ISRAEL JOURNAL OF MATHEMATICS 96 (1996), 553–578

ON THE DECOMPOSITION OF CYCLIC ALGEBRAS

BY

L.H. ROWEN

Department of Mathematics, Bar-Ilan University
Ramat-Gan, 52900 Israel
e-mail: rowen@bimacs.cs.biu.ac.il

AND

J.-P. TIGNOL*

Département de Mathématiques, Université catholique de Louvain
B-1348 Louvain-la-Neuve, Belgium
e-mail: tignol@agel.ucl.ac.be

Dedicated to the memory of S.A. Amitsur

ABSTRACT

A cyclic algebra $(K/F, \sigma, a)$ of degree n has *property* $D(f)$ if it decomposes as a tensor product of a cyclic algebra of degree $e = \frac{n}{f}$ containing L (the fixed subfield under σ^e) and a cyclic subalgebra of degree f containing an f-th root of a. Although $D(2)$ holds for every cyclic algebra of degree 4 and exponent 2, $D(p)$ fails for Brauer algebras of degree p^2 and exponent p, and $D(2)$ fails for Brauer algebras of degree 8 and exponent 2. Using this, one fills the gap in [6, Theorem 4] and [7, Theorem 7.3.28], to show that the example given there is indeed tensor indecomposable of degree p^2 and exponent p. An easy ultraproduct argument provides an example containing all p^k roots of 1, for all k.

* Supported in part by the National Fund for Scientific Research (Belgium).
Received June 9, 1995

Introduction

The aim of this paper is to investigate the possible decompositions of cyclic division algebras into tensor products of cyclic subalgebras. More precisely, let K/F be a cyclic field extension of degree n and let σ be a generator of the Galois group $\mathrm{Gal}(K/F)$. For any element $a \in F^\times$, the cyclic algebra $(K/F, \sigma, a)$ is defined as

$$(K/F, \sigma, a) = K \oplus Kz \oplus \cdots \oplus Kz^{n-1}$$

where z is an indeterminate subject to the following relations:

$$\begin{aligned} zk &= \sigma(k)z \quad \text{for } k \in K, \\ z^n &= a. \end{aligned}$$

This algebra is central simple over F of degree n (i.e. dimension n^2). See [7] or [5, §30] for background information on cyclic algebras.

If $n = ef$, the element z^e centralizes the subfield $L \subset K$ elementwise invariant under σ^e, and the cyclic algebra $(K/F, \sigma, a)$ contains the commutative subalgebra

$$L(z^e) \simeq L \otimes_F F(z^e) \simeq L \otimes_F F\left(\sqrt[f]{a}\right).$$

We say that the cyclic algebra $(K/F, \sigma, a)$ has **property** $D(f)$ if it decomposes into a tensor product of a cyclic subalgebra of degree e containing L and a cyclic subalgebra of degree f containing an f-th root of a:

$$(K/F, \sigma, a) \simeq (L/F, \sigma, b) \otimes_F (M/F, \tau, a)$$

for some $b \in F^\times$ and some cyclic extension M/F of degree f.

Standard arguments reduce investigation of property $D(f)$ to the case where the degree n is a power of a prime (see Proposition 3 below). We show that property $D(f)$ is related to the existence of cyclic splitting fields of a particular type for certain cyclic algebras (see Proposition 4) and that property $D(2)$ holds for every cyclic algebra of degree 4 and exponent 2 (see Proposition 6). Our main result (Theorem 10) is that certain cyclic division algebras constructed by Brauer [2] yield examples of algebras of degree p^2 and exponent p which do not have property $D(p)$ for p any odd prime, and of algebras of degree 8 and exponent 2 which do not have property $D(2)$. In the last section, these algebras are used to produce indecomposable division algebras of prime exponent. For any odd prime p, we construct indecomposable division algebras of degree p^2 and

exponent p over a field of characteristic zero containing a primitive p-th root of unity. An ultraproduct construction yields examples where the base field contains a primitive p^n-th root of unity for all integer n.

1. Cohomological formulation of property $D(f)$

Let F be an arbitrary field. Fix some separable closure F_s of F and let $\Gamma_F = \mathrm{Gal}(F_s/F)$ denote the absolute Galois group of F. Recall that the Brauer group $\mathrm{Br}(F)$ is isomorphic to the second cohomology group $H^2(\Gamma_F, F_s^\times)$ under an isomorphism induced by the crossed-product construction:

$$\Delta\colon H^2(\Gamma_F, F_s^\times) \xrightarrow{\sim} \mathrm{Br}(F).$$

Let $X(F)$ denote the character group of Γ_F:

$$X(F) = \mathrm{Hom}(\Gamma_F, \mathbb{Q}/\mathbb{Z}) = H^2(\Gamma_F, \mathbb{Z}).$$

A character $\chi \in X(F)$ of order n takes values in the subgroup $(\frac{1}{n}\mathbb{Z})/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$ and defines a cyclic extension K/F of degree n consisting of the elements of F_s which are fixed under the subgroup $\ker\chi \subset \Gamma_F$; moreover, if $\gamma \in \Gamma_F$ is such that $\chi(\gamma) = 1/n \in \mathbb{Q}/\mathbb{Z}$, then the image of γ in $\Gamma_F/\ker\chi = \mathrm{Gal}(K/F)$ is a generator σ of $\mathrm{Gal}(K/F)$. For any $a \in F^\times = H^0(\Gamma_F, F_s^\times)$, the cup-product

$$\chi \cup a \in H^2(\Gamma_F, F_s^\times)$$

corresponds to the Brauer class of the cyclic algebra $(K/F, \sigma, a)$ under the isomorphism Δ.

