BULLETIN DE LA S. M. F.

JEAN-RENÉ TORT

Sur deux invariants d'un corps de niveau fini

Bulletin de la S. M. F., tome 106 (1978), p. 161-168
<http://www.numdam.org/item?id=BSMF_1978__106__161_0>

Bull. Soc. math. France,
106, 1978, p. 161-168.

SUR DEUX INVARIANTS D'UN CORPS DE NIVEAU FINI

PAR

JEAN-RENÉ TORT
[Université de Pau]

RÉSUMÉ. — Afin de minorer le nombre de classes modulo un carré dans un corps non formellement réel, D. Z. DJOKOVIĆ pose le problème de la détermination de la longueur minimale d'une partition d'un graphe en cliques. Dans une première partie, cet article donne, à l'aide de nouveaux invariants, un caractère plus intrinsèque au résultat de DJOKOVIĆ. Dans une seconde partie, le problème est résolu dans un cas particulier et, pour terminer les graphes associés au corps des nombres 2-adiques sont construits.

ABSTRACT. — Looking for a lower bound for the number of square classes in a non formally real field, D. Z. DJOKOVIĆ was led to the problem of estimating the minimal length of partitions in cliques of a graph. The first part of this paper introduces new invariants which are used to give a more intrinsic form to DJOKOVIĆ's result. In a second part, the problem is solved in a special case. Finally, the graphs associated with the Q_2-field are constructed as an illustrative example.

1. Introduction

Soit K un corps de caractéristique différente de 2, non formellement réel, de niveau $s = 2^k$, q le nombre de classes des éléments de K^* modulo 1 carré. Dans [6], PFISTER a d'abord montré que $q \geqslant 2^{k\,(k+1)/2}$, puis CHANG [2], a prouvé que $q \geqslant 16.(2^s/s^2)$ si $s > 8$. D. Z. DJOKOVIĆ, [3], a démontré que $q \geqslant 2^{s+1}/s$ pour $s \geqslant 2$. Pour obtenir ce résultat, il a été amené à définir un graphe dont il s'agit de trouver la longueur minimale d'une partition en cliques. Le but de cet article est de donner, à l'aide de la définition de nouveaux invariants du corps, un caractère plus intrinsèque au résultat de DJOKOVIĆ. Dans une seconde partie, nous calculons cette longueur dans un cas particulier, ce qui améliore la minoration correspondante de DJOKOVIĆ. Enfin, pour terminer, nous étudions les graphes associés aux valeurs 1 et 2 de s, et nous considérons les graphes associés au corps des nombres 2-adiques qui est l'un des corps les plus simples de niveau 4.

2. Les invariants $q_i(K)$

Dans tout ce qui suit, K est un corps non formellement réel, de caractéristique différente de 2, de niveau s, et de nombre de classes modulo 1 carré q fini. Nous utiliserons ici les notations de T. Y. LAM, [4], à savoir : pour tout entier m, $D_K(m) = D_m(m\langle 1 \rangle)$ est l'ensemble des éléments de K^* sommes de m carrés. On a alors dans K^* une « filtration » :

$$D_K(1) \subset D_K(2) \subset \ldots \subset D_K(s+1) = K^*,$$

$D_K(s+1) = K^*$ car, pour tout x de K^*, on a

$$x = \left(\frac{x+1}{2}\right)^2 - \left(\frac{x-1}{2}\right)^2,$$

et -1 est somme de s carrés.

En fait, d'après PFISTER [5], une véritable filtration du groupe multiplicatif K^* est

$$D_K(1) \subset D_K(2) \subset \ldots \subset D_K(2^t) \subset \ldots \subset D_K(s) \subset K^*.$$

D'où la définition suivante.

