7. Applications

forme quadratique f comme $f \simeq <1> \oplus f'$. Alors $k(f) = F(\sqrt{-f'(X')})$, où $X' = (X_2, \ldots, X_m)$ et $F = k(X')$. Supposons $q_{k(f)}$ isotrope. Alors par [4], 2.5.1, on a:

$$q_F \simeq a <1, f'(X')> \oplus q' \simeq <a> \oplus q'' .$$

Donc $a \in D(q_F) \subset D_m(q)$.

D'autre part, $<1, f'(X')>$ représente f sur $F(X_1) = k(X_1, \ldots, X_m)$. Donc $a <1, f'(X')>$ représente af sur $k(X_1, \ldots, X_m)$. On en déduit que $af \in D_m(q)$. Comme $a \in D_m(q)$, on a $f \in <D_m(q)>$.

7. Applications

Voici quelques applications du théorème 1:

Sommes de carrés

Corollaire 1. *Soit s un entier positif. Si un polynôme $f \in k[X_1, \ldots, X_m]$ est une somme de 2^s carrés dans $k(X_1, \ldots, X_m)$, alors tout polynôme irréductible et unitaire divisant f avec un exposant impair est une somme de 2^s carrés dans $k(X_1, \ldots, X_m)$.*

Soit q la forme quadratique somme de 2^s carrés. Alors q est une forme de Pfister, donc $D(q) = <D(q)>$ (cf. [4], chap. 2, § 10 ou [3], chap. 10, cor. 1.7). Le corollaire découle de l'implication $a) \Rightarrow b)$ du théorème 1, appliqué au produit des polynômes irréductibles divisant f avec un exposant impair.

Le cas $m = 1$ de ce corollaire est dû à Kaplansky (cf. [4], chap. 10, cor. 2.10).

Principe de Hasse

Soit k un corps de nombres. On note v une place (finie ou infinie) de k, et k_v le complété de k en v. Soit q une forme quadratique anisotrope sur k.

Corollaire 2. *Soit $f \in k[X]$. Alors*

$$f \in <D(q_{k_v(X)})> \text{ pour toute place } v \text{ de } k \Leftrightarrow f \in <D(q_{k(X)})> .$$

Il est clair que $f \in <D(q_{k(X)})> \Rightarrow f \in <D(q_{k_v(X)})>$ pour toute place v de k.

Montrons la réciproque. Par le théorème de Hasse-Minkowski (voir par exemple [4], chap. 6, §6, cor. 6.6 a)), si $a \in k$ est tel que $a \in D(q_{k_v})$ pour toute place v de k, alors $a \in D(q)$. Donc, par la partie $a) \Rightarrow b)$ du théorème 1, on peut supposer que f est irréductible et unitaire.

Supposons que $f \in \langle D(q_{k_v(X)}) \rangle$ pour toute place v de k. Alors la partie $b) \Rightarrow c)$ du théorème 1 implique que $q_{k_v(f)}$ est isotrope pour toute place v de k. Par le théorème de Hasse-Minkowski (cf. [4], chap. 6, §6, th. 6.5), on en déduit que $q_{k(f)}$ est isotrope. Donc, par la partie $c) \Rightarrow b)$ du théorème 1, $f \in D(q_{k(X)})$.

Une variante du nombre de Pythagore

Pour tout corps F et pour tout entier $n \geqslant 1$, on note $D_F(n) \subset F^*/F^{*2}$ l'ensemble des sommes de n carrés d'éléments de F, et $\langle D_F(n) \rangle$ le sous-groupe de F^*/F^{*2} engendré par $D_F(n)$.

Lorsque $F = k(X_1, \ldots, X_m)$, on note $D_m(n) = D_F(n)$.

Rappelons que le *niveau* d'un corps F, noté $s(F)$, est par définition le plus petit entier s tel que $-1 \in D_F(s)$. Si -1 n'est pas une somme de carrés dans F, alors on pose $s(F) = \infty$, et l'on dit que F est *formellement réel.*

COROLLAIRE 3. *Supposons que k soit formellement réel. Soit $f \in k[X_1, \ldots, X_m]$ un polynôme irréductible et unitaire. Alors*

$$f \in \langle D_m(n) \rangle \Leftrightarrow s(k(f)) < n .$$

Soit q la forme quadratique somme de n carrés. Comme k est formellement réel, q est anisotrope. Il est clair que

$$s(k(f)) < n \Leftrightarrow q_{k(f)} \text{ isotrope .}$$

Par le corollaire du théorème 1, on a

$$q_{k(f)} \text{ isotrope } \Leftrightarrow f \in \langle D_m(n) \rangle .$$

Ceci démontre le corollaire.

Soit $D_F(\infty) = \bigcup_{n=1}^{\infty} D_F(n)$. Le *nombre de Pythagore $p(F)$* de F est le plus petit entier n tel que $D_F(n) = D_F(\infty)$. S'il n'existe aucun entier avec cette propriété, alors on pose $p(F) = \infty$.

Notation. On note $p'(F)$ le plus petit entier n tel que $\langle D_F(n) \rangle = D_F(\infty)$. S'il n'existe aucun entier avec cette propriété, alors on pose $p'(F) = \infty$.

COROLLAIRE 4. *Supposons que* k *soit formellement réel, et que* $m \geqslant 1$. *Alors* $p'(k(X_1, \ldots, X_m)) = \sup\{s(k(f)) + 1, f \in k[X_1, \ldots, X_m]$ *unitaire et irréductible, avec* $s(k(f)) < \infty\}$.

