ON A CLASS OF FIELDS ADMITTING ONLY CYCLIC EXTENSIONS OF PRIME POWER DEGREE

REMO MORESI(*)

Abstract. We will give three characterizations of such fields and an application to quadratic forms in characteristic 2.

1. Introduction

Let K be a field of characteristic $p \neq 0$.

It is often useful to know exactly how K is embedded in its separable closure, or more particularly how K is embedded in its p-separable closure.

This is equivalent to having exact information about all finite separable extensions of K, respectively all finite separable extensions of K having degree a power of p.

The simplest (nontrivial) instance of this situation obviously occurs when all such extensions are cyclic (i.e. normal with cyclic Galois group). In the separable case perfect fields with this property are called *quasi-finite* (cf. e.g. [5, ch. XIII.2]) In the p-separable case we will call them *p-cyclic*. The present work gives three characterizations of p-cyclic fields K. The first identifies them as the fields with $(K: P(K)) = p$, where $P(k) := \{a^p - a / a \in K\}$.

To describe the second let K_{ps} be the p-separable closure of K and $\alpha \in K \setminus P(K)$. Call an extension $K \subset\!\!\!\rightarrow L \subset\!\!\!\rightarrow K_{ps}$ *α-maximal*

(*) This work has been supported by D.I.U.C. (Dirección de Investigaciones de la Pontificia Universidad Católica de Chile).

Recebido em 10/11/83. Versão definitiva em 20/08/84.

if it is maximal with the property "$\alpha \notin P(L)$" and call K it self α-*maximal* if the extension $K \subset K \subset K_{ps}$ is α-maximal.

It then turns out that "p-cyclic" is equivalent with "α-maximal" for some α. (The reader may note here some analogy with an idea of E. Artin: cf. e. g. S. Lang, Algebra, p. 230, Ex. 3&4).

The third characterization is made in terms of the Galois group of K_{ps} over K: this group is isomorphic to the p-adic integers Z_p if and only if K is p-cyclic.

It is interesting to observe that each characterization reflects a different point of view useful for applications: the first is "practical", the second is "intrinsic" and the last is especially adapted to the methods of Galois cohomology.

There are many possibilities for proving the above result: for example, using [4, ch. II-4, cor. 1] or [6, Satz p. 237] the proof would be quite short. But the matter is simple enough to be handled elementarily: we will only use the criterion of Albert for cyclic extensions (cf. Lemma 1), a key-lemma on the behaviour of $P(K)$ under separable extensions of degree p and some basic facts about inverse limits.

A p-cyclic field K has the following interesting property: the subgroup $\mathrm{Br}_p(K)$ of p-torsion of the Brauer group $\mathrm{Br}(K)$ of K is trivial. If $p = 2$, this says that every quaternion algebra over K splits. We shall apply this fact to the theory of quadratic forms in characteristic two getting a partial answer to a question of Baeza [2].

Throghout the paper we shall make use of the following elementary facts:

i) The degree of a finite extension $K \subset L \subset K_{ps}$ is a power of p.

ii) The galois group of a normal separable infinite extension of fields $K \subset E$ is isomorphic to the inverse limit of the Galois groups of all finite Galois extensions $K \subset L \subset E$. The morphisms are the restrictions.

iii) $Z_p \cong \varprojlim_n Z/p^nZ$ (with respect to the projections $Z/p^{n+1}Z \to Z/p^nZ$).

iv) A *regular* quadratic form q over a field K of characteristic two can be represented as follows

$$q = \perp_{i=1}^{n} [a_i, b_i] \perp \perp_{j=1}^{m} [c_j], \qquad a_i, b_i, c_j \in K$$

where

$[a,b]$ and $[c]$ denote the form $ax^2+xy+by^2$, $a,b \in K$, and cx^2, $c \in K\setminus\{0\}$, respectively.

A form q with representation

$$q = \perp_{i=1}^{n} [a_i, b_i]$$

is called *non-singular*.

v) A cyclic p-algebra A of degree p over K is fully characterized by a separable subfield $K(P^{-1}(a))$ and a purely inseparable subfield $K(\sqrt[p]{b})$, $a,b \in K$. We write $A = [a,b]$.

