On the symbol length of p-algebras

Mathieu Florence

Abstract

The main result of this paper is Theorem 1.1: let k be a field of characteristic $p > 0$, and let A/k be a central simple algebra of index $d = p^n$ and exponent p^e. Then A is split by a purely inseparable extension of k of the form $k(\sqrt[p^e]{a_i}, i = 1 \ldots d-1)$. Combining this result with a theorem of Albert -of which we include a new proof- we get that any such algebra is Brauer equivalent to the tensor product of at most $d-1$ cyclic algebras of degree p^e. This improves drastically the previously known upper bounds (cf. introduction for more details).

The author would like to thank O. Gabber, P. Mammone, D. Saltman and J.-P. Tignol for heplful suggestions. He also thanks the referees for their remarks, which helped improve the clarity of the exposition.

1. Introduction

Let k be a field. If k contains all roots of unity, it is known by the theorem of Merkurjev and Suslin that any central simple algebra over k, of exponent e prime to the characteristic of k, is Brauer equivalent to the tensor product of cyclic algebras of degree e. To the question 'how many cyclic algebras are needed?', very little is known. This question is called the symbol length problem. It has recently been discussed in the survey article [ABGV], pages 230-231. Before stating our theorem, let us recall some known results. Rosset and Tate proved that a central simple algebra of prime degree p, with p prime to the characteristic of k, is Brauer equivalent to the tensor product of at most $(p-1)!$ cyclic algebras of degree p. If $p > 2$, this bound may be improved down to $(p-1)!/2$. We refer to [GS], proposition 7.4.13 and exercise 7.10, for details. In this paper, we concentrate on the case 'orthogonal' to the previous one: that of p-algebras, that is, when k has characteristic $p > 0$ and the algebras under consideration have exponent a power of p. In this case, the theory has mainly been developed by Albert and Teichmüller. By a theorem of Teichmüller (cf. *loc. cit.*, theorem 9.1.4) , we know that an algebra of exponent p^e is Brauer equivalent to a tensor product of cyclic algebras of degree p^e(note that a result of Albert (*loc. cit.*, theorem 9.1.8) states that such an algebra is in fact Brauer equivalent to a cyclic one; more precisely, Albert shows that a tensor product of cyclic p-algebras remains cyclic). Here again, we might ask for a bound on the number of cyclic algebras needed. Let us briefly recall the results previously known. In [T], it is proven that an algebra of index p^r and exponent p^e is Brauer equivalent to the tensor product of $p^r!(p^r!-1)$ cyclic algebras of degree p^e. For algebras of degree p, Mammone ([M], proposition 5.2) improved this bound to $(p-1)!$. Note also that Mammone and Merkurjev ([MM], proposition 5) proved that a -cyclic- p-algebra of degree p^n and exponent p^e is Brauer equivalent to a tensor product of p^{n-e} cyclic algebras of degree p^e.

2010 Mathematics Subject Classification 20G15
Keywords: Central simple algebras, Severi-Brauer varieties.

The main result of this paper is the following theorem.

Theorem 1.1. *Let k be a field of characteristic $p > 0$. Let A/k be a division algebra of index $d = p^n$ and exponent p^e. Then there exists $d-1$ elements $a_1, \dots, a_{d-1}$ in k such that the field extension*

$$k(\sqrt[p^e]{a_i}, i = 1 \dots d-1)$$

splits A. In particular, A is Brauer equivalent to a tensor product of $d-1$ cyclic algebras of degree p^e.

The paper is organized as follows. After introducing notation and recalling some basic material in section 2, we give in section 3 the proof of two elementary auxiliary tools. The first one is proposition 3.3, stating that, over a field of characteristic $p > 0$, base-changing by the Frobenius induces multiplication by p in the Brauer group. It can be found in [J], theorem 4.1.2; or in [KOS], theorem 3.9, for any ring of characteristic p. We include here a slightly different proof. The second one is proposition 3.4 which is well-known but plays a key rôle in the proof of the main theorem, which is the object of section 4. The last section is devoted to the proof of a structure theorem for some commutative unipotent algebraic groups. Roughly speaking, it says the following. Let K/k be a finite purely inseparable field extension. Then the algebraic k-group $U := R_{K/k}(\mathbb{G}_\mathrm{m})/\mathbb{G}_\mathrm{m}$ is unipotent. To split it, i.e. to make it acquire a composition series with quotients isomorphic to $\mathbb{G}_\mathrm{a}$, it suffices to mod out the (finite constant) subgroup generated by the images in $U(k)$ of a system of generators of K as a k-algebra. This yields Albert's theorem as an immediate corollary.