DÉFINITION 1. — Pour tout i, i variant de 1 à $s+1$, nous noterons $q_i(K)$ le nombre des classes dans K^*/K^{*2} d'éléments de $D_K(i)$. Par définition, nous avons

$$q_1(K) \leqslant q_2(K) \leqslant \ldots \leqslant q_i(K) \leqslant \ldots \leqslant q_{s+1}(K) = q.$$

Soit K un corps non formellement réel dont le niveau est s, et

$$-1 = \alpha_1^2 + \alpha_2^2 + \ldots + \alpha_s^2$$

une écriture de -1 comme somme de s carrés, on a alors $0 = \alpha_0^2 + \alpha_1^2 + .. + \alpha_s^2$ avec $\alpha_0 = 1$. Soit maintenant $S = \{0, 1, \ldots, s\}$ et, pour tout I contenu dans S, $\alpha_I = \sum_{j \in I} \alpha_j^2$ avec $\alpha_\Phi = \alpha_S = 0$. Considérons alors J, appartenant à $\mathscr{P}_{i+1}(S)$ (ensemble des parties de S à $i+1$ éléments), par définition, $\alpha_J \in D_K(i+1)$. De plus, α_J n'appartient pas à $D_K(i)$, car sinon le niveau de K serait inférieur à s. Soient I et J deux éléments de $\mathscr{P}_{i+1}(S)$ tels que card $(I-J)$ soit supérieur ou égal à 2, l'on sait alors, d'après CHANG [2], que α_I et α_J n'appartiennent pas à la même classe modulo 1 carré. Afin de savoir ce qui se passe lorsque les éléments I et J de $\mathscr{P}_{i+1}(S)$ sont tels que card $(I-J) = 1$, DJOKOVIĆ a défini le graphe $\Gamma_{s,\, i+1}$.

3. Le graphe $\Gamma_{s,\,i}$ et ses partitions en cliques

DÉFINITIONS 2. — $\Gamma_{s,\,i}$, pour i variant de 1 à s, est le graphe dont les sommets sont les éléments de $\mathscr{P}_i(S)$ dans lequel deux sommets I et J sont reliés si, et seulement si, card $(I-J) = 1$.

$\mathscr{O}(\Gamma_{s,\,i})$ sera l'ordre de $\Gamma_{s,\,i}$ c'est-à-dire le nombre de sommets du graphe.

Type d'une clique : Soit C une clique (sous-graphe complet) de $\Gamma_{s,\,i}$ de cardinal supérieur ou égal à 3; I, J, K trois sommets de C. Comme nous devons avoir card $(I-J) =$ card $(I-K) =$ card $(J-K) = 1$, deux seules possibilités existent :

(α) il existe T, élément de $\mathscr{P}_{i+1}(S)$, tel que

$$I \subset T, \qquad J \subset T, \qquad K \subset T;$$

(β) il existe R, élément de $\mathscr{P}_{i-1}(S)$, tel que

$$R \subset I, \qquad R \subset J, \qquad R \subset K.$$

Dans le cas (α) (resp. (β)), nous dirons que C est une clique de type 1 (resp. de type 2). Si C est une clique de cardinal inférieur ou égal à 2, nous dirons que C est de type indéterminé.

Base d'une clique : Soit C une clique telle que card $C \geqslant 3$ de type 1 (resp. de type 2), engendrée par $T \in \mathscr{P}_{i+1}(S)$ (resp. $R \in \mathscr{P}_{i+1}(S)$), nous dirons que T (resp. R) est la base de C.

Longueur minimale d'une partition en cliques de $\Gamma_{s,\,i}$: Nous désignerons par $t(P)$ la longueur d'une partition P de $\Gamma_{s,\,i}$ en cliques, et nous poserons $T(s, i) = \inf[t(P)]$.

4. Étude de $T(s, i)$ et applications

Par définition, $\Gamma_{s,\,s}$ et $\Gamma_{s,\,1}$ sont des graphes complets, donc $T(s, s) = T(s, 1) = 1$.

