PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 127, Number 9, Pages 2587–2590
S 0002-9939(99)04508-6
Article electronically published on April 9, 1999

SUR LES p-CORPS

M. N'KANZA

(Communicated by Lance W. Small)

ABSTRACT. Here we give new examples of fields in characteristic 2 whose u-invariant and $\hat{u}$-invariant are different: $u(K) = 2$, $\hat{u}(K) = 2^m$ or ∞ $(m \in \mathbb{N}, m \geq 1)$. These fields are also p-fields.

RÉSUMÉ. Nous donnons ici de nouveaux exemples de corps K en caractéristique 2 dont le u-invariant et le $\hat{u}$-invariant diffèrent. Plus précisément: $u(K) = 2$ et $\hat{u}(K) = 2^m$ ou ∞ $(m \in \mathbb{N}, m \geq 1)$. Ces corps sont aussi des p-corps.

1. INTRODUCTION

Soit $\overline{\mathbb{Q}}$ une clôture algébrique des rationnels et $a \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$. Soit encore E le sous-corps de $\overline{\mathbb{Q}}$ maximal pour la propriété de ne pas contenir a (l'existence de E est assurée par le lemme de Zorn). Ce corps E a la propriété remarquable que toute extension finie est cyclique, c.à.d si $[M : E] < \infty$ alors M est une extension galoisienne de E et $Gal(M/E)$ est cyclique. Moresi s'est inspiré de cette construction (voir [M]), qui est due à Artin (voir [L, p.230, ex.3]), pour fournir les premiers exemples de corps K de caractéristique 2 tels que $u(K) = 2$ et $\hat{u}(K) = 2^m$ $(m \in \mathbb{N}, m \geq 1)$ ou $\hat{u}(K) = \infty$. Rappelons que par définition:

(1)
$$u(K) = \max\{\dim q : \ q \text{ forme quadratique non singulière anisotrope sur } K\}$$

et

(2) $$\hat{u}(K) = \max\{\dim q : \ q \text{ forme quadratique anistrope sur } K\}.$$

Dans le paragraphe 2 nous généralisons encore cette construction pour fournir de nouveaux exemples de corps de caractéristique 2 ayant la propriété précédente. D'autre part cette généralisation donne aussi des exemples de p-corps. Cette notion de p-corps a été introduite par Pfister. On dit qu'un corps K est un p-corps, p étant premier , si $[L : K]$ est une puissance de p pour toute extension finie L de K. Pfister a montré (voir [P]) que ces p-corps ont des propriétés arithmétiques intéressantes et a énoncé la conjecture suivante: Si tout système de formes quadratiques $q_1, \dots , q_r$ définies sur K en n variables, $n > r$, a une solution non triviale sur K alors K est un p-corps. Cette conjecture a été récemment résolue par D. Leep en caractéristique 0 (voir [Le]) et est toujours ouverte en caractéristique > 0.

Received by the editors April 2, 1997 and, in revised form, November 18, 1997.
1991 *Mathematics Subject Classification.* Primary 11Exx.
Je remercie le Professeur P. Mammone pour les nombreux entretiens que nous avions eus ensemble lors de la préparation de ce travail-ci de ma thèse annexe (présentée le 26 Juin 1991 à l'Université de Mons).

2. Résultats sur les corps $(a_1, \dots, a_n)$-maximaux

2.1. **Notions.** Soit K un corps de caractéristique p. Notons par $\wp$ le morphisme additif de K dans K qui envoie x sur $\wp(x) := x^p - x$. L'ensemble $\wp(K)$ est non seulement un sous-groupe additif de K mais puisque pour $b \in F_p$, le corps premier, et $x \in K$ on a $b.(x^p - x) = (bx)^p - bx \in \wp(K)$, le sous-groupe additif $\wp(K)$ est aussi un espace vectoriel sur F_p. On peut donc considérer le quotient $K/\wp(K)$ comme un espace vectoriel sur F_p. Si $a_1, \dots, a_n \in K$, on notera $\langle \overline{a}_1, \dots, \overline{a}_n \rangle_K$ le sous-espace vectoriel de $K/\wp(K)$ engendré par les éléments $a_1 + \wp(K), \dots, a_n + \wp(K)$.