2. p-Cyclic Fields

Lemma 1. *Let K be a field of characteristic p, $K \subset L_0$ a cyclic extension, S a generator for the corresponding Galois group and $L := L_0(P^{-1}(\beta))$, $\beta \in L_0 \setminus P(L_0)$. For $K \subset L$ to be cyclic it is necessary and sufficient that $\beta^S - \beta = \gamma^p - \gamma$ for some $\gamma \in K$ with $T_K^{L_0}(\gamma) \neq 0$.*

Proof. Let ξ be a root of $x^p - x - \beta$. As is well known, S extends to $S_1 : L \to L$ iff $S_1(\xi)$ is root of $x^p - x - \beta^S$. This implies

$\beta \equiv \beta^S \pmod{P(L_0)}$, say $\beta^S - \beta = P(\gamma)$, $\gamma \in K$. Putting $S_1(\xi) = \xi + \gamma$, one computes $S^{[L_0:K]}(\xi) = \xi + T_K^{L_0}(\gamma)$. So we see that the trace of γ determines the order of S_1. The rest follows easily. (see [1, ch. IX.3, th. 3 & th. 4] for details).

Lemma 2: *Let K be a field of characteristic p with $(K:P(K)=p$; $\beta \in K \setminus P(K)$ and $E := K(P^{-1}(\beta))$. Then $(E: P(E)) = p$.*

Proof. It is easy to compute that

$$P(E) = \left\{ \sum_{i=0}^{p-1} (P(\lambda_i) + \rho_p(i))\theta^i / \lambda_i \in K, \rho_p(i) = \sum_{j=i+1}^{p-1} \binom{j}{i} \lambda_j^p \beta^{j-i}, \right.$$

$$\left. \rho_p(p-1) := 0 \right\} \quad \text{where} \quad \theta := P^{-1}(\beta). \quad \text{We claim that}$$

$$P(E) = K \oplus K\theta \oplus \ldots \oplus K\theta^{p-2} \oplus P(K) \cdot \theta^{p-1} =: B$$

Let $a_0 + a_1\theta + \ldots + a_{p-2}\theta^{p-2} + P(\lambda_{p-1})\theta^{p-1} \in B$, λ_{p-1}, $a_i \in K$. There is an $n \in \{0,\ldots,p-1\}$, $\lambda_{p-2} \in K$ such that

$$a_{p-2} = n\beta + P(\lambda_{p-2}).$$

Consider $P(\lambda_{p-2}) + (p-1)\lambda_{p-1}^p \beta = P(\lambda_{p-2}) + \rho_p(p-2, \lambda_{p-1})$.

There is an $m \in \{0,\ldots,p-1\}$ for which

$$(p-1)\lambda_{p-1}^p \beta \equiv m\beta \pmod{P(K)}.$$

We need $m = n$. If $m \neq n$, say $m > n$, then let $r := m-n$ and consider $\tilde{\lambda}_{p-1} := \lambda_{p-1} + r$ in place of λ_{p-1}. It follows that

$$(p-1)\tilde{\lambda}_{p-1}^p \beta \equiv n\beta \equiv a_{p-2} \pmod{P(K)}.$$

One can argue similarly to find $\lambda_{p-2}, \ldots, \lambda_0 \in K$ such that

$$P(\lambda_0 + \lambda_1\theta + \ldots + \lambda_{p-1}\theta^{p-1}) = a_0 + a_1\theta + \ldots + a_{p-2}\theta^{p-2} + P(\lambda_{p-1})\theta^{p-1}.$$

This proves $B \subseteq P(E)$. Since the other inclusion is obvious, we get $B = P(E)$.

It is now an easy matter to prove that

$$E/P(E) \cong K/P(K)$$

which establishes the lemma.

We can now state the main theorem (cf. definitions and notations in the introduction).

Theorem 1. *Let K be a field of characteristic p, $\alpha \in K \setminus P(K)$. The following are equivalent:*

1. *K is α-maximal*
2. *$(K:P(K)) = p$*
3. *K is p-cyclic*
4. *$\mathrm{Aut}_K(K_{ps}) \cong Z_p$.*

Proof. *(1) $\Longrightarrow$ (2):* is clear.

(2) $\Longrightarrow$ (3): Let $K \subset L \subset K_{ps}$ be a finite extension and $\bar{L}$ the normal closure of L in K_{ps}. Then $K \subset \bar{L}$ is finite and Galois with degree a power of p (f. *1(i)*). There exists $m \in \mathbb{N}$ and a chain of subfields

$$K = L_0 \subset L_1 \subset \ldots \subset L_m = \bar{L}.$$

Such that $[L_{i+1}:L_i] = p \quad \forall\, i = 0,\ldots,m-1$.

By induction we can assume that $K \subset L_{m-1}$ is cyclic and by Lemma 2 $(\bar{L}:P(\bar{L})) = (L_{m-1}: P(L_{m-1})) = p$.