THÉORÈME 1. — *Soit K un corps non formellement réel dont le niveau s est fini. Alors, pour tout i variant de* 1 *à* $s-1$, *on a*

$$q_{i+1}(K) - q_i(K) \geqslant T(s, i+1).$$

Démonstration. — Nous avons vu plus haut que si I et J sont deux éléments de $\mathscr{P}_{i+1}(S)$ et que, si α_I et α_J sont dans la même classe, alors card $(I-J) = 1$, et donc les sommets I et J sont adjacents dans $\Gamma_{s,\,i+1}$. On réalise alors une partition de l'ensemble des sommets de $\Gamma_{s,\, i+1}$ de telle manière que deux sommets I et J appartiennent à la même partie si, et seulement si, α_I et α_J sont dans la même classe. Si $(C_i)_{i=1,\, \ldots,\, n}$ est la partition, par construction, chaque C_k, k variant de 1 à n, est une clique de $\Gamma_{s,\, i+1}$. Par suite, les α_J, pour J dans $\mathscr{P}_{i+1}(S)$, appartiennent à un nombre de classes supérieur à la longueur d'une partition de $\Gamma_{s,\, i+1}$ en cliques, et donc

$$q_{i+1}(K)-q_i(K) \geqslant T(s,\, i+1) \qquad \text{pour} \quad 1 \leqslant i \leqslant s-1.$$

THÉORÈME 2. — *Pour tout i variant de* 1 *à* $s+1$, *on a*

$$T(s,\, i) = T(s,\, s+1-i).$$

Démonstration. — Soit (C_k), k variant de 1 à $t(P)$, une partition P de $\Gamma_{s,\, i}$ en cliques. Posons $C_k = \{ I_{k_1}, \ldots, I_{k_r};\ I_{k_j} \in \mathscr{P}_i(S) \}$. Par passage au complémentaire sur les sommets I_{k_j}, on obtient la clique

$$D_k = \{ S-I_{k_1}, \ldots, S-I_{k_r} \} \quad \text{de } \Gamma_{s,\, s+1-i}.$$

L'ensemble des D_k, k variant de 1 à $t(P)$, constitue une partition en cliques de $\Gamma_{s,\, s+1-i}$ de longueur $t(P)$, et par suite $T(s,\, s+1-i) \leqslant T(s,\, i)$. Mais l'opération étant symétrique, on en déduit aussi l'inégalité dans l'autre sens, et par suite $T(s,\, i) = T(s,\, s+1-i)$.

COROLLAIRE. — *Soit K un corps non formellement réel dont le niveau s est fini, q le cardinal de K^*/K^{*2}*; alors :

$$q = \textstyle\sum_{i=1}^{s} [q_{i+1}(K)-q_i(K)]+q_1(K)$$

et, pour $s \geqslant 2$:

$$q \geqslant 2[\textstyle\sum_{i=1}^{s/2} T(s,\, i)].$$

Démonstration. — On a

$$q = q_{s+1}(K) = \textstyle\sum_{i=1}^{s} [q_{i+1}(K)-q_i(K)]+q_1(K).$$

D'où

$$q = q_{s+1}(K)-q_s(K)+\textstyle\sum_{i=1}^{s-1} [q_{i+1}(K)-q_i(K)]+q_1(K)$$

et donc

$$q \geqslant \textstyle\sum_{i=1}^{s-1} [q_{i+1}(K)-q_i(K)]+q_1(K).$$

Or $q_1(K) = 1 = T(s,\, 1)$ et, d'après le théorème 1, pour i variant de 1 à $s-1$, $q_{i+1}(K)-q_i(K) \geqslant T(s,\, i+1)$, d'où

$$q \geqslant \textstyle\sum_{i=1}^{s-1} T(s,\, i+1)+T(s,\, 1) = \textstyle\sum_{i=1}^{s} T(s,\, i).$$

Or on sait (Pfister) que, si K est un corps non formellement réel, s est une puissance de 2; donc, avec le théorème 2, on a, pour $s \geqslant 2$,

$$q \geqslant 2\left[\sum_{i=1}^{s/2} T(s, i)\right].$$

Détermination de $T(s, 2)$.

Théorème 3. — *On a* $T(s, 2) = s-1$ *pour* $s \geqslant 2$.