2. Notation, definitions

Let l be a field. We denote by $\bar{l}$ (resp. l_s) an algebraic (resp. separable) closure of l. We denote by $\mathrm{Br}(l)$ the Brauer group of l. if V is an l-vector space, we denote by $\mathbb{A}_l(V)$ the affine space of V, with functor of points sending an l-algebra A to $V \otimes_l A$. It is also canonically endowed with the structure of an algebraic l-group (vector group). We denote by $\mathbb{P}_l(V)$ the projective space of lines in V. These two notions obviously extend to the case of a locally free module of finite rank over any commutative base ring.

2.1 Cohomology.

Let G/l be an algebraic group. We shall write $H^1(l, G)$ for the first cohomology set for the fppf topology with coefficients in G. It coincides with Galois cohomology if G/l is smooth. Accordingly, if G is commutative, we write $H^i(l, G)$ for the higher fppf cohomology groups.

2.2 Severi-Brauer varieties.

If A is a central simple algebra of degree (=square root of the dimension) n, we denote by $\mathrm{SB}(A)$ the Severi-Brauer variety associated to A. As usual, $\mathrm{SB}(A)(\bar{l})$ is the set of right ideals of $A \otimes_l \bar{l}$, of dimension n (as a $\bar{l}$-vector space). Recall that, if $A = \mathrm{End}(V)$, for V an l-vector space of dimension n, we have a canonical identification between $\mathbb{P}_l(V)$ and $\mathrm{SB}(A)$: to a line $d \subset V$, we associate the right ideal of endomorphisms whose image is contained in d. A Severi-Brauer variety is thus nothing else than a twisted projective space.

2.3 Cyclic algebras.

Let $a \in l^*$ and let $n \geqslant 1$ be an integer. Denote by σ the class of 1 in the group $\mathbb{Z}/n\mathbb{Z}$. Let M/l be a Galois l-algebra, of group $\mathbb{Z}/n\mathbb{Z}$. Consider the l-algebra A, generated by M and an indeterminate y, subject to the relations

$$y^n = a$$

and

$$y^{-1}\lambda y = \sigma(\lambda),$$

for all $\lambda \in M$. The algebra A is central simple; it is called the cyclic algebra associated to M and a, usually denoted by $(M/l, a)$. Its class in the Brauer group of l is the cup product of the class of a in $H^1(l, \mu_n)$ and that of M/l in $H^1(l, \mathbb{Z}/n\mathbb{Z})$ (cf. [GS], 2.5 and 4.7).

2.4 Twisting varieties by torsors.

Let G/l be an algebraic group (= l-group scheme of finite type). To the data of a (left) action of G on a quasi-projective variety X, together with a (right) G-torsor T over l, one can associate the twist

$${}^T X := (T \times_l X)/G,$$

where G acts on $T \times_l X$ by the formula $(t, x).g = (tg, g^{-1}x)$. For a proof that this twist indeed exists and for the statement of some of its basic properties (including, in particular, functoriality for G-equivariant morphisms), we refer to [F], propositions 2.12 and 2.14. Note that the change of structure group for torsors is a special case of twisting. More precisely, let $f : G \longrightarrow H$ be a homomorphism of algebraic l-groups and let T/l be a (right) G-torsor. Then G acts (on the left) on H via f. One can thus form the twist ${}^T H$, which is nothing but the H-torsor $f_*(T)$ obtained from T by change of structure group using f.

2.5 Frobenius twist.

Assume that l has characteristic $p > 0$.
Denote by $\mathrm{Frob} : l \longrightarrow l$ the Frobenius $x \mapsto x^p$. If X is an l-scheme, we put

$$X^{(p)} := X \times_{\mathrm{Spec(Frob)}} \mathrm{Spec}(l),$$

the Frobenius twist of X. Recall that there exists a canonical l-morphism

$$F_X : X \longrightarrow X^{(p)}.$$

When $X = \mathrm{Spec}(A)$ is affine, it is nothing but the Spec of the l-algebra homomorphism

$$A \otimes_{\mathrm{Frob}} l \longrightarrow A,$$

$$x \otimes \lambda \mapsto \lambda x^p.$$

2.6 Weil scalar restriction (for $\mathbb{G}_{\mathrm{m}}$).

Let $A \longrightarrow B$ be a finite locally free morphism of commutative rings. Then there is a Weil scalar restriction functor $R_{B/A}$, at least for affine B-schemes. We shall only need to apply this functor to the multiplicative group $\mathbb{G}_{\mathrm{m}}$, in which case $R_{B/A}(\mathbb{G}_{\mathrm{m}})$ is the open A-subscheme of $\mathbb{A}_A(B) = \mathrm{Spec}(\mathrm{Sym}_A(B^*))$ whose points are invertible elements of B. It has $\mathbb{G}_{\mathrm{m}}$ as a subgroup scheme, and the quotient $R_{B/A}(\mathbb{G}_{\mathrm{m}})/\mathbb{G}_{\mathrm{m}}$ is easily seen to be representable by the open A-subscheme of $\mathbb{P}_A(B)$ whose points are line subbundles of B, locally directed by an invertible element of B.