Définition. Soit K un corps de caractéristique p et $a_1, a_2, \dots, a_n \in K$. On dit que K est $(a_1, a_2, \dots, a_n)$-maximal si pour toute extension séparable finie L de K on a:

$$\dim_{F_p} \langle \overline{a}_1, \dots, \overline{a}_n \rangle_K = n \text{ et } \dim_{F_p} \langle \overline{a}_1, \dots, \overline{a}_n \rangle_L < n \tag{3}$$

pour toute extension séparable finie L de K. Bien-entendu $\langle \overline{a}_1, \dots, \overline{a}_n \rangle_L$ désigne le sous-espace vectoriel de $L/\wp(L)$ engendré par $a_1 + \wp(L), \dots, a_n + \wp(L)$. Dans [M] Moresi avait considéré le cas $n = 1$ et pour $a \in K \setminus \wp(K)$ avait défini le corps K comme a-maximal si pour toute extension séparable finie L de K , $\wp^{-1}(a) \in L$. La définition ci-dessus généralise donc celle de Moresi.

Le lemme suivant sera utilisé pour démontrer que si K est $(a_1, \dots, a_n)$-maximal alors $K/\wp(K) = \langle \overline{a}_1, \dots, \overline{a}_n \rangle_K$.

2.2. **Résultat préliminaire.**

Lemme 1. *Soit K un corps de caractéristique p et $a, b \in K$. Si $\dim_{F_p} \langle \overline{a}, \overline{b} \rangle_K = 2$ alors $a \notin \wp(K(\wp^{-1}(b)))$.*

Démonstration. Posons $T := \wp^{-1}(b)$. Un élément quelconque de $\wp(K(T))$ s'écrit (*)

$$(\wp(l_0) + r(0)) + (\wp(l_1) + r(1))T + \cdots + (\wp(l_{p-2}) + r(p-2))T^{p-2} + \wp(l_{p-1})T^{p-1}$$

pour certains $l_0, l_1, \dots, l_{p-1} \in K$ et où la fonction r_p est définie par la formule

$$r(i) = \sum_{j=i+1}^{p-1} \begin{pmatrix} j \\ i \end{pmatrix} l_j^p b^{j-i} \text{ avec } i = 0, 1, \dots, p-2, \tag{4}$$

et où

$$\begin{pmatrix} j \\ i \end{pmatrix} = \frac{j!}{i!(j-i)!}. \tag{5}$$

Supposons maintenant que $a \in \wp(K(T))$. L'élément a est donc de la forme (*) pour certains $l_1, l_2, \dots, l_{p-1}$ dans K. En particulier ceci nous dit que tous les coefficients de $T^i, i = 1, \dots, p-1$, sont nuls. On a donc $\wp(l_{p-1}) = 0$ et par suite $l_{p-1} \in F_p$. On a aussi

$$\wp(l_{p-2}) + (p-1)l_{p-1}^p b = 0,$$

c-à-d $\wp(l_{p-2}) = l_{p-1}b$.

Puisque $b \notin \wp(K)$ on voit que $l_{p-1} = 0$ et par conséquent $l_{p-2} \in F_p$. En continuant de cette manière on arrive à:

$$l_{p-1} = l_{p-2} = \ldots = l_2 = 0 \text{ et } l_1 \in F_p.$$

On a donc: $a = l_0^p - l_0 + l_1 b$. Ce qui contredit l'hypothèse: $\dim_{F_p} \langle \overline{a}, \overline{b} \rangle_K = 2$. $\square$

Théorème 2. *Soit K un corps de caractéristique p et $a_1, \dots, a_n \in K$. Si K est $(a_1, \dots, a_n)$-maximal alors*

(a) $K/\wp(K) = \langle \overline{a}_1, \dots, \overline{a}_n \rangle_K$*; en particulier $K/\wp(K)$ est de dimension finie.*

(b) $Br_p(K) = 0$*, la partie de p-torsion du groupe de Brauer de K est triviale, c.à.d.* $Br_p = 0$.