If $n = ef$, the character $f\chi$ has order e; it defines the fixed subfield $L \subset K$ under σ^e. Therefore, the main property quoted in the introduction can be restated as follows:

> for $\chi \in X(F)$ and $a \in F^\times$, the cup-product $\chi \cup a$ satisfies property $D(f)$ if there is a decomposition
>
> $$\chi \cup a = f\chi \cup b + \theta \cup a \tag{1}$$
>
> for some $b \in F^\times$ and some $\theta \in X(F)$ of order f.

PROPOSITION 1: *The cup-products $\chi \cup a$ which have property $D(f)$ are killed by the least common multiple m of e and f. If e and f are relatively prime, then every cup-product $\chi \cup a$ has property $D(f)$.*

Proof: Since m kills both terms on the right-hand side of (1), it also kills the left-hand side. If e and f are relatively prime, then there are integers e', f' such that $ee' + ff' = 1$. Every cup-product $\chi \cup a$ may then be decomposed as

$$\chi \cup a = f\chi \cup a^{f'} + (ee'\chi) \cup a. \qquad \blacksquare$$

We next observe that the condition that the character θ in (1) has order f can be weakened to: $f\theta = 0$.

PROPOSITION 2: *Let $\chi \in X(F)$ be a character of order n and $a \in F^\times$. If*

$$\chi \cup a = f\chi \cup b + \theta \cup a \tag{2}$$

for some $b \in F^\times$ and some $\theta \in X(F)$ such that $f\theta = 0$, then $\chi \cup a$ satisfies property $D(f)$.

Proof: Let f' be the order of the character θ in (2); then f' divides f. Suppose $f = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ and $f' = p_1^{\alpha_1'} \cdots p_r^{\alpha_r'}$ are the prime factorizations of f and f'. We then have $\alpha_i' \leq \alpha_i$ for all $i = 1, \ldots, r$. Let

$$\psi_i = \begin{cases} p_i^{-\alpha_i} n(\chi - \theta) & \text{if } \alpha_i' < \alpha_i, \\ 0 & \text{if } \alpha_i' = \alpha_i. \end{cases}$$

If $\alpha_i' < \alpha_i$, then $p_i^{-1} n\theta = 0$, hence

$$p_i^{\alpha_i - 1} \psi_i = p_i^{-1} n\chi \neq 0.$$

Therefore, the order of ψ_i is $p_i^{\alpha_i}$ in this case. Moreover, multiplying both sides of (2) by $p_i^{-\alpha_i} n$, we get

$$p_i^{-\alpha_i} n(\chi - \theta) \cup a = 0,$$

hence

$$\psi_i \cup a = 0 \qquad \text{for } i = 1, \ldots, r.$$

Therefore, $\theta' = \psi_1 + \cdots + \psi_r + \theta$ has order f and satisfies $\theta' \cup a = \theta \cup a$. Substituting $\theta' \cup a$ for $\theta \cup a$ in (2), we see that $\chi \cup a$ satisfies property $D(f)$. $\blacksquare$

The next proposition yields the reduction to the prime power degree case announced in the introduction. Suppose $n = n_1 n_2$ where n_1 and n_2 are relatively prime. For e, f such that $ef = n$, consider the greatest common divisors:

$$e_1 = \gcd(e, n_1), \qquad f_1 = \gcd(f, n_1),$$
$$e_2 = \gcd(e, n_2), \qquad f_2 = \gcd(f, n_2),$$

so that

$$n_1 = e_1 f_1 \qquad \text{and} \qquad n_2 = e_2 f_2.$$

Let $m_1, m_2 \in \mathbb{Z}$ be such that $n_1 m_1 + n_2 m_2 = 1$.

PROPOSITION 3: *For any character $\chi \in X(F)$ of order n, set*

$$\chi_1 = n_2 m_2 \chi \qquad \text{and} \qquad \chi_2 = n_1 m_1 \chi,$$

so that $\chi_i \in X(F)$ has order n_i and

$$\chi = \chi_1 + \chi_2.$$

For $a \in F^\times$, the cup-product $\chi \cup a$ has property $D(f)$ if and only if $\chi_1 \cup a$ has property $D(f_1)$ and $\chi_2 \cup a$ has property $D(f_2)$.