2.7 Kähler differentials and the logarithmic differential.
Let $A \longrightarrow B$ be a morphism of commutative rings. We denote by $\Omega_{B/A}$ the B-module of Kähler differentials. Recall there is a group homomorphism

$$\mathrm{dlog} : B^*/A^* \longrightarrow \Omega_{B/A},$$

$$x \mapsto \frac{dx}{x}.$$

If moreover $A \longrightarrow B$ is finite locally free, and $\Omega_{B/A}$ is a finite locally free A-module, we can consider dlog as a morphism of A-group schemes

$$R_{B/A}(\mathbb{G}_{\mathrm{m}})/\mathbb{G}_{\mathrm{m}} \longrightarrow \mathbb{A}_A(\Omega_{B/A}).$$

In the sequel, k is a field of characteristic $p > 0$.

3. Auxiliary results

Lemma 3.1. *Let G/k be an algebraic group, and let T/k be a G-torsor. Denote by $F_G : G \longrightarrow G^{(p)}$ the Frobenius morphism. Then $(F_G)_*(T)$ and $T^{(p)}$ are canonically isomorphic as $G^{(p)}$-torsors.*

Proof. There is a morphism

$$\Psi : T \times_l G^{(p)} \longrightarrow T^{(p)},$$

$$(t, h) \mapsto F_T(t)h.$$

It is $G^{(p)}$-equivariant, where $G^{(p)}$ acts on the left-hand side by the formula $(t, h).h' = (t, hh')$. Now, let G act on $T \times_l G^{(p)}$ by the formula

$$g.(t, h) = (tg^{-1}, F_G(g)h),$$

and trivially on $T^{(p)}$. I claim that Ψ is then G-equivariant as well. This amounts to saying that, on the level of functors of points, we have the formula

$$F_T(tg^{-1})F_G(g)h = F_T(t)h,$$

where t (resp. g, h) is a point of T (resp. G, $G^{(p)}$). In other words, we have to check that

$$F_T(tg) = F_T(t)F_G(g).$$

Consider the action map

$$a : T \times_k G \longrightarrow T.$$

We know that the square

$$\begin{tikzcd} T \times_k G \arrow[r, "a"] \arrow[d, "F_{T \times_k G}"] & T \arrow[d, "F_T"] \\ T^{(p)} \times_k G^{(p)} \arrow[r, "a^{(p)}"] & T^{(p)} \end{tikzcd}$$

commutes. This yields the equality we had to check. Thus, Ψ induces a morphism of $G^{(p)}$-torsors

$$(F_G)_*(T) = (T \times_l G^{(p)})/G \longrightarrow T^{(p)},$$

which is an isomorphism (as is any morphism between torsors). □

Proposition 3.2. *Let A be a central simple algebra of degree n. Then*

$$A^{(p)} := A \otimes_{\mathrm{Frob}} k$$

is Brauer equivalent to $A^{\otimes p}$.

Proof. We have a commutative diagram of morphisms of algebraic k-groups

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{G}_{\mathrm{m}} \arrow[r] \arrow[d] & \mathrm{GL}_n \arrow[r] \arrow[d] & \mathrm{PGL}_n \arrow[r] \arrow[d] & 1 , \\
1 \arrow[r] & \mathbb{G}_{\mathrm{m}}^{(p)} \arrow[r] & \mathrm{GL}_n^{(p)} \arrow[r] & \mathrm{PGL}_n^{(p)} \arrow[r] & 1
\end{tikzcd}$$

where the vertical arrows are the Frobenius morphisms. Since all groups appearing here are defined over $\mathbb{F}_p$, we have canonical isomorphisms $\mathbb{G}_{\mathrm{m}}^{(p)} \simeq \mathbb{G}_{\mathrm{m}}, \mathrm{GL}_n^{(p)} \simeq \mathrm{GL}_n$ and $\mathrm{PGL}_n^{(p)} \simeq \mathrm{PGL}_n$. The vertical map on the left is then nothing but $x \mapsto x^p$. Denote by $\delta : H^1(k, \mathrm{PGL}_n) \longrightarrow \mathrm{Br}(k)$ the boundary map. For any PGL_n-torsor T/k, the above diagram -or more accurately the exact sequence it induces in fppf cohomology- implies that

