ISRAEL JOURNAL OF MATHEMATICS 76 (1991), 73–80

ON THE CORESTRICTION OF p^n-SYMBOL

BY

P. MAMMONE

Université de Mons, Belgique

AND

A. MERKURJEV

Leningrad State University, USSR

ABSTRACT

Let F be a field of characteristic p. Teichmüller proved that any p-algebra over F of index p^n and exponent p^e is similar to a tensor product with at most $p^n!(p^n!-1)$ factors of cyclic p-algebras over F of degree p^e. In this note we improve Teichmüller bound for two particular types of p-algebras. Let L be a finite separable extension of F. If A is a cyclic p-algebra over L of degree p^e we show that $\mathrm{Cor}_{L/F}A$, the corestriction of A, is similar to a tensor product with at most $[L:F]$ factors of cyclic p-algebras over F of degree p^e. Moreover we prove that $[L:F]$ is the best possible bound. From this we deduce that if A is a cyclic p-algebra over F of degree p^n and exponent p^e then A is similar to a tensor product with at most p^{n-e} factors of cyclic p-algebras over F of degree p^e.

Introduction

Let F be a field of characteristic p. We denote by $W_n(F)$ the group of truncated Witt vectors of length n [see J, §III.4]. If $\omega \in W_n(F)$ and $a \in F^\star(:= F-\{0\})$ the symbol $[\omega, a)_F$ will represent the cyclic p-algebra of degree p^n over F generated by elements $\theta_1, \theta_2, \ldots, \theta_n, u$ satisfying the rules

$$u^{p^n} = a,$$
$$\mathcal{P}\theta := \theta^p - \theta = \omega$$

Received March 24, 1991 and in revised form June 11, 1991

and

$$u\theta u^{-1} = \theta + 1,$$

where θ is the Witt vector $(\theta_1, \theta_2, \dots, \theta_n) \in W_n(F(\theta_1, \dots, \theta_n))$,

$$\theta^p := (\theta_1^p, \theta_2^p, \dots, \theta_n^p),$$
$$u\theta u^{-1} := (u\theta_1 u^{-1}, \dots, u\theta_n u^{-1}),$$
$$1 := (1, 0, \dots, 0) \in W_n(F).$$

We call these algebras p^n-symbol algebras. For $n = 1$ we get the usual p-symbol algebra [see R, p. 269].

Witt proved that any cyclic p-algebra of degree p^n is a p^n-symbol algebra [see Wi, §6]. The class of a p^n-symbol algebra over F in $\mathrm{Br}(F)$, the Brauer group of F, will be called a p^n-symbol. To simplify notations we still denote by $[\omega, a)_F$ the class of the p^n-symbol algebra $[\omega, a)_F$ in $\mathrm{Br}(F)$. These p^n-symbols satisfy the following rules.

PROPOSITION 1: *Let ω, ω' in $W_n(F)$; $a_1, a_2, \dots, a_n$ in F and b, b' in F^* then, in $\mathrm{Br}(F)$, we have*

(i) $[\omega, b)_F + [\omega', b)_F = [\omega + \omega', b)_F$,
(ii) $[\omega, b)_F + [\omega, b')_F = [\omega, bb')_F$,
(iii) $[(0, a_1, a_2, \dots, a_n), b)_F = [(a_1, \dots, a_n), b)_F$,
(iv) $[(b, 0, \dots, 0), b)_F = 0$.

Proof: See [Wi; Satz 15, 16] for (i) (ii) and (iii), and [T1] for (iv). ∎

We can now rewrite an important theorem due to Albert with the symbol notations:

PROPOSITION 2 ([A, chap.VII, theorem 28]): *Let A be a p-algebra over F split by a purely inseparable extension $F(\sqrt[p^n]{a_1}, \sqrt[p^n]{a_2}, \dots, \sqrt[p^n]{a_s})$. Then in $\mathrm{Br}(F)$ we have*

$$[A] = \sum_{i=1}^{s} [\omega_i, a_i)_F$$

for some $\omega_1, \omega_2, \dots, \omega_s$ in $W_n(F)$.

In [T2, Satz 27] Teichmüller proved that any p-algebra of exponent p^e and index p^n is split by a purely inseparable extension K of exponent e (i.e. $K^{p^e} \subset F$) such that $[K : F] = p^{e \cdot p^n! \cdot (p^n! - 1)}$. So by Proposition 2 we deduce that the p^e-symbols generate $\mathrm{Br}_{p^e}(F)$, the p^e-torsion subgroup of $\mathrm{Br}(F)$ ($:= \{\alpha \in \mathrm{Br}(F) : p^e\alpha = 0\}$). And moreover, for a given p-algebra A of index p^n and exponent p^e, Teichmüller's result tells us that $[A]$ is a sum, in $\mathrm{Br}(F)$, of p^e-symbols with at most $p^n!(p^n!-1)$ terms. This yields an upper bound of the number of terms in the decomposition of the class of any p-algebra of index p^n.