Proof: Suppose first $\chi \cup a$ has property $D(f)$ and consider a decomposition

$$\chi \cup a = f\chi \cup b + \theta \cup a$$

for some $b \in F^\times$ and some $\theta \in X(F)$ such that $f\theta = 0$. Multiplying both sides of this equality by $n_2 m_2$ (resp. by $n_1 m_1$), we get

$$\chi_1 \cup a = f_1 \chi_1 \cup b^{f_2} + \theta_1 \cup a \qquad (\text{resp. } \chi_2 \cup a = f_2 \chi_2 \cup b^{f_1} + \theta_2 \cup a)$$

where $\theta_1 = n_2 m_2 \theta \in X(F)$ is such that $f_1 \theta_1 = 0$ and $\theta_2 = n_1 m_1 \theta \in X(F)$ is such that $f_2 \theta_2 = 0$. Therefore, $\chi_1 \cup a$ has property $D(f_1)$ and $\chi_2 \cup a$ has property $D(f_2)$.

Conversely, if $a \in F^\times$ is such that $\chi_1 \cup a$ has property $D(f_1)$ and $\chi_2 \cup a$ has property $D(f_2)$, then

$$\chi_1 \cup a = f_1 \chi_1 \cup b_1 + \theta_1 \cup a \qquad \text{and} \qquad \chi_2 \cup a = f_2 \chi_2 \cup b_2 + \theta_2 \cup a \tag{3}$$

for some $b_1, b_2 \in F^\times$ and some $\theta_1, \theta_2 \in X(F)$ such that $f_1 \theta_1 = f_2 \theta_2 = 0$. We have

$$f_1 \chi_1 \cup b_2^{e_1} = n_1 \chi_1 \cup b_2 = 0,$$

hence, multiplying by $f_2 m_1$:

$$f\chi_1 \cup b_2^{e_1 m_1} = 0. \tag{4}$$

On the other hand, since $n_1 m_1 + n_2 m_2 = 1$ we have $\chi_1 = n_2 m_2 \chi_1 = f_2(e_2 m_2)\chi_1$, hence

$$f_1 \chi_1 \cup b_1 = f\chi_1 \cup b_1^{e_2 m_2}.$$

Taking (4) into account, it follows that

$$f_1\chi_1 \cup b_1 = f\chi_1 \cup b_1^{e_2m_2} b_2^{e_1m_1}.$$

Similarly,

$$f_2\chi_2 \cup b_2 = f\chi_2 \cup b_1^{e_2m_2} b_2^{e_1m_1},$$

hence, adding the two equations in (3), we get

$$\chi \cup a = f\chi \cup b_1^{e_2m_2} b_2^{e_1m_1} + (\theta_1 + \theta_2) \cup a.$$

Since $f(\theta_1+\theta_2) = 0$, this relation shows that $\chi \cup a$ satisfies property $D(f)$. ∎

2. Cyclic splitting

As in the introduction, we denote by K/F a cyclic field extension of degree n and by L the unique intermediate subfield such that $[K : L] = f$, $[L : F] = e$. Assume $f \neq 1, n$. In view of Proposition 3, we further assume n is a power of a prime p.

PROPOSITION 4: *Let $a \in F^\times$. If the cyclic algebra $(K/F, \sigma, a)$ has property $D(f)$, then every cyclic algebra $(M/F, \tau, a)$ of degree dividing f is split by a cyclic extension K'/F of degree n containing L as an intermediate extension.*

Proof: Let $\chi \in X(F)$ denote the character of order n such that

$$\Delta(\chi \cup a) = (K/F, \sigma, a) \qquad \text{in } \mathrm{Br}(F).$$

Since property $D(f)$ is assumed to hold for $(K/F, \sigma, a)$, or equivalently for $\chi \cup a$, we have

$$\chi \cup a = f\chi \cup b + \theta \cup a \tag{5}$$

for some $b \in F^\times$ and some $\theta \in X(F)$ such that $f\theta = 0$.

For any $\psi \in X(F)$ such that $f\psi = 0$, let $\chi' = \chi - \theta + \psi \in X(F)$. Since $f\theta = f\psi = 0$, we have

$$f\chi' = f\chi;$$

since n is a prime power, it follows that χ' has order n, hence it defines a cyclic extension K'/F of degree n containing L. Moreover, from (5) it follows that

$$(\chi - \theta) \cup a = f\chi' \cup b = \chi' \cup b^f,$$

hence

$$\psi \cup a = \chi' \cup ab^{-f}.$$

Therefore, $\Delta(\psi \cup a)$ is split by K'. ∎

Note that the converse of Proposition 4 does not hold: if F is a local field, $a \in F$ is a uniformizing parameter and L/F is the (unique) unramified extension of degree e, then every cyclic algebra $(M/F, \tau, a)$ of degree dividing f is split by an extension of degree f of L which is cyclic over F, namely by the unramified extension K/F of degree n (see [8, Chapitre 12, §2]). However, $(K/F, \sigma, a)$ does not decompose, since its exponent is equal to its degree.