$$p\delta([T]) = \delta([(F_{\mathrm{PGL}_n})_*(T)]).$$

But $[(F_{\mathrm{PGL}_n})_*(T)] = [T^{(p)}] \in H^1(k, \mathrm{PGL}_n)$, by lemma 3.1. Moreover, if T corresponds to the central simple algebra A (of degree n), then $T^{(p)}$ corresponds to $A^{(p)}$. The proposition is proved. $\square$

Remark 3.3. From the canonical isomorphism $\mathrm{SB}(A^{(p)}) \simeq \mathrm{SB}(A)^{(p)}$ (the formation of Severi-Brauer varieties commutes with base-change), we get a statement equivalent to that of the previous proposition: let $V = \mathrm{SB}(A)$ be a Severi-Brauer variety over k. Then $V^{(p)}$ is k-isomorphic to the Severi-Brauer variety associated to a central simple algebra of the same degree as A, Brauer equivalent to $A^{\otimes p}$.

Proposition 3.4. *Let K/k be a finite purely inseparable extension. Denote by $r(K/k)$ the minimal cardinality of a subset of K which generates K as a k-algebra. Then $r(K/k) = \dim_K(\Omega_{K/k})$. In particular, it is invariant under separable field extensions. More precisely, if l/k is a separable field extension, we have*

$$r(K/k) = r(K \otimes_k l/l).$$

Proof. Put $r = r(K/k)$ and $d = \dim_K(\Omega_{K/k})$. There exists elements $x_1, \ldots, x_r$ in K such that $K = k[x_1, \ldots, x_r]$. Hence the inequality $r \geqslant d$. Now, choose $y_1, \ldots, y_d$ in K such that the dy_i's form a K-basis of $\Omega_{K/k}$. Put $K' = k[y_1, \ldots, y_d]$. We have the first fundamental exact sequence of K-vector spaces

$$\Omega_{K'/k} \otimes_{K'} K \longrightarrow \Omega_{K/k} \longrightarrow \Omega_{K/K'} \longrightarrow 0,$$

from which we instantly infer that $\Omega_{K/K'} = 0$, hence that K'/K is separable, hence that $K' = K$. This shows that $r \leqslant d$. The assertion about invariance under separable extensions is then trivial. $\square$

4. Proof of theorem 1.1

The goal of this section is to use the material discussed previously in order to prove theorem 1.1. We can assume that k is infinite.

Let $V := \mathrm{SB}(A)$. By remark 3.3, we know that $V^{(p^e)}$ (V twisted by the e-th power of the Frobenius) is k-isomorphic to a projective space. Consider the canonical morphism

$$F : V \longrightarrow V^{(p^e)}$$

which is given by composing the $F_{V^{(p^i)}} : V^{(p^i)} \longrightarrow V^{(p^{i+1})}$. Extend scalars to k_s; we obtain a morphism F_s, where both the source and target of F_s are isomorphic to $\mathbb{P}^{d-1}_{k_s}$. More precisely F_s is nothing else but the morphism

$$\mathbb{P}^{d-1}_{k_s} \longrightarrow \mathbb{P}^{d-1}_{k_s},$$

$$[x_1 : \ldots : x_d] \mapsto [x_1^{p^e} : \ldots : x_d^{p^e}].$$

Hence the finite, purely inseparable field extension $k_s(V)/k_s(V^{(p^e)})$ induced by F_s is of degree $p^{(d-1)e}$, of exponent e and obtained by extracting p^e-th roots of $d-1$ elements of $k_s(V^{p^e})$; namely, the elements $x_1/x_d, x_2/x_d \ldots x_{d-1}/x_d$. By proposition 3.4, we get that the field extension $k(V)/k(V^{(p^e)})$ (of the same degree $p^{(d-1)e}$ and exponent e) is generated by $d-1$ elements $y_1, \ldots, y_{d-1} \in k(V)$. Note that we don't know much about an explicit possible choice of the y_i's. Put $a_i = y_i^{p^e} \in k(V^{(p^e)})$. We have a surjection