Démonstration. — Soit

$$C_i = \{\{i, j\};\ i+1 \leqslant j \leqslant s\} \qquad \text{pour} \quad i \text{ variant de } 0 \text{ à } s-3,$$

$$C_{s-2} = \{\{s-2, s-1\}, \{s-2, s\}, \{s-1, s\}\}.$$

Alors $(C_i)_{i=0, \ldots, s-2}$ est une partition de $\Gamma_{s, 2}$ en cliques, et par suite

$$T(s, 2) \leqslant s-1.$$

Nous allons maintenant démontrer, par récurrence sur s, que $T(s, 2) = s-1$. Pour $s = 2$, $\Gamma_{2, 2} = \{ \{ 0, 1 \}, \{ 0, 2 \}, \{ 1, 2 \} \}$, et par suite $T(2, 2) = 1$. Supposons donc que

$$T(k, 2) = k-1 \qquad \text{si} \quad k > 2.$$

Soit maintenant $(A_i)_{i=1, \ldots, n}$ une partition de $\Gamma_{k+1, 2}$ de longueur minimale, nous avons $n \leqslant k$. Dans cette partition figure au moins une clique de type 2, car sinon toutes les cliques seraient de type 1 ou indéterminé et donc, pour tout i, card $A_i \leqslant 3$. D'où

$$\sum_{i=1}^{n} \operatorname{card} A_i \leqslant 3\,k < \mathcal{O}(\Gamma_{k+1, 2}).$$

Soit donc A_1 cette clique, nous pouvons supposer, à l'aide d'une bijection, que $\{ k+1 \}$ en est la base. Définissons alors $(B_i)_{i=1, \ldots, n}$ de la façon suivante :

$$B_1 = \{\{k+1, y\};\ y = 0, \ldots, k\},$$

$$B_i = A_i - \{\{k+1, y\};\ \{k+1, y\} \in A_i\} \qquad \text{pour} \quad i \geqslant 2.$$

On obtient ainsi une nouvelle partition de $\Gamma_{k+1, 2}$ de longueur n et telle que card $B_1 = k+1$. De plus, aucun élément $\{ x, k+1 \}$ ne figure dans les B_i pour $i \geqslant 2$, et donc $(B_j)_{j=2, \ldots, n}$ constitue une partition de $\Gamma_{k, 2}$. Par hypothèse de récurrence, il nous faut donc $n-1 \geqslant k-1$, d'où $n \geqslant k$, et donc $T(k+1, 2) = k$.

Comme conséquence immédiate des théorèmes 1 et 3 nous avons le corollaire suivant.

COROLLAIRE. — *On a* $q_2(K)-q_1(K) \geqslant s-1$.

Nous venons donc de démontrer que $T(s, 2) = C_{s-1}^{2-1}$. Néanmoins, l'hypothèse que $T(s, i) = C_{s-1}^{i-1}$, qui permettrait de répondre par l'affirmative à une conjecture de CHANG dans [2], n'est déjà plus valable pour $i = 3$. En effet, la partition suivante, dans le cas de $s = 6$, $i = 3$, prouve que $T(6, 3) \leqslant 9$:

$$C_1 = \{\{0, 1, 2\}, \{0, 1, 3\}, \{0, 1, 4\}, \{0, 1, 5\}, \{0, 1, 6\}\},$$
$$C_2 = \{\{0, 2, 3\}, \{1, 2, 3\}, \{2, 3, 4\}, \{2, 3, 5\}, \{2, 3, 6\}\},$$
$$C_3 = \{\{0, 4, 5\}, \{1, 4, 5\}, \{2, 4, 5\}, \{3, 4, 5\}, \{4, 5, 6\}\},$$
$$C_4 = \{\{0, 5, 6\}, \{1, 5, 6\}, \{2, 5, 6\}, \{3, 5, 6\}\},$$
$$C_5 = \{\{0, 4, 6\}, \{1, 4, 6\}, \{2, 4, 6\}, \{3, 4, 6\}\},$$
$$C_6 = \{\{0, 2, 4\}, \{0, 2, 5\}, \{0, 2, 6\}\},$$
$$C_7 = \{\{0, 3, 4\}, \{0, 3, 5\}, \{0, 3, 6\}\},$$
$$C_8 = \{\{1, 2, 4\}, \{1, 2, 5\}, \{1, 2, 6\}\},$$
$$C_9 = \{\{1, 3, 4\}, \{1, 3, 5\}, \{1, 3, 6\}\}.$$

Nous avons d'ailleurs donné dans [7], sans démonstration, le résultat lorsque $i = 3$.