In this note we improve Teichmüller's bound for two special types of p-algebras. If L is a finite separable extension of F, $\omega \in W_n(L)$ and $a \in L^\star$ then we show that $\mathrm{cor}_{L/F}[\omega, a)_L$ is a sum of p^n-symbols with at most $[L : F]$ terms. Moreover, this bound is the best possible. This is a generalization of [M, §3] and [R–T]. We also prove that the class of a cyclic p-algebra of degree p^n and exponent p^e is a sum of p^e-symbols with at most p^{n-e} terms.

See [R] or [D] for unexplained notation or terminology.

1. The Corestriction of p^n-Symbols

Let F be a field of characteristic p, F_s be a separable closure of F and L be a finite extension of F in F_s. Let $G_F = \mathrm{Gal}(F_s/F)$ and $G_L = \mathrm{Gal}(F_s/L)$. Recall that G_L acts on $W_n(L)$ by

$$\sigma \cdot (\theta_1, \theta_2, \ldots, \theta_n) = (\sigma(\theta_1), \sigma(\theta_2), \ldots, \sigma(\theta_n)).$$

Moreover for any $\chi \in H^1(G_F, \mathbb{Z}/p^n\mathbb{Z})$, there exists $\omega \in W_n(F)$ such that $\chi(\sigma) = \sigma(\omega) - \omega \in \mathbb{Z}/p^n\mathbb{Z}, \forall \sigma \in G_F$ (see [S] p. 163). We will write this element χ_ω. We denote by $\mathrm{cor}_{L/F}$ the corestriction homomorphism form $\mathrm{Br}(L)$ to $\mathrm{Br}(F)$ (see [R], §7.3]) and by cor the corestriction homomorphism of cohomological groups defined in [S, Chap. VII, §7] or [Ta, §2].

PROPOSITION 3 (Projection formula):
(i) $\mathrm{cor}_{L/F}[\omega, a)_L = [\omega, Nr_{L/F}(a))_F \quad \forall \omega \in W_n(F)$ and $a \in L^\star$.
(ii) $\mathrm{cor}_{L/F}[\omega, a)_L = [Tr_{L/F}(\omega), a)_F \quad \forall \omega \in W_n(L)$ and $a \in F^\star$.

Proof: From the exact sequence

$$1 \to F_s^\star \xrightarrow{\cdot p^n} F_s^\star \to F_s^\star/F_s^{\star p^n} \to 1$$

we deduce the exact sequence

$$1 \to H^1(G_F, F_s^\star/F_s^{\star p^n}) \to H^2(G_F, F_s^\star) \xrightarrow{\cdot p^n} H^2(G_F, F_s^\star),$$

and so we see that

$$H^1(G_F, F_s^\star/F_s^{\star p^n}) \simeq \mathrm{Br}_{p^n}(F).$$

Now by the Projection formula [W; Prop. 4.3.7, p. 160] for the following cup-product:

$$H^1(G_F, \mathbf{Z}/p^n\mathbf{Z}) \times H^0(G_F, F_s^\star) \xrightarrow{\cup} H^1(G_F, F_s^\star/F_s^{\star p^n})$$

and the fact that cor and $\mathrm{cor}_{L/F}$ commute with the above isomorphism we see that it suffices to check that for $a \in H^0(G_L, F_s^\star) = L^\star$ and $\chi_\omega \in H^1(G_L, \mathbf{Z}/p^n\mathbf{Z})$ we have

$$\mathrm{cor}\, a = Nr_{L/F}(a)$$

and

$$\mathrm{cor}\, \chi_\omega = \chi_{Tr_{L/F}\omega}\,.$$

We leave this to the reader. ∎

The next lemma is crucial in the proof of our main result.

LEMMA: *Let L be a finite separable extension of F of degree r. If $a \in L$ then $\sqrt[p^n]{a} \in L(\sqrt[p^n]{b_0}, \sqrt[p^n]{b_1}, \ldots, \sqrt[p^n]{b_{r-1}})$ for some $b_0, b_1, \ldots, b_{r-1}$ in F.*

Proof: Since $F(a) = F(a^{p^n}) \subset L$ we have

$$a = \sum_{i=0}^{r-1} b_i a^{ip^n}$$

for some $b_0, b_1, \ldots, b_{r-1}$ in F. And so

$$\sqrt[p^n]{a} = \sum_{i=0}^{r-1} \sqrt[p^n]{b_i} \cdot a^i. \qquad ∎$$

Here now is our main result.