$$k(V^{(p^e)})[X_1, \ldots X_{d-1}]/ < X_i^{p^e} - a_i > \longrightarrow k(V),$$

$$X_i \mapsto y_i,$$

which is an isomorphism since both sides are $k(V^{(p^e)})$-vector spaces of the same dimension $p^{(d-1)e}$. This isomorphism gives the field extension $k(V)/k(V^{(p^e)})$ the structure of a $\mu_{p^e}^{d-1}$-torsor. Hence there is a rational action of $\mu_{p^e}^{d-1}$ on V which generically gives $F : V \longrightarrow V^{(p^e)}$ the structure of a $\mu_{p^e}^{d-1}$-torsor. More accurately, there exists a nonempty Zariski open $U \subset V^{(p^e)}$ such that $\tilde{F} := F_{|F^{-1}(U)} : F^{-1}(U) \longrightarrow U$ can be given the structure of a $\mu_{p^e}^{d-1}$-torsor. But since U is a nonempty open of a projective space, its set of k-rational points is nonempty. The fiber of $\tilde{F}$ over such a point is a $\mu_{p^e}^{d-1}$-torsor T which splits A (recall that in general a finite commutative k-algebra B splits A if and only if $V(B)$ is nonempty; here T is canonically embedded in V). But the k-algebra of functions on T is local, with residue field a field of the type

$$k(\sqrt[p^e]{a_i}, i = 1 \ldots d-1),$$

which then splits A as well. This proves the first statement of the theorem. Combine it with Albert's theorem (theorem 5.7) to obtain the second statement.

5. Structure of some unipotent groups and a new proof of Albert's theorem

In this section, we give a structure theorem for the unipotent group $R_{K/k}(\mathbb{G}_\mathrm{m})/\mathbb{G}_\mathrm{m}$, when K/k is a purely inseparable field extension (theorem 5.6), from which we derive a new proof of Albert's theorem.

Lemma 5.1. *Let A be a commutative ring of characteristic p. Put $B := A[Y]/ < Y^p >$. Denote by y the class of Y in B. For $\lambda = a_0 + a_1 y + \ldots + a_{p-1} y^{p-1} \in B$, there exists $b \in B^*$ such that*

$$\lambda dy = db/b$$

if and only if $a_{p-1} = a_0^p$.

Proof. Assume that $a_{p-1} = a_0^p$. Since dlog is a group homomorphism, it suffices to deal with the cases where $\lambda = ay^k$ $(k = 1 \ldots p-2)$ and $\lambda = a + a^p y^{p-1}$. Pick an integer $1 \leqslant k \leqslant p-1$ and pick $a \in A$. Put

$$b = 1 + ay^k + a^2 y^{2k}/2! + \ldots + a^{p-1} y^{(p-1)k}/(p-1)!$$

(truncated exponential series). An easy computation shows that

$$db = kay^{k-1}bdy$$

if $k > 1$ and that

$$db = a(b - a^{p-1}y^{p-1}/(p-1)!)dy = b(a + a^p y^{p-1}/b)dy = b(a + a^p y^{p-1})dy$$

if $k = 1$. In the last equalities, we have used the fact that $(p-1)! = -1 \mod p$ and that $1/b = 1 \mod yB$. The claim follows.
Assume now that $\lambda = db/b$ for $b \in B^*$. We have to show that $a_{p-1} = a_0^p$. Assume that b factors as

$$b = c(1 - x_0 y) \dots (1 - x_{p-1} y),$$

with $c \in A^*$ and $x_i \in A$. Since dlog is a group homomorphism, it suffices to deal with the case $b = 1 - xy$. We then compute:

$$db/b = d(1 - xy)/(1 - xy) = (-x - x^2 y - \dots - x^p y^{p-1})dy,$$

and the fact to check becomes trivial. To conclude, it suffices to remark that b factors in the way above after a faithfully flat ring extension of A (for instance the well-known 'universal splitting algebra' for b, cf. [G], lemma S), and the equality $a_{p-1} = a_0^p$ might be checked after such a base change.

□

Remark 5.2. In [O], proposition VI. 5.3, Oesterlé studies the unipotent group $R_{K/k}(\mathbb{G}_\mathrm{m})/\mathbb{G}_\mathrm{m}$, where $K = k(t^{1/p})$ is a purely inseparable extension of k. He shows that this group is isomorphic to the subgroup of $\mathbb{G}_\mathrm{a}^p$ given by the equation

$$(E) : x_0^p + x_1^p t + \dots + x_{p-1}^p t^{p-1} = x_{p-1}.$$

His proof uses the logarithmic differential as well, and is not unrelated to our approach. In short, what has to be shown is the following. Put $t' = t^{1/p}$. Given $y = y_0 + y_1 t' + \dots + y_{p-1} t'^{p-1} \in K$, then

$$dy/y = (x_0 + x_1 t' + \dots + x_{p-1} t'^{p-1})dt',$$

with the x_i's satisfying equation (E) above. As an exercise, the reader may provide a short proof of Oesterlé's result using lemma 5.1, which corresponds to the 'trivial' case $t = 0$. We thank one of the referees for suggesting us to insert this remark.