5. Détermination des partitions $\Gamma_{1,i}$, $\Gamma_{2,i}$ et de $\Gamma_{4,i}$ lorsque $K = \mathbf{Q}_2$

Lorsque $s = 1$, soit $-1 = a^2$; alors $S = \{0, 1\}$, $I_1 = \{0\}$, $I_2 = \{1\}$, et $\alpha_{I_1} = 1$, $\alpha_{I_2} = a^2$. Donc α_{I_1} et α_{I_2} sont dans la même classe, et la partition de $\Gamma_{1,1}$ est donc réduite à une clique $C_1 = \{I_1, I_2\}$.

Lorsque $s = 2$, écrivons $-1 = a^2+b^2$; alors $S = \{0, 1, 2\}$, $I_1 = \{0\}$, $I_2 = \{1\}$, $I_3 = \{2\}$, $J_1 = \{0, 1\}$, $J_2 = \{0, 2\}$, $J_3 = \{1, 2\}$. Pour $i = 1$, on retrouve le résultat précédent, et la partition de $\Gamma_{2,1}$ est constituée par la seule clique $\{I_1, I_2, I_3\}$. Pour $i = 2$, on a $\alpha_{J_1} = 1+a^2$, $\alpha_{J_2} = 1+b^2$, $\alpha_{J_3} = a^2+b^2$; mais alors α_{J_1}, α_{J_2}, α_{J_3} sont dans la même classe, à savoir celle de -1, et donc la partition de $\Gamma_{2,2}$ est constituée par la clique $\{J_1, J_2, J_3\}$. On remarque donc que dans les exemples précédents la partition de $\Gamma_{s,i}$ construite par DJOKOVIĆ est une partition de longueur minimale.

Étudions maintenant le graphe associé au corps des nombres 2-adiques. On sait, d'après [4], que le niveau de Q_2 est 4 et que l'indice de K^*/K^{*2} est $q = 8$. D'autre part, un système de représentants des classes du groupe quotient $Q/{}_2^*Q_2^{*2}$ nous est donné, d'après [1], par 1, 3, 5, 7, 2.1, 2.3, 2.5, 2.7. Considérons le polynôme $F(X) = X^2+7$ à coefficients dans Z_2. D'après le lemme de Hensel, on a

$$F(1) \equiv 0 \quad [8], \qquad F'(1) = 2 \not\equiv 0 \quad [4],$$

donc il existe x élément de $\mathbf{Z}_2$ tel que $F(x) = 0$ et $x \equiv 1$ [4]. Par suite, il existe $x \in \mathbf{Z}_2$ tel que

$$-1 = 1+1+4+x^2.$$

Déterminons alors les partitions de $\Gamma_{4,\,2}$ et $\Gamma_{4,\,3}$ associées à cette décomposition de -1 en somme de carrés. Avec les notations précédentes, nous avons donc :

$$\alpha_0 = \alpha_1 = \alpha_2 = 1, \qquad \alpha_3 = 2, \qquad \alpha_4 = x.$$

(*a*) *Détermination de la partition de* $\Gamma_{4,\,2}$. — Posons

$$I_1 = \{0, 1\}, \qquad I_2 = \{0, 2\},$$
$$I_3 = \{0, 3\}, \qquad I_4 = \{0, 4\}, \qquad I_5 = \{1, 2\}, \qquad I_6 = \{1, 3\},$$
$$I_7 = \{1, 4\}, \qquad I_8 = \{2, 3\}, \qquad I_9 = \{2, 4\}, \qquad I_{10} = \{3, 4\}.$$