THEOREM: *Let L be a finite separable extension of F, $[L : F] = r$. Let $[\omega, a)_L$ be a p^n-symbol in $\mathrm{Br}(L)$, then*

$$\mathrm{cor}_{L/F}[\omega, a)_L = \sum_{i=1}^{r} [\omega_i, a_i)_F$$

for some $\omega_1, \omega_2, \ldots, \omega_r$ in $W_n(F)$ and $a_1, a_2, \ldots, a_r$ in F^*.

Proof: By the lemma

$$L(\sqrt[p^n]{a}) \subset L(\sqrt[p^n]{b_1})L(\sqrt[p^n]{b_2}), \ldots, L(\sqrt[p^n]{b_r})$$

for some $b_1, b_2, \ldots, b_r$ in F. And therefore the purely inseparable extension $L(\sqrt[p^n]{b_1}, \ldots, \sqrt[p^n]{b_r})$ of L clearly splits the p^n-symbol algebra $[\omega, a)_L$. So by Proposition 2 there exists $\omega_1, \omega_2, \ldots, \omega_r$ in $W_n(L)$ such that

$$[\omega, a)_L = \sum_{i=1}^{r} [\omega_i, b_i)_L.$$

And finally by Proposition 3(ii) in $\mathrm{Br}(F)$ we have

$$\mathrm{cor}_{L/F}[\omega, a)_L = \sum_{i=1}^{r} [Tr_{L/F}\omega_i, b_i)_F . \qquad \blacksquare$$

The following comment has been pointed out by the referee. If F is of transcendence degree d over a perfect field, then for any finitely generated subfield E of F, $E^{1/p}$ is generated over E by $d+1$ elements. If L is a finite separable extension of F of degree r, then the corestriction of any p^n-symbol from L to F is a sum of at most m p^n-symbols in F, where $m = \min(r, d+1)$.

2. An Example

The theorem above shows that if L is a finite separable extension of F of degree r then any element of $\mathrm{Br}_{p^n}(F)$ which is the corestriction of a p^n-symbol in $\mathrm{Br}_{p^n}(L)$ is a sum of p^n-symbols with at most r terms.

The following example proves that this bound is the best possible. Let

$$u_1, v_1, \ldots, u_r, v_r$$

be $2r$ independent variables over a field k of characteristic p. Let

$$L := k(u_1, v_1, \ldots, u_r, v_r)$$

and σ be the automorphism of L defined by

$$\sigma_{|k} = 1_k,$$
$$\sigma(u_i) = u_{i+1} \text{ for } 1 \leq i < r \text{ and } \sigma(u_r) = u_1,$$
$$\sigma(v_i) = v_{i+1} \text{ for } 1 \leq i < r \text{ and } \sigma(v_r) = v_1.$$

Let $F := \mathrm{Fix}\, \sigma$. In [M, §4] it is proved that the corestriction of the p-symbol $[u_1, v_1)_L$ (i.e. $\mathrm{cor}_{L/F}[u_1, v_1)_L$) is not a sum of less than $r = [L : F]$ p-symbols in $\mathrm{Br}(F)$. Similarly we have

PROPOSITION 4: *Let $\omega = (u_1, 0, \ldots, 0) \in W_n(L)$, then $\mathrm{cor}_{L/F}[\omega, v_1)_L$ is not a sum of p^n-symbols with less than r terms.*

Proof: Recall first that for $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in W_n(L)$ we have $p.\alpha = (0, \alpha_1^p, \ldots, \alpha_{n-1}^p)$. So using the rules in Proposition 1 we see that in $\mathrm{Br}(F)$

$$\begin{aligned} p^{n-1}.\mathrm{cor}_{L/F}[\omega, v_1) &= \mathrm{cor}_{L/F}[p^{n-1}.\omega, v_1)_L \\ &= \mathrm{cor}_{L/F}[u_1^{p^{n-1}}, v_1)_L \\ &= \mathrm{cor}_{L/F}[u_1, v_1)_L. \end{aligned}$$

Since for any p^n-symbol α clearly $p^{n-1}.\alpha$ is a p-symbol, we conclude by the remark above. ∎

3. On the Decomposition of Cyclic p-Algebras

The following proposition improves Teichmüller's bound for cyclic p-algebras.