Lemma 5.3. *Let A be a commutative ring of characteristic p, with* $\mathrm{Spec}(A)$ *connected. Pick $t \in A^*$ and put $B := A[X]/ < X^p - t >$. Denote by x the class of X in B. For $b \in B^*$, there exists $\alpha \in A$ such that*

$$db/b = \alpha dx/x \in \Omega_{B/A}$$

if and only if b is of the form ax^n, for some integer n and some $a \in A^*$.

Proof. The B-module $\Omega_{B/A}$ is free of rank one with generator dx. Write $b = \sum_{i=0}^{p-1} a_i x^i$, with $a_i \in A$. The equality

$$db/b = \alpha dx/x$$

reads as

$$\sum_{i=0}^{p-1} i a_i x^i = \sum_{i=0}^{p-1} \alpha a_i x^i.$$

It follows that $\alpha^p-\alpha=\Pi_{i=0}^{p-1}(\alpha-i)$ annihilates all a_i's, hence b, hence is zero since b is invertible. Since $\mathrm{Spec}(A)$ is connected, we deduce that α belongs to $\mathbb{F}_p$. Let n be an integer whose class is α. The equality

$$db/b=\alpha dx/x$$

can now be rewritten as $d(bx^{-n})=0$, which obviously implies the conclusion of the lemma. □

PROPOSITION 5.4. *Let A be a commutative ring of characteristic p. Let $t\in A^*$. Put $B:=A[X]/<X^p-t>$. Denote by x the class of X in B. Put*

$$\Omega'_{B/A}:=\Omega_{B/A}/<A\frac{dx}{x}>;$$

it is a free A-module of rank $p-1$. We have an exact sequence of A-group schemes

$$1\longrightarrow\mathbb{Z}/p\mathbb{Z}\stackrel{n\mapsto x^n}{\longrightarrow}R_{B/A}(\mathbb{G}_{\mathrm{m}})/\mathbb{G}_{\mathrm{m}}\longrightarrow\mathbb{A}_A(\Omega'_{B/A})\longrightarrow 1,$$

where the morphism on the right is the composition of

$$dlog: R_{B/A}(\mathbb{G}_{\mathrm{m}})/\mathbb{G}_{\mathrm{m}}\longrightarrow\mathbb{A}_A(\Omega_{B/A})$$

with the quotient map

$$\mathbb{A}_A(\Omega_{B/A})\longrightarrow\mathbb{A}_A(\Omega'_{B/A}).$$

Proof. Injectivity and exactness in the middle follow from lemma 5.3, where we can replace A by an arbitrary commutative A-algebra and base-change B accordingly. We now check surjectivity. We will show the following. For any element $bdx\in\Omega_{B/A}$, there exists a faithfully flat ring extension A'/A, together with an invertible $b'\in B\otimes_A A'$ such that

$$\frac{db'}{b'}=bdx$$

modulo $A'\frac{dx}{x}$. Base-changing A to an arbitrary A-algebra then yields surjectivity. By base-changing A to a faithfully flat A-algebra in which t is a p-th power (B itself will do), we can assume that $t=u^p$ is a p-th power in A. Put $y:=x-u\in B$; then B becomes isomorphic to $A[Y]/<Y^p>$. Take $b=a_0+a_1y+\ldots+a_{p-1}y^{p-1}\in B$. In $\Omega_{B/A}$, we have

$$\frac{dx}{x}=\frac{dy}{y+u}=(u^{-1}-u^{-2}y+u^{-3}y^2+\ldots+(-1)^{p-1}u^{-p}y^{p-1})dy.$$

After a finite étale extension of A, we can assume the equation

$$(a_0+\alpha u^{-1})^p=a_{p-1}+(-1)^{p-1}\alpha u^{-p}$$

has a solution $\alpha\in A$. Replacing b by $b+\alpha\frac{dx}{x}$, we can assume that $a_0^p=a_{p-1}$. Apply lemma 5.1 to conclude. □

Remark 5.5. The preceding proposition can be slightly generalized as follows. Let R be a commutative ring of characteristic p. Let A be an R-algebra which is finite and locally free. Let t, B, x and $\Omega'_{B/A}$ be as in the proposition. Then there is an exact sequence of R-group schemes

$$1\longrightarrow\mathbb{Z}/p\mathbb{Z}\stackrel{n\mapsto x^n}{\longrightarrow}R_{B/R}(\mathbb{G}_{\mathrm{m}})/R_{A/R}(\mathbb{G}_{\mathrm{m}})\longrightarrow\mathbb{A}_R(\Omega'_{B/A})\longrightarrow 1.$$

The proof is exactly the same and will be omitted.