On a alors :

$$\alpha_{I_1} = \alpha_{I_2} = \alpha_{I_5} = 2,$$
$$\alpha_{I_3} = \alpha_{I_6} = \alpha_{I_8} = 5,$$
$$\alpha_{I_4} = \alpha_{I_7} = \alpha_{I_9} = 1+x^2 = -6,$$
$$\alpha_{I_{10}} = 4+x^2 = -3.$$

D'où, en utilisant le système de représentants définis plus haut, on trouve comme partition :

$$\{I_1, I_2, I_5\}, \qquad \{I_3, I_6, I_8, I_{10}\}, \qquad \{I_4, I_7, I_9\},$$

soit donc une partition avec deux cliques de type 2, une clique de type 1.

(*b*) *Détermination de la partition de* $\Gamma_{4,\,3}$. — Soit

$$J_1 = \{0, 1, 2\}, \quad J_2 = \{0, 1, 3\},$$
$$J_3 = \{0, 1, 4\}, \quad J_4 = \{0, 2, 3\}, \quad J_5 = \{0, 2, 4\}, \quad J_6 = \{0, 3, 4\},$$
$$J_7 = \{1, 2, 3\}, \quad J_8 = \{1, 2, 4\}, \quad J_9 = \{1, 3, 4\}, \quad J_{10} = \{2, 3, 4\}.$$

On a, dans ce cas,

$$\alpha_{J_1} = 3, \qquad \alpha_{J_3} = \alpha_{J_5} = \alpha_{J_8} = 2+x^2 = -5,$$
$$\alpha_{J_2} = \alpha_{J_4} = \alpha_{J_7} = 6, \qquad \alpha_{J_6} = \alpha_{J_9} = \alpha_{J_{10}} = 5+x^2 = -2$$

et, comme précédemment, on trouve qu'alors la partition de $\Gamma_{4,\,3}$ est constituée par

$$\{J_1, J_3, J_5, J_8\}, \qquad \{J_2, J_4, J_7\}, \qquad \{J_6, J_9, J_{10}\},$$

donc deux cliques de type 1 et une clique de type 2.

On remarque ici aussi que le passage au complémentaire sur les sommets des cliques constituant la partition de $\Gamma_{4,\,2}$ nous donnait directement la partition de $\Gamma_{4,\,3}$, associée à cette décomposition de -1 en somme de quatre carrés. Si l'on considère une autre décomposition de -1 en somme de quatre carrés, on trouve alors des partitions de $\Gamma_{4,\,2}$ et $\Gamma_{4,\,3}$ qui se déduisent de celles que nous venons d'établir par des permutations de S.

BIBLIOGRAPHIE

[1] Borevitch (Z. I.) et Chafarevitch (I. R.). — *Théorie des nombres.* — Paris, Gauthier-Villars, (1967) (*Monographies internationales de Mathématiques modernes*, 8].

[2] Chang (P. L.). — On the number of square classes of a field with finite stufe, *J. of Number Theory*, t. 6, 1974, p. 360-368.

[3] Djoković (D. Z.). — Level of a field and the number of square classes, *Math. Z.*, t. 135, 1974, p. 267-269.

[4] Lam (T. Y.). — *The algebraic theory of quadratic forms.* — New York, W. A. Benjamin, 1973 (*Mathematics Lecture Note Series*).

[5] Pfister (A.). — Zur Darstellung von -1 als Somme von Quadratem in einem Körper, *J. London math. Soc.*, t. 40, 1965, p. 159-165.

[6] Pfister (A.). — Quadratische Formen in beliebigen Körpern, *Invent. Math.*, t. 1, 1966, p. 116-132.

[7] Tort (J. R.). — Sur un problème de partition de longueur minimale d'un graphe, *C. R. Acad. Sc. Paris*, t. 284, 1977, série A, p. 647-649.

(Texte reçu le 23 mai 1977.)

Jean-René Tort,
Département de Mathématiques,
Faculté des Sciences exactes,
Université de Pau,
64010 Pau-Université.