3. Algebras of degree 4

The aim of this section is to show that every cyclic algebra of degree 4 and exponent 2 has property $D(2)$. In the case where the characteristic is different from 2, this property also follows from general results concerning algebras of degree 4 and exponent 2: see [3, Proposition 5.2].

If the characteristic of the base field F is different from 2, then for $a, b \in F^\times$ we denote by $(a, b)_F$ the quaternion algebra generated by two elements i, j subject to

$$i^2 = a, \qquad j^2 = b, \qquad ji = -ij.$$

If the characteristic of F is 2, then for $a \in F$ and $b \in F^\times$ we denote by $[a, b)_F$ the quaternion algebra generated by two elements i, j subject to

$$\wp(i) = i^2 - i = a, \qquad j^2 = b, \qquad ji = ij + j.$$

LEMMA 5: *Let L/F be a quadratic field extension. For every character $\psi \in X(L)$ of order 2 and every $x \in L^\times$ there exist $\theta \in X(F)$ and $y \in F^\times$ such that $2\theta = 0$ and*

$$(\psi + \mathrm{res}_{L/F}(\theta)) \cup (xy) = 0.$$

Proof: We consider separately the cases where char. $F \neq 2$ and char. $F = 2$.

If char. $F \neq 2$, the cup-product $\psi \cup x$ represents a quaternion algebra $(\ell, x)_L$, for some $\ell \in L^\times$ such that $\ker \psi = \mathrm{Gal}(F_s/L(\sqrt{\ell}))$. We then have to show that there exist $f, y \in F^\times$ such that $(\ell f, xy)_L$ is split. If $x \in F^\times$, we may choose $f = 1$, $y = x$; similarly, if $\ell \in F^\times$ we may choose $f = \ell$, $y = 1$. If $x, \ell \notin F^\times$ we

may find $f, y \in F^\times$ such that $\ell f + xy = 0$ or 1, since the dimension of L over F is 2. The elements f, y then satisfy the required conditions.

If char. $F = 2$, the cup-product $\psi \cup x$ represents a quaternion algebra $[\ell, x)_L$ for some $\ell \in L$ such that $\ker \psi = \mathrm{Gal}(F_s/F(\wp^{-1}(\ell)))$; we have to show that there exist $f \in F$, $y \in F^\times$ such that $[\ell + f, xy)_L$ is split. If $x \in F^\times$, we may take $f = 0$, $y = x$; similarly, if $\ell \in F$ we may take $f = \ell$, $y = 1$. If $x, \ell \notin L$, then $1, \ell$ is a basis of L over F, hence we may find $f \in F$, $y \in F^\times$ such that $\ell = f + xy$. Then $[\ell + f, xy)_L = [xy, xy)_L$ is split. ∎

PROPOSITION 6: *Property $D(2)$ holds for every cyclic algebra of degree 4 and exponent 2.*

Proof: Let $\chi \in X(F)$ be a character of order 4 and let $a \in F^\times$. Let also L denote the quadratic field extension of F associated with 2χ. If $\chi \cup a$ has exponent 2, then $2\chi \cup a = 0$, hence a is a norm from L: let $a = N_{L/F}(x)$ for some $x \in L^\times$. The lemma shows that one can find $\theta \in X(F)$, $y \in F^\times$ such that $2\theta = 0$ and

$$\mathrm{res}_{L/F}(\chi + \theta) \cup (xy) = 0.$$

Taking the corestriction of both sides, we get by the projection formula:

$$(\chi + \theta) \cup N_{L/F}(xy) = 0.$$

Since $N_{L/F}(xy) = ay^2$ and $2\theta = 0$, it follows that

$$\chi \cup (ay^2) + \theta \cup a = 0,$$

hence

$$\chi \cup a = 2\chi \cup y + \theta \cup a. \qquad \blacksquare$$

Remark: The proposition above takes a very explicit form in the case where the base field F contains a primitive 4-th root of unity ζ_4. In that case, Kummer theory shows that every cyclic F-algebra of degree 4 is a symbol algebra $A_{\zeta_4}(a, b)_F$, i.e. an algebra generated by two elements i, j subject to

$$i^4 = a, \qquad j^4 = b, \qquad ji = \zeta_4 ij.$$

The algebra $A_{\zeta_4}(a, b)_F$ represents the image of the symbol $\{a, b\} \in K_2F$ under the norm-residue homomorphism $R_{\zeta_4} : K_2(F) \to \mathrm{Br}(F)$ (see [4]).