(c) *Pour* $p = 2$, $u(K) = 2$.

Démonstration. Pour (a): soient $b \in K \setminus \wp(K)$ et $L = K(\wp^{-1}(b))$. Comme K est $(a_1, \dots, a_n)$-maximal $\dim_{F_p} \langle \overline{a}_1, \dots, \overline{a}_n \rangle_L < n$. En d'autres termes, il existe $i_1, i_2, \dots, i_n \in F_p$ tels que $a := i_1 a_1 + \dots + i_n a_n \in \wp(L)$. Par le lemme 1 on déduit alors que $\dim_{F_p} \langle \overline{a}, \overline{b} \rangle_K = 1$ ou encore $b + \wp(K) \in \langle \overline{a_1}, \dots, \overline{a_n} \rangle_K$.

(b) est une conséquence immédiate d'un théorème de Saltman qui dit que si $\dim_{F_p} K/\wp(K) < \infty$ alors $Br_p(K) = 0$ (voir [S]). On conclut alors par (a).

Pour (c): comme $Br_2(K) = 0$, on a en particulier que toute algèbre de quaternions $[a, b)_K$ (c-à-d l'algèbre engendrée par i, j tels que $i^2 + i = a$, $j^2 = b$ et $ji = ij + j$) est isomorphe à $M_2(K)$. Puisque ceci vaut pour tout $a \in K$ et tout $b \in K^*$ on en déduit que la forme quadratique norme $X^2 + XY + aY^2$ représente tout élément de K^*. Car une forme quadratique non singulière de dimension 4 est du type $b(X^2 + XY + aY^2) + c(Z^2 + ZT + dT^2)$; celle-ci est clairement isotrope. □

Avant de construire des corps maximaux K avec $u(K) = 2$ et $\hat{u}(K) = 2^m$ ou ∞, voici un lemme, d'un intérêt indépendant, que l'on utilisera dans la construction.

Lemme 3. *Soit K un corps de caractéristique* 2 *tel que* $[K : K^2] > 1$. *Si* $u(K) = 2$ *alors* $\hat{u}(K) = [K : K^2]$.

Démonstration. Si $[K : K^2] = n$ et si $c_1, c_2, \dots, c_n$ est une base de K sur K^2 on voit facilement que la forme quadratique $c_1 X_1^2 + c_2 X_2^2 + \dots + c_n X_n^2$ est anisotrope. D'où: $\hat{u}(K) \geq [K : K^2]$. En fait puisque les seules formes quadratiques non singulières et anisotropes sont de dimension deux, c-à-d du type $a(X^2 + XY + bY^2)$, on en déduit que les seules formes quadratiques anisotropes de dimension stictement plus grande que $n = [K : K^2]$ ne peuvent être que du type

$$(**) \qquad a(X^2 + XY + bY^2) + c_1 X_1^2 + c_2 X_2^2 + \dots + c_{n-1} X_{n-1}^2.$$

En utilisant la proposition 1.*ii*) page 5 de [MMW] on voit que ceci ne peut jamais se produire. En effet s'il existait une forme quadratique anisotrope du type (**) la proposition citée impliquerait que $u(K) = 2[K : K^2] > 2$. Ce qui contredirait l'hypothèse $u(K) = 2$. □

2.3. **Construction des corps maximaux.** Soient $X_1, \dots, X_m$ des indéterminées sur F_2 et $K = F_2(X_1, \dots, X_m)$. On a: $[K : K^2] = 2^m$. Fixons $n \leq m$. On a bien: $\dim_{F_2} \langle \overline{X_1}, \dots, \overline{X_n} \rangle_K = n$. On peut donc considérer L une clôture $(X_1, \dots, X_n)$-maximale dans la clôture séparable de K.