We choose $\beta \in L_{m-1}$ such that $\bar{L} = L_{m-1}(P^{-1}(\beta))$.

Let S be a generator of $\mathrm{Aut}_K(L_{m-1})$.

There is an $n \in \{1,\ldots,p-1\}$ and $\gamma \in K$ with $\beta^S = n\beta + P(\gamma)$.

Looking at the powers of S we see that $n = 1$. Noting that the trace function $T: L_{m-1} \to K$ is not zero, and that $\bar{L}$ depends only on the class of β mod. $P(L_{m-1})$, we can assume that $T(\gamma) \neq 0$.

Applying Lemma 1 we see that $K \subset\!\!\to \bar{L}$ is cyclic. Because $K \subseteq L \subseteq \bar{L}$, $K \subset\!\!\to L$ is cyclic too, and $L = \bar{L}$.

(3) ⟹ (4): This is clear, because of *1(ii)* & *1(iii)*.

(4) ⟹ (1): Let $K \subset\!\!\to L \subset\!\!\to K_{ps}$ be a finite extension (nontrivial). L is cyclic over K and there is $K \subset\!\!\to L_0 \subset\!\!\to L$ with $[L_0:K]=p$. Note now that it must be $(K:P(K)) = p$ (otherwise it would be possible to find a noncyclic extension of K of degree p^2). So K and L_0 satisfy the assumptions of Lemma 2. In the proof of this lemma it is shown that $K \subseteq P(L_0)$. In particular $K \subseteq P(L)$, which means that K is α-maximal for any $\alpha \in K\backslash P(K)$. This completes the proof.

As a corollary of Theorem 1 and [3, Th. 3] we obtain immediately

Theorem 2. *Let K be p-cyclic. Then* $\mathrm{Br}_p(K) = \{1\}$.

We are now ready to apply the results just obtained.

3. An application to quadratic forms in characteristic 2

Let K be a field of characteristic 2. As remarked in *1(iv)*, there are two types of quadratic forms over K. We define

$\tilde{u}(K) := \max\{\dim q/q$ anisotropic regular form over $K\}$

$u(K) := \max\{\dim q/q$ anisotropic nonsingular form over $K\}$

$\tilde{u}(K)$, $u(K)$ are obviously invariants of K and one has $u(K) < \tilde{u}(K)$.

Moreover, one can easily prove that

$$[K:K^2] \leq \tilde{u}(K) \leq 2[K:K^2].$$

In [2], R. Baeza asks if one can "separate" the two invariants (i.e. for $m,n \in \mathbb{N}$, $1 \leq m \leq n$, is there a field K with $u(K) = 2^m$, $\tilde{u}(K) = 2^n$?). It is not difficult to construct examples of fields K with $u(K) = 0$ and $\tilde{u}(K)$ any power of 2 (or ∞). We can now answer affirmatively the above question in the case where $m = 1$. We will prove

Theorem 3. *Let r be a power of 2 or ∞. Then there is a field K,* $\mathrm{char}(K) = 2$, *with $u(K) = 2$, $\tilde{u}(K) = r$.*

Proof. Let K be any field of char 2 with $[K:K^2] = r$ $K \neq P(K)$. Let $\alpha \in K\backslash P(K)$ and let $K \subset\!\!\to L \subset\!\!\to K_{2s}$ be an α-maximal extension. Then L is p-cyclic and by Th. 3, $u(L) = 2$. Moreover, $[L:L^2] = [K:K^2]$ (see e.g. [2] for a proof) and it follows that $\tilde{u}(K) = [L:L^2]$.

References

[1] A.A. Albert; *Modern Higher Algebra*, Un. Chicago Press, Chicago 1961.

[2] R. Baeza; *Comparing u-invariant of fields of characteristic 2*, Bol. Soc. Bras. Mat. 13 (1982) 105-114.

[3] D. Saltman; *Splittings of cyclic p-algebras*, Proc. Am. Math. Soc. 62 (1977) 223-228.

[4] J.P. Serre; *Cohomologie goloisienne*, Lectures Notes in Math. Springer Berlin-Heidelberg-NY 1964.

[5] J.P. Serre; *Corps locaux*, Actualités scientifiques et industrielles 1296, Herrmann, Paris 1962.

[6] E. Witt; *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f*, J.R.A. Math. 174 (1936) 237-245.

Remo Moresi
Universidad Católica
Departamento de Matemáticas
Casilla 114-D
Santiago de Chile