PROPOSITION 5: *Let A be a cyclic p-algebra of degree p^n and exponent p^e. Then $[A]$ is a sum of p^e-symbols in $\mathrm{Br}(F)$ with at most p^{n-e} terms.*

Proof: Let K be a maximal subfield of A cyclic over F, and L an extension of F in K such that $[K : L] = p^e$. Then by [Ti, Lemma] the image of the corestriction homomorphism

$$\mathrm{cor}_{L/F} : \mathrm{Br}(K/L) \to \mathrm{Br}(K/F)$$

is the p^e-torsion subgroup $\mathrm{Br}_{p^e}(K/F)$. Since $[A] \in \mathrm{Br}_{p^e}(K/F)$, then

$$[A] = \mathrm{cor}_{L/F}[\omega, a)_L$$

for some p^e-symbol in $\mathrm{Br}(L)$. The theorem gives the thesis. ∎

Observe that for $e = n$ the proposition gives the expected bound (i.e. 1).

4. Remark

Let $F(a)$ and $F(c)$ be finite separable extensions of F. In [M] it is proved that the corestriction homomorphism satisfies the following reciprocity law:

$$\mathrm{cor}_{F(a)/F}[a, f(a))_{F(a)} = \mathrm{cor}_{F(c)/F}[c, p(c))_{F(c)}$$

where $f(x) = \mathrm{Irr}(c, F)$ and $p(x) = \mathrm{Irr}(a, F)$.

It would be interesting to know how this formula generalizes to p^n-symbols.

It is perhaps useful to observe that in general

$$\mathrm{cor}_{F(a)/F}[(a,0,\ldots,0),f(a))_{F(a)} \neq \mathrm{cor}_{F(c)/F}[(c,0,\ldots,0),p(c))_{F(c)}.$$

Indeed, let $M = \mathbf{F}_2(X_1, X_2, X_3, Y_1, Y_2)$, the rational function field in five variables over $\mathbf{F}_2$. Let σ be the automorphism of M which permutes cyclically X_1, X_2, X_3 and fixes Y_1, Y_2 and similarly let τ be the automorphism of M which permutes cyclically Y_1, Y_2 and fixes X_1, X_2, X_3. Set $F := \mathrm{Fix}\ \langle\sigma,\tau\rangle, f(x) = \mathrm{Irr}\ (Y_1, F)$ and $p(x) = \mathrm{Irr}\ (X_1, F)$. Then using the rules of Proposition 1 it can be shown that

$$\begin{aligned}&\mathrm{cor}_{F(x_1)/F}[(X_1,0),f(X_1))_{F(X_1)} - \mathrm{cor}_{F(Y_1)/F}[(Y_1,0),p(Y_1))_{F(Y_1)}\\ &= [(X_1+X_2+X_3)(Y_1+Y_2), Y_1+Y_2)_F\,.\end{aligned}$$

Since the quaternion algebra $[(X_1+X_2+X_3)(Y_1+Y_2),(Y_1+Y_2))_F$ is a division algebra (this is clearly a division algebra over M) this proves our observation.

References

[A] A.A. Albert, *Structure of Algebras*, A.M.S. Coll. Publ. Vol. 24, A.M.S., New York, 1939.

[J] N. Jacobson, *Lectures in Abstract Algebra III*, Van Nostrand, Princeton, 1964.

[D] P.K. Draxl, *Skew fields*, London Math. Soc. Lecture Notes Series, Vol. 81, 1983.

[M] P. Mammone, *Sur la corestriction des p-symboles*, Comm. in Alg. **14** (1986), 517–529.

[R] L.H. Rowen, *Ring Theory II*, Academic Press, New York, 1988.

[R–T] S. Rosset and J. Tate, *A reciprocity law for K_2-traces*, Comm. Math. Helv. **58** (1983), 38–47.

[S] J.P. Serre, *Corps locaux*, Hermann, Paris, 1962.

[T1] O. Teichmüller, *Zerfallende zyklische p-Algebren*, J. Rein Angew. Math. **176** (1937), 157–160.

[T2] O. Teichmüller, *p-Algebren*, Deutsche Math. **1** (1936), 362–388.

[Ta] J. Tate, *Relations between K_2 and Galois cohomology*, Invent. Math. **36** (1976), 257–274.

[Ti] J.P. Tignol, *Cyclic Algebras of small exponent*, Proc. Am. Math. Soc. **89** (1983), 587–588.

[W] J.E. Weiss, *Cohomology of Groups*, Academic Press, New York, 1969.

[Wi] E. Witt, *Zyklische Körper und Algebren der charakteristik p vom* Grad p^n, J. Reine Angew. Math. **176** (1937), 126–140.