According to [4], we have

$$A_{\zeta_4}(a,b)_F^2 = (a,b)_F \qquad \text{in } \mathrm{Br}(F);$$

therefore, if $A_{\zeta_4}(a,b)_F$ has exponent 2, then $b = x^2 - ay^2$ for some $x, y \in F$. If $x, y \neq 0$, we have the following relations in K_2F:

$$\{a,b\} = \{a,x^2\} + \{a, 1 - a(x^{-1}y)^2\}$$

and

$$\{a, 1 - a(x^{-1}y)^2\} + \{(x^{-1}y)^2, 1 - a(x^{-1}y)^2\} = \{a(x^{-1}y)^2, 1 - a(x^{-1}y)^2\} = 0,$$

hence

$$\begin{aligned}\{a,b\} &= 2\{a,x\} - 2\{x^{-1}y, 1 - a(x^{-1}y)^2\} \\ &= 2\{a,x\} - 2\{x^{-1}y, b\} + 4\{x^{-1}y, x\}.\end{aligned}$$

Taking the image of both sides under the norm residue map, we get

$$A_{\zeta_4}(a,b)_F = (a,x)_F \otimes (x^{-1}y, b)_F.$$

4. Property $D(p)$

In this section,we investigate the case where K/F is an extension of prime-power degree p^n and $f = p$, assuming that the base field F contains a primitive p-th root of unity. We obtain various characterizations of property $D(p)$ which are used in the proof of Theorem 10 and in the construction of indecomposable algebras in section 7.

Throughout this section, we fix the following notation: p is a prime, ζ_p is a primitive p-th root of unity in F and K/F is a cyclic field extension of degree p^n (with $n \geq 2$). Let σ denote a generator of the Galois group $\mathrm{Gal}(K/F)$ and let L denote the intermediate field of codimension p in K. By Kummer theory, we have

$$K = L(\delta)$$

for some δ such that $\sigma^{p^{n-1}}(\delta) = \zeta_p\delta$. Let $d = \delta^p \in L^\times$.

LEMMA 7: *The element $\lambda = \sigma(\delta)\delta^{-1} \in K$ lies in $L^\times$ and satisfies*

$$\lambda^p = \sigma(d)d^{-1} \qquad \text{and} \qquad N_{L/F}(\lambda) = \zeta_p.$$

Every cyclic extension K'/F of degree p^n containing L has the form

$$K' = L(\sqrt[p^n]{fd}) \qquad \text{for some } f \in F^\times,$$

and every field extension of the form $L(\sqrt[p^n]{fd})$ with $f \in F^\times$ is cyclic of degree p^n over F.

Proof: We have

$$\sigma^{p^{n-1}}(\lambda) = \sigma^{p^{n-1}+1}(\delta)\sigma^{p^{n-1}}(\delta)^{-1} = \sigma(\zeta_p\delta)\,(\zeta_p\delta)^{-1} = \lambda,$$

hence $\lambda \in L^\times$. Raising both sides of the relation $\lambda = \sigma(\delta)\delta^{-1}$ to the p-th power, we get $\lambda^p = \sigma(d)d^{-1}$. Moreover,

$$N_{L/F}(\lambda) = \prod_{i=0}^{p^{n-1}-1} \sigma^i(\lambda) = \prod_{i=0}^{p^{n-1}-1} [\sigma^{i+1}(\delta)\sigma^i(\delta)^{-1}] = \sigma^{p^{n-1}}(\delta)\delta^{-1} = \zeta_p.$$

(Compare [1, p. 206].)

Suppose K'/F is a cyclic field extension of degree p^n containing L, and let σ' be a generator of $\mathrm{Gal}(K'/F)$ such that $\sigma'|_L = \sigma|_L$. We also have $K' = L(\delta')$ for some δ' such that $\sigma'^{p^{n-1}}(\delta') = \zeta_p\delta'$. Let $d' = \delta'^p$ and $\lambda' = \sigma'(\delta')\delta'^{-1}$. Arguing as above, we see $\lambda' \in L^\times$ and $N_{L/F}(\lambda') = \zeta_p$. Therefore, $N_{L/F}(\lambda'\lambda^{-1}) = 1$, and Hilbert's Theorem 90 yields an element $u \in L^\times$ such that

$$\lambda'\lambda^{-1} = \sigma(u)u^{-1}.$$

Raising both sides to the p-th power, we get

$$\sigma(d')d'^{-1} \cdot d\sigma(d)^{-1} = \sigma(u)^p u^{-p},$$

hence $d'd^{-1}u^{-p} \in F^\times$. Letting $f = d'd^{-1}u^{-p}$, we have $d' \equiv fd \bmod L^{\times p}$, hence

$$K' = L(\sqrt[p^n]{d'}) = L(\sqrt[p^n]{fd}).$$

Conversely, if $d' = fd$ for some $f \in F^\times$, then $d' \notin L^{\times p}$, since otherwise $d \equiv f^{-1} \bmod L^{\times p}$, hence $L(\sqrt[p^n]{d}) \simeq L \otimes_F F(\sqrt[p^n]{f^{-1}})$ is not cyclic over F. Since $\sigma(d')d'^{-1} = \sigma(d)d^{-1} = \lambda^p$, there is an F-automorphism of $L(\sqrt[p^n]{d'})$ which extends σ and maps $\sqrt[p^n]{d'}$ to $\lambda\sqrt[p^n]{d'}$. This proves $L(\sqrt[p^n]{d'})$ is cyclic over F. ∎