Proposition 4. $u(K) = 2$ *et* $\hat{u}(K) = 2^m$.

Démonstration. Puisque L est $(X_1, \dots, X_m)$-maximal, $u(L) = 2$ par le théorème 2. Donc par le lemme 3 on sait aussi que $\hat{u}(L) = [L : L^2]$. Mais puisque L est une extension séparable de K on a: $[L : L^2] = [K : K^2] = 2^m$, voir par exemple [B, lemme 1.3]. □

Nous terminons en faisant remarquer que si K est de caractéristique p et est $(a_1, \dots, a_n)$-maximal pour certains $a_1, \dots, a_n \in K$ alors K est un p-corps.

Proposition 5. *Soit K un corps de caractéristique p et $a_1, \dots, a_n \in K$. Si K est $(a_1, \dots, a_n)$-maximal, alors K est un p-corps.*

Démonstration. Par [K, particulierement le théorème 57] il suffit de démontrer que si M est une extension finie de K alors p divise $[M : K]$. On peut évidemment supposer que M est une extension séparable de K. Dans ce cas par maximalité on sait qu'il existe $a \in K \setminus \wp(K)$ tel que $K(\wp^{-1}(K)) \subset M$. D'où la thèse. □

3. Questions ouvertes (en caractéristique 2)

1. Si $u(K) = 4$, alors qu'en est-il de $\hat{u}(K)$? Atteint-il la borne inférieure $[K : K^2]$ ou la borne supérieure $2[K : K^2]$?

2. Dans ce travail la séparation entre $u(K)$ et $\hat{u}(K)$ a lieu avec $\hat{u}(K)$ atteignant sa borne inférieure. Existe-t-il des corps K pour lesquels $u(K)$ et $\hat{u}(K)$ sont différents avec

a) $u(K)$ atteignant sa borne supérieure, c.à.d $u(K) < \hat{u}(K) = 2[K : K^2]$?

b) $[K : K^2] < \hat{u}(K) < 2[K : K^2]$
(e.g. $2 < n = [K : K^2] < \hat{u}(K) = n + 2 < 2[K : K^2]$)?

References

[B] R. Baeza: Comparing u-invariants of characteritic 2 Bol.Soc.Bras.Mat. 13(1992) p. $105-114$. MR **84f:**10027

[Bl] A. Blanchard: Les corps non commutatifs, Coll. Sup., P.U.F., 1972. MR **50:**7242

[K] I. Kaplanski: Fields and Rings, Univ. Chicago Press, 1972. MR **50:**2139; MR **96a:**12001

[L] S. Lang: Algebra , Addison-Wesley, 1970. MR **86j:**00003 (second edition)

[Le] D. Leep: Pfister conjectures on quadratic co-fields , Journal füdie reine und angewandte Mathematik 404(1990), 209 – 220. MR **91d:**11036

[MMW] P. Mammone, R. Moresi, A. Wadsworth: u-invariants of fields of characteristic 2 , Math. Z. 208(1991), 335 – 347. MR **92m:**11033

[M] R. Moresi:On a class of fields admitting only cyclic extensions of prime power degree. Bol. Soc. Bras. Mat.Vol 15(1984), p. $101 - 107$. MR **87g:**12003

[P] Pfister: Systems of quadratic forms, Bull. Soc. Math. France, Mémoire 59(1979), p. $115 - 123$. MR **80j:**10033

[S] D. Saltman: Splittings of cyclic p-algebras, Proc. Am. Math. Soc. 62(1977), p. $223-228$. MR **55:**8006

Université de Mons, Faculté des Sciences, Département de Mathématique, Avenue V. Maistriau, 15, B- 7000 Mons, Belgique