We now concentrate on the case of our field k.

Proposition 5.6. *Let $t_1, \ldots, t_r$ be elements of k^*, and $n_1, \ldots, n_r$ be positive integers. Put*

$$K = \bigotimes_{i=1}^{r} k[X_i]/ < X_i^{p^{n_i}} - t_i > .$$

Put

$$U_{K/k} := R_{K/k}(\mathbb{G}_\mathrm{m})/\mathbb{G}_\mathrm{m};$$

it is a smooth, connected, commutative (unipotent) k-group scheme. For each i, denote by G_i the subgroup of $U_{K/k}$ generated by the class x_i of X_i in K^*; it is isomorphic to $\mathbb{Z}/p^{n_i}\mathbb{Z}$. Denote by $V_{K/k}$ the cokernel of the inclusion

$$\Pi_{i=1}^{r} G_i \longrightarrow U_{K/k}.$$

Then $V_{K/k}$ has a composition series with quotients isomorphic to $\mathbb{G}_\mathrm{a}$. In particular, it has trivial H^i for each $i \geqslant 1$.

Proof. Induction on the sum of the n_i's. Put

$$K' = k[x_1^p, x_2, \ldots, x_r].$$

Then G_i, $i \geqslant 2$, is a subgroup of $U_{K'/k}$ as well. Denote by G'_1 the subgroup of $U_{K'/k}$ generated by x_1^p; it is isomorphic to $\mathbb{Z}/p^{(n_1-1)}\mathbb{Z}$. Denote by $V_{K'/k}$ the quotient $U_{K'/k}/(G'_1 \times \Pi_{i=2}^{r} G_i)$; it is a subgroup of $V_{K/k}$. It is enough to show that the quotient $V_{K/k}/V_{K'/k}$ is isomorphic to a product of $\mathbb{G}_\mathrm{a}$'s, then induction applies.
By remark 5.5 applied to $R = k$, $A = K'$ and $t = X_1^p$ (the K-algebra B then being canonically isomorphic to K), we obtain an exact sequence of k-group schemes:

$$1 \longrightarrow \mathbb{Z}/p\mathbb{Z} \overset{n \mapsto x_1^n}{\longrightarrow} R_{K/k}(\mathbb{G}_\mathrm{m})/R_{K'/k}(\mathbb{G}_\mathrm{m}) \longrightarrow \mathbb{A}_k(\Omega'_{K'/K}) \longrightarrow 1,$$

yielding an isomorphism from $V_{K/k}/V_{K'/k}$ to $\mathbb{A}_k(\Omega'_{K'/K})$, which is of course, as a k-group scheme, isomorphic to a product of copies of $\mathbb{G}_\mathrm{a}$'s.

□

Theorem 5.7. *(Albert). Let $K = k[\sqrt[p^{n_i}]{a_i}, i = 1 \ldots r]$ be a purely inseparable field extension. Let $\alpha \in \mathrm{Br}(k)$ be in the kernel of the restriction map $\mathrm{Br}(k) \longrightarrow \mathrm{Br}(K)$. Then there exists $\mathbb{Z}/p^{n_i}\mathbb{Z}$-Galois k-algebras M_i such that*

$$\alpha = \sum_{i=1}^{r} [(M_i, a_i)]$$

in $\mathrm{Br}(k)$.

Proof. Put

$$K' = \bigotimes_{i=1}^{r} k[X_i]/ < X_i^{p^{n_i}} - a_i > .$$

The k-algebra K' is finite-dimensional, local, with residue field K. Recall that there is (as for any scheme) a Brauer group $\mathrm{Br}(K')$, defined as $H^2(\mathrm{Spec}(K'), \mathbb{G}_\mathrm{m})$ (for the étale or fppf topology, it is the same here since $\mathbb{G}_\mathrm{m}$ is smooth). It corresponds to the group of equivalence classes of Azumaya algebras over K', and the natural map $\mathrm{Br}(K') \longrightarrow \mathrm{Br}(K)$ is an isomorphism. Put