Let $\hat{F} = F((t))$ and $\hat{L} = L((t))$ be the power series fields in one indeterminate t over F and L respectively. Let $a \in F^\times$. We denote by $A_{\zeta_p}(t,a)_{\hat{F}}$ the symbol algebra over $\hat{F}$ generated by two elements i, j subject to

$$i^p = t, \qquad j^p = a, \qquad ji = \zeta_p ij.$$

If $a \notin L^{\times p}$, we also let $L^\sharp = L(\sqrt[p]{a})$ and $F^\sharp = F(\sqrt[p]{a})$.

PROPOSITION 8: *With the notation above, the following conditions are equivalent:*

(i) *The cyclic algebra $A = (K/F, \sigma, a)$ satisfies property $D(p)$.*

(ii) *Either $a \in L^{\times p}$ or there exists $x \in L^\sharp$ such that*

$$N_{L^\sharp/F^\sharp}(x) = \zeta_p \qquad \text{and} \qquad N_{L^\sharp/L}(x) = 1.$$

(iii) *Either $a \in L^{\times p}$ or $d \in F^\times \cdot N_{L^\sharp/L}(L^\sharp)$.*

(iv) *The symbol algebra $A_{\zeta_p}(t, a)_{\hat{F}}$ is split by an extension of degree p of $\hat{L}$ which is cyclic over $\hat{F}$.*

Proof: (i) $\Rightarrow$ (ii): Suppose $a \notin L^{\times p}$ and

$$A \simeq (L/F, \sigma, b) \otimes A_{\zeta_p}(u, a)_F$$

for some $u \in F^\times$. Extending scalars to L, we get

$$A_L = A_{\zeta_p}(u, a)_L \qquad \text{in } \mathrm{Br}(L).$$

On the other hand, A_L is also Brauer-equivalent to the centralizer of L in A, which is

$$(K/L, \sigma^{p^{n-1}}, a) = A_{\zeta_p}(d, a)_L.$$

Therefore, $A_{\zeta_p}(du^{-1}, a)_L$ is split, which means that there exists $y \in L^\sharp$ such that

$$N_{L^\sharp/L}(y) = du^{-1}.$$

Let $x = \lambda y \sigma(y)^{-1} \in L^\sharp$, where λ is defined in Lemma 7. Straightforward calculations yield

$$N_{L^\sharp/F^\sharp}(x) = N_{L/F}(\lambda) = \zeta_p$$

and

$$\begin{aligned} N_{L^\sharp/L}(x) &= \lambda^p \, N_{L^\sharp/L}(y) \, \sigma(N_{L^\sharp/L}(y))^{-1} \\ &= \sigma(d) d^{-1} \, du^{-1} \, \sigma(du^{-1})^{-1} \\ &= 1. \end{aligned}$$

(ii) $\Rightarrow$ (iii): Suppose $a \notin L^{\times p}$. If $x \in L^\sharp$ is such that

$$N_{L^\sharp/F^\sharp}(x) = \zeta_p \qquad \text{and} \qquad N_{L^\sharp/L}(x) = 1,$$

then $N_{L^\sharp/F^\sharp}(x\lambda^{-1}) = 1$, hence Hilbert's Theorem 90 yields an element $y \in L^\sharp$ such that

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

From the relation $N_{L^\sharp/L}(x) = 1$ it follows that

$$\sigma(N_{L^\sharp/L}(y))\, N_{L^\sharp/L}(y)^{-1} = \lambda^p = \sigma(d)d^{-1},$$

hence $N_{L^\sharp/L}(y)d^{-1} \in F^\times$. This shows $d \in F^\times \cdot N_{L^\sharp/L}(L^\sharp)$.

(iii) $\Rightarrow$ (iv): If $a \in L^{\times p}$, then the algebra $A_{\zeta_p}(t,a)_{\hat{F}}$ is split by $K((t))$, since it is already split by $L((t))$. If $d = f\, N_{L^\sharp/L}(y)$ for some $f \in F^\times$ and some $y \in L^{\sharp\times}$, then the symbol algebra $A_{\zeta_p}(df^{-1},a)_L$ is split, hence

$$A_{\zeta_p}(t,a)_{\hat{L}} \simeq A_{\zeta_p}(dtf^{-1},a)_{\hat{L}}.$$

Therefore, the algebra $A_{\zeta_p}(t,a)_{\hat{F}}$ is split by $\hat{L}(\sqrt[p]{dtf^{-1}})$, which by Lemma 7 is an extension of degree p of $\hat{L}$ cyclic over $\hat{F}$.

