Si L est une extension finie de K , $i(A \otimes_K L) = [L : K] i(A)$.

La considération de cet invariant local permet de résoudre sans difficulté le problème de la représentation de -1 comme sommes de deux carrés dans un corps de nombres. On est tout de suite ramené à résoudre ce problème, lorsque K est une extension du corps 2-adique $\mathbb{Q}_2$ (énoncé du théorème 4 bis). Dire que -1 est somme de deux carrés dans K revient à dire que la forme quadratique $X^2 + Y^2 + Z^2 + T^2$ représente 0 dans K . Soit alors H l'algèbre de quaternions sur $\mathbb{Q}_2$, de base 1 , i , j , k, avec $i^2 = j^2 = -1$, $ij = -ji = k$. La $\mathbb{Q}_2$-algèbre H est un corps gauche de rang 2^2 sur $\mathbb{Q}_2$. L'invariant $i(H)$ vaut donc $1/2$ (on a $2i(H) = 0$, et $i(H) \neq 0$ d'après (iv)). Soit $H_K = H \otimes_{\mathbb{Q}_2} K$. Dire que $X^2 + Y^2 + Z^2 + T^2$ représente 0 dans K revient à dire que H_K possède des diviseurs de 0 , donc est une algèbre de matrices sur K . Par conséquent, -1 est somme de deux carrés dans K si et seulement si $i(H_K) = 0 \mod \mathbb{Z}$.

Comme $i(H_K) = [K : \mathbb{Q}_2]\, i(H)$, (v) , on obtient une démonstration rapide du théorème 4 bis.

§. V. - PROBLEMES SUR LES ENTIERS

La considération des corps de quaternions permet parfois de résoudre des problèmes de représentations d'entiers par des formes quadratiques. Ainsi, en vérifiant que le sous-anneau A de H de base sur $\mathbb{Z}$ 1 , i , j , $\frac{1+i+j+k}{2}$ a tous ses idéaux à gauche principaux, on montre que tout entier positif n peut se représenter sous la forme $n = \frac{x^2 + y^2 + z^2 + t^2}{4}$, avec x , y , z , t entiers ; de-là, il est facile d'arriver au théorème des quatre carrés. Mais on peut aussi obtenir des résultats sur les formes à trois variables. A titre d'exemple, démontrons le

THEOREME DES TROIS CARRES. Un entier positif m est somme de trois carrés entiers si et seulement si m n'est pas de la forme $4^a(8k+7)$.

Des remarques élémentaires sur les congruences prouvent que $4^a(8k+7)$ n'est pas somme de trois carrés dans $\mathbb{Q}$. Il suffit de prouver que si m est un entier positif, sans facteur carré non congru à -1 modulo 8, alors m est somme de trois carrés dans $\mathbb{Z}$.

On vérifie que la forme quadratique $mX^2 - Y^2 - Z^2 - T^2$ représente 0 localement partout : c'est trivial à chaque place p impaire ($X^2+Y^2+Z^2$ représente 0 modulo p) et à l'infini ; c'est vrai sur $\mathbb{Q}_2$ grâce à la condition $m \not\equiv -1$ modulo 8. On peut donc écrire $m = a^2+b^2+c^2$, avec $a, b, c \in \mathbb{Q}$. Il résulte de cette remarque que $\mathbb{Q}(\sqrt{-m})$ est isomorphe à un sous-corps de H (par exemple à $\mathbb{Q}(ai+bj+ck)$). Notons q' le quaternion $ai+bj+ck$. Soit A' un ordre maximal contenant q'. Comme les idéaux à gauches de A sont tous principaux, A' et A sont des ordres conjugués i.e. : il existe $x \in H^*$, tel que $A' = xAx^{-1}$. Soit $q = x^{-1}q'x$. Alors, $q \in A$. On peut donc écrire $q = \alpha+\beta i+\gamma j+\delta k$, où $2\alpha, 2\beta, 2\gamma, 2\delta$ sont les entiers de même parité. Mais la trace réduite de q' est nulle. Il en est donc de même de celle de q. Par conséquent, $\alpha = 0$, et β, γ, δ sont entiers. La norme réduite de q est égale à $\beta^2+\gamma^2+\delta^2$ d'une part, et à la norme réduite de q' d'autre part. Mais cette dernière n'est autre que m. C. Q. F. D.

On montrerait de même en considérant le corps de quaternions de base sur $\mathbb{Q}$ $1, i, j, k$ avec $i^2 = -1$, $j^2 = -3$, $ij = -ji = k$ qu'un entier positif est représenté par la forme $x^2+y^2+3z^2$ si et seulement si il n'est pas de la forme $9^a(9k+6)$.

Pour un procédé basé sur les classes de formes quadratiques, voir Mordell ([4], chapitre 20).

-:-:-:-

BIBLIOGRAPHIE

[1] S. CHOWLA. - On the representation of -1 as a sum of squares in a cyclotomic field. J. of Number Theory 1 (1969) p. 208-210.

[2] P. et S. CHOWLA. - Determination of the Stufe of certain cyclotomic fields. J. of Number Theory 2 (1970) p. 271-272.

[3] G. GRAS. - Note sur la représentation de -1 comme somme de carrés dans un corps de nombres. Grenoble (1971) (non publié).

[4] MORDELL. - Diophantine equations. Academic Press (1969).

[5] C. MOSER. - Représentation de -1 par une somme de carrés dans certains corps locaux et globaux et dans certains anneaux d'entiers algébriques. C. R. A. S., Paris, t. 271, (1970) p. 1200-1203.

[6] A. PFISTER. - Zur Darstellung von -1 als Summe von Quadraten in einen Körper. J. Lond. Math. Soc. 40 (1965) p. 159-165.

[7] J. P. SERRE. - Corps locaux. Hermann, Paris (1962).

[8] J. P. SERRE. - Cours d'arithmétique.

-:-:-:-

Jacques MARTINET
U. E. R. de Mathématiques
et d'Informatique
Université de Bordeaux 1
351, cours de la Libération
33 - T A L E N C E