Démonstration. Posons

$$p' = p'(k(X_1, \ldots, X_m)),$$

$$p'' = \sup\{s(k(f)) + 1, f \in k[X_1, \ldots, X_m] \text{ unitaire et irréductible, avec } s(k(f)) < \infty\}.$$

Soit $f \in k[X_1, \ldots, X_m]$ irréductible et unitaire. Si $f \in \langle D_m(n) \rangle$, alors par le corollaire 3 on a $s(k(f)) < n$. Donc $p'' \leqslant p'$. Réciproquement, si $s(k(f)) < n$ alors par le corollaire 3 $f \in \langle D_m(n) \rangle$ pour tout polynôme irréductible et unitaire de $k[X_1, \ldots, X_m]$. Pour montrer que $p' \leqslant p''$, il reste donc à démontrer que $p'(k) \leqslant p''$. Soit $d \in k^*$ une somme de carrés, $d \notin k^{*2}$. Posons $f(X) = X^2 + d \in k[X]$. Alors f est un polynôme unitaire et irréductible. On a $k(f) = k(\sqrt{-d})$. Supposons que $s(k(f)) = n$. Alors il existe $a_1, \ldots, a_n, b_1, \ldots, b_n \in k$ tels que $-1 = (a_1 + b_1\sqrt{-d})^2 + \ldots + (a_n + b_n\sqrt{-d})^2$. Alors $-1 = a_1^2 + \ldots + a_n^2 - d(b_1^2 + \ldots + b_n^2)$. Donc $d(b_1^2 + \ldots + b_n^2)^2 = (a_1^2 + \ldots + a_n^2 + 1) \cdot (b_1^2 + \ldots + b_n^2)$. Ceci entraîne que $d \in \langle D_k(n+1) \rangle$.

En utilisant des résultats de Colliot-Thélène et Jannsen [1], on obtient

COROLLAIRE 5. *Soient* k *un corps de nombres réel,* X, Y *et* Z *des variables. Alors*

a) $p'(k(X)) = 2, 3$ *ou* 5;

b) $p'(k(X, Y)) = 2, 3$ *ou* 5;

c) $p'(k(X, Y, Z)) = 2, 3, 5$ *ou* 9.

En effet, par [1], th. 4.1, (b) et (c), on voit que $s(k(f)) = 1, 2, 4$ ou ∞ si f est un polynôme irréductible et unitaire de $k[X]$ ou $k[X, Y]$ et $s(k(f)) = 1, 2, 4, 8$ ou ∞ si f est un polynôme irréductible et unitaire de $k[X, Y, Z]$. Par le corollaire précédent, ceci démontre l'affirmation.

Le corollaire ci-dessus et les résultats et conjectures de [1] suggèrent la conjecture suivante:

CONJECTURE. *Soit* k *un corps de nombres réel, et soient* $X_1, \ldots, X_m$ *des variables,* $m \geqslant 4$. *Alors* $p'(k(X_1, \ldots, X_m))$ *est de la forme*

$$p'(k(X_1, \ldots, X_m)) = 2^r + 1,$$

où $r \in \{0, \ldots, m\}$.

Finalement, remarquons que le cas des corps de nombres totalement imaginaires est beaucoup plus simple :

PROPOSITION. *Soit* k *un corps de nombres totalement imaginaire. Alors*

$$p'(k(X_1, \ldots, X_m)) = 2, 3 \quad ou \quad 5\ ,$$

quel que soit $m \geqslant 1$.

En effet, si k est totalement imaginaire, alors $s(k) = 1, 2$ ou 4 (voir par exemple [4], chap. XI). Comme tout élément d'un corps de caractéristique différente de 2 peut s'écrire comme différence de deux carrés, on a $p(k(X_1, \ldots, X_m)) \leqslant 5$, quel que soit m. Le lemme suivant montre que si $p(k(X_1, \ldots, X_m)) = 4$, alors $p'(k(X_1, \ldots, X_m)) \leqslant 3$. Ceci démontre la proposition.

LEMME. *Soit* F *un corps de caractéristique différente de* 2. *Alors*

$$D_F(4) \subset D_F(3) \, . \, D_F(3) \subset \langle D_F(3) \rangle \ .$$

Soit $H = (-1, -1)$ l'algèbre de quaternions de Hamilton sur F. Soit H' le sous-groupe additif des quaternions purs de H. Notons N la norme réduite. Alors $N(H) = D_F(4)$, $N(H') = D_F(3)$. Pour démontrer le lemme, il suffit donc de vérifier que pour tout $a \in H$, il existe $b \in H'$ tel que $ab \in H'$. Mais cette condition consiste en une équation linéaire en trois variables, laquelle a toujours une solution.

BIBLIOGRAPHIE

[1] COLLIOT-THÉLÈNE, J.-L. et U. JANNSEN. Sommes de carrés dans les corps de fonctions. *C. R. Acad. Sci. Paris 312* (1991), 759-762.

[2] GILLE, Ph. R-équivalence et principe de norme en cohomologie galoisienne. *C. R. Acad. Sci. Paris 316* (1993), 315-320.

[3] KNEBUSCH, M. Specialization of quadratic and symmetric bilinear forms, and a norm theorem. *Acta Arithmetica 24* (1973), 279-299.

[4] LAM, T.Y. *Algebraic Theory of Quadratic Forms.* Benjamin (1973).

[5] MERKURJEV, A. Norm principle for algebraic groups. *Journal Algebra and Analysis,* à paraître.

[6] —— R-equivalence on adjoint classical groups. Notes manuscrites, octobre 1993.

[7] SCHARLAU, W. *Quadratic and Hermitian Forms.* Grundlehren Math. Wiss 270, Springer-Verlag (1985).