(iv) $\Rightarrow$ (i): Let M be an extension of degree p of $\hat{L}$ which is cyclic over $\hat{F}$ and splits $A_{\zeta_p}(t,a)_{\hat{F}}$. By Lemma 7, we have $M = \hat{L}(\sqrt[p]{fd})$ for some $f \in \hat{F}^\times$. Since $\hat{F}$ is Henselian with respect to the t-adic valuation and char. $F \neq p$, every equation $X^p - (1+ts) = 0$ with $s \in F[[t]]$ has a solution in $F[[t]]$, hence the elements in $1 + tF[[t]]$ are p-th powers. Therefore, multiplying f by a p-th power in $\hat{F}$ if necessary, we may assume $f = f_0t^j$ for some $f_0 \in F^\times$ and some $j \in \mathbb{Z}$:

$$M = \hat{L}\left(\sqrt[p]{f_0dt^j}\right).$$

Since f_0dt^j is a p-th power in M, the algebra $A_{\zeta_p}(f_0dt^j,a)_M$ is split. Since by hypothesis $A_\zeta(t,a)_M$ is split, it follows that M splits $A_{\zeta_p}(f_0d,a)_F$. Let $\overline{M}$ denote the residue field of M for the extension of the t-adic valuation. Witt's exact sequence for the Brauer group of a complete discretely valued field (see [8, Chapitre 12, §3]) shows that the p-torsion part of $\mathrm{Br}(\overline{M})$ injects into $\mathrm{Br}(M)$; therefore, $A_{\zeta_p}(f_0d,a)_F$ splits over $\overline{M}$.

We claim that $A_{\zeta_p}(f_0d,a)_F$ splits over L. This is clear if $j \not\equiv 0 \bmod p$, because then M is totally ramified over $\hat{L}$, hence $\overline{M} = \overline{\hat{L}} = L$.

Suppose $j \equiv 0 \bmod p$. Then $M = L(\sqrt[p]{f_0d})((t))$. If $a \notin M^{\times p}$, then the equation $t = N_{M(\sqrt[p]{a})/M}(s)$ has no solution $s \in M(\sqrt[p]{a})$, since taking the image of both sides under the t-adic valuation would yield $1 \in p\mathbb{Z}$. Therefore, $a \in M^{\times p}$, hence M contains $F(\sqrt[p]{a})((t))$; but M is cyclic over $F((t))$, hence it contains a unique

extension of degree p of $F((t))$, and this extension is contained in $\hat{L}$. Therefore, we have in this case

$$F(\sqrt[p]{a})((t)) \subset \hat{L},$$

hence $a \in L^{\times p}$, and L splits $A_{\zeta_p}(f_0 d, a)_F$. This proves the claim.

We have thus proved that $A_{\zeta_p}(f_0 d, a)_L$ is split, hence

$$A_{\zeta_p}(d, a)_L \simeq A_{\zeta_p}(f_0^{-1}, a)_F \otimes L.$$

Now, as observed at the beginning of the proof, A_L is Brauer-equivalent to $A_{\zeta_p}(d, a)_L$. Therefore, $A \otimes_F A_{\zeta_p}(f_0, a)_F$ is split by L, hence

$$A \simeq (L/F, \sigma, b) \otimes_F A_{\zeta_p}(f_0^{-1}, a)_F$$

for some $b \in F^\times$. This proves that A satisfies property $D(p)$. ∎

5. A technical lemma

Let α, β be automorphisms of order a, b respectively of some field M. Assume α and β generate a group G of automorphisms of M which is isomorphic to $(\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$. For $\gamma \in G$ of order g and $x \in M^\times$, we let

$$N_\gamma(x) = x \cdot \gamma(x) \cdot \cdots \cdot \gamma^{g-1}(x).$$

Assume M is the field of fractions of some unique factorization domain D preserved under α and β. These automorphisms therefore induce well-defined automorphisms of the factor group $M^\times/D^\times$, where $D^\times$ denotes the groups of units of D. We shall also use the notation $N_\gamma(\xi)$ for $\xi \in M^\times/D^\times$, although it could be written more precisely as $D^\times N_\gamma(\xi)$.

Consider the following condition:

(*) For all $r \in D^\times$ and $\gamma \in G$ such that $N_\gamma(r) = 1$, there exists $u \in D^\times$ such that $N_\alpha(u) = N_\alpha(r)$ and $N_\beta(u) = 1$.

This condition is actually symmetric in α and β; indeed, if $u \in D^\times$ satisfies the relations above, then $u' = u^{-1}r$ satisfies $N_\alpha(u') = 1$ and $N_\beta(u') = N_\beta(r)$. It automatically holds if γ is in the subgroup generated by α or in the subgroup generated by β: if for instance γ is in the subgroup generated by α, then $N_\gamma(r) = 1$ implies $N_\alpha(r) = 1$, hence the relations above hold with $u = 1$.