$$U_{K'/k} := R_{K'/k}(\mathbb{G}_\mathrm{m})/\mathbb{G}_\mathrm{m}.$$

As usual, from the long exact sequence in (Galois) cohomology associated to the short exact sequence

$$1 \longrightarrow \mathbb{G}_{\mathrm{m}} \longrightarrow R_{K'/k}(\mathbb{G}_{\mathrm{m}}) \longrightarrow U_{K'/k} \longrightarrow 1,$$

we deduce that

$$H^1(k, U_{K'/k}) = \mathrm{Ker}(\mathrm{Br}(k) \longrightarrow \mathrm{Br}(K')) = \mathrm{Ker}(\mathrm{Br}(k) \longrightarrow \mathrm{Br}(K)).$$

We can then view α as a class in $H^1(k, U_{K'/k})$.
By proposition 5.6, we have an exact sequence

$$1 \longrightarrow \Pi_{i=1}^r \mathbb{Z}/p^{n_i}\mathbb{Z} \longrightarrow U_{K'/k} \longrightarrow V_{K'/k} \longrightarrow 1,$$

with $V_{K'/k}$ having trivial H^1. We thus have a surjection

$$s : \Pi_{i=1}^r H^1(k, \mathbb{Z}/p^{n_i}\mathbb{Z}) \longrightarrow H^1(k, U_{K'/k}).$$

Let i be an integer between 1 and r, and let M_i be a Galois $\mathbb{Z}/p^{n_i}\mathbb{Z}$-algebra over k. By (a variant of the) construction 2.5.1 of [GS], we see that

$$s([M_i/k]) = [M_i/k, a_i]$$

in $\mathrm{Br}(k)$, whence the result. □

Remark 5.8. We present here Albert's theorem as a corollary of proposition 5.6. The usual proofs of this theorem are completely different. To the author's knowledge, the shortest one is to be found in [GS], theorem 9.1.1, where the theorem is attributed to Hochschild. Meanwhile, we are grateful to David Saltman for pointing out that this theorem is actually due to Albert, cf. [A], theorem 28, page 108. It is likely that the proof of Albert's theorem presented in [GS] is due to Hochschild. Roughly speaking, it goes as follows. As in the proof of proposition 5.6, the crucial case is that of $K = k[\sqrt[p]{a}]$. It is first shown that α is represented by a central simple algebra A/k, of degree p, containing K; this appears to be a classical fact. Put $x = \sqrt[p]{a} \in K$. Using a simple but clever construction, one then exhibits a maximal $\mathbb{Z}/p\mathbb{Z}$-Galois algebra $M \subset A$ such that , for each $m \in M$, one has $xmx^{-1} = \sigma(m)$, where σ is the class of 1 in $\mathbb{Z}/p\mathbb{Z}$. This shows that $A = (M/k, a)$.

References

A A. A. Albert.— *Structure of algebras*, AMS Colloquium Publications **XXIV** (1939).

ABGV A. Auel, E. Brussel, S. Garibaldi, U. Vishne.— *Open problems on central simple algebras*, Transform. Groups **16** (2011), no. 1, 219–264.

F M. Florence.— *On the essential dimension of cyclic p-groups*, Invent. Math. **171** (2008), no. 1, 175–189.

G O. Gabber.— *Some theorems on Azumaya algebras*, in Groupe de Brauer, Lecture Notes in Math. **844** (1981), 129–209.

GS P. Gille, T. Szamuely.— *Central simple algebras and Galois cohomology*, Cambridge University Press (2006).

KOS M.-A. Knus, M. Ojanguren, D. Saltman.— *Brauer groups in characteristic p*, in Brauer Groups, Evanston 1975, Springer LNM **549**.

J N. Jacobson.— *Finite-dimensional division algebras over fields*, corrected 2nd printing, Springer-Verlag (2010).

M P. Mammone.— *Sur la corestriction des p-symboles*, Comm. Algebra **14** (1986), no. 3, 517–529.

MM P. Mammone, A. Merkurjev.— *On the corestriction of p^n-symbol*, Israel J. Math. **76** (1991), no. 1-2, 73–79.

O J. Oesterlé.— *Nombres de Tamagawa et groupes unipotents en caractéristique p*, Invent. Math. **78** (1984), 13–88.

T O. Teichmüller.— *p-Algebren*, Deutsche Mathematik **1** (1936), 362–388.

Mathieu Florence mathieu.florence@gmail.com
Equipe de Topologie et Géométrie Algébriques, Institut de Mathématiques de Jussieu, 4, place Jussieu, 75005 Paris.