LEMMA 9: *If condition (*) holds, then every $\xi \in M^\times/D^\times$ such that $N_\alpha(\xi) = N_\beta(\xi) = 1$ has a representative $x \in M^\times$ such that $N_\alpha(x) = N_\beta(x) = 1$.*

Proof: By hypothesis, $M^\times/D^\times$ is a free abelian group with a basis consisting of the images $\overline{P}$ of irreducible elements $P \in D$. Each element $\prod \overline{P}^{n(P)} \in M^\times/D^\times$ has a well-defined length:

$$\ell(\prod \overline{P}^{n(P)}) = \sum n(P),$$

and since D is stable under α,

$$\ell(N_\alpha(\xi)) = a\,\ell(\xi)$$

for $\xi \in M^\times/D^\times$. Therefore, if ξ is such that $N_\alpha(\xi) = N_\beta(\xi) = 1$, then $\ell(\xi) = 0$. Let

$$\xi = \frac{\overline{P_1} \cdots \overline{P_n}}{\overline{Q_1} \cdots \overline{Q_n}}$$

where $P_1, \ldots, P_n, Q_1, \ldots, Q_n$ are irreducible elements in D.

If $n = 0$, then 1 is a representative of ξ and $N_\alpha(1) = N_\beta(1) = 1$; we then argue by induction on n.

The equations $N_\alpha(\xi) = N_\beta(\xi) = 1$ yield

$$N_\alpha(\overline{P_1} \cdots \overline{P_n}) = N_\alpha(\overline{Q_1} \cdots \overline{Q_n}), \qquad N_\beta(\overline{P_1} \cdots \overline{P_n}) = N_\beta(\overline{Q_1} \cdots \overline{Q_n}).$$

The first equation can be written as

$$\prod_{i=0}^{a-1} \alpha^i(\overline{P_1}) \cdots \alpha^i(\overline{P_n}) = \prod_{i=0}^{a-1} \alpha^i(\overline{Q_1}) \cdots \alpha^i(\overline{Q_n}).$$

Each of the factors $\alpha^i(\overline{P_j})$, $\alpha^i(\overline{Q_k})$ is the image in $M^\times/D^\times$ of an irreducible element in D; therefore, by the unique factorization property, each $\overline{P_i}$ must be equal to some $\alpha^j(\overline{Q_k})$. Changing the numbering of $\overline{Q_1}, \ldots, \overline{Q_n}$ if necessary, we may assume that for all $i = 1, \ldots, n$,

$$\overline{P_i} = \alpha^{a(i)}(\overline{Q_i}) \qquad \text{for some } a(i) = 0, \ldots, a-1.$$

Similarly, from the second equation it follows that each $\overline{P_i}$ is equal to some $\beta^j(\overline{Q_k})$, so that there is a permutation π of $\{1, \ldots, n\}$ such that for all $i = 1, \ldots, n$,

$$\overline{P_i} = \beta^{b(i)}(\overline{Q_{\pi(i)}}) \qquad \text{for some } b(i) = 0, \ldots, b-1.$$

If the permutation π is not a cycle, then one can decompose

$$\{1,\dots,n\} = I_1 \cup I_2$$

where I_1, I_2 are non-empty disjoint subsets preserved by π; then

$$N_\alpha\left(\prod_{i\in I_k}\overline{P_i}\right) = N_\alpha\left(\prod_{i\in I_k}\overline{Q_i}\right) \text{ and } N_\beta\left(\prod_{i\in I_k}\overline{P_i}\right) = N_\beta\left(\prod_{i\in I_k}\overline{Q_i}\right) \text{ for } k = 1,2.$$

By the induction hypothesis, one can find a representative x_k of $\prod_{i\in I_k}(\overline{P_i}/\overline{Q_i})$ in $M^\times$ such that $N_\alpha(x_k) = N_\beta(x_k) = 1$; then x_1x_2 is a representative of ξ, and $N_\alpha(x_1x_2) = N_\beta(x_1x_2) = 1$.

We may thus assume that π is a cycle*. Changing the numbering of $\overline{P_1},\dots,\overline{P_n}$, $\overline{Q_1},\dots,\overline{Q_n}$ again, we may assume that $\pi(i) = i+1 \bmod n$ for $i = 1,\dots,n$. Since

$$\overline{P_i} = \beta^{b(i)}(\overline{Q_{i+1}}) \qquad \text{for } i = 1,\dots,n \pmod n,$$

we can choose $\beta^{b(i)}(Q_{i+1})$ as a representative of $\overline{P_i}$ for $i = 1,\dots,n \pmod n$. We shall therefore assume moreover that

$$P_i = \beta^{b(i)}(Q_{i+1}) \qquad \text{for } i = 1,\dots,n \pmod n. \tag{6}$$

The equation $\overline{P_i} = \alpha^{a(i)}(\overline{Q_i})$ now yields elements $r_i \in D^\times$ such that

$$\alpha^{a(i)}(Q_i) = r_iP_i \qquad \text{for } i = 1,\dots,n. \tag{7}$$

By (6), it follows that

$$\alpha^{a(i)}(Q_i) = r_i\beta^{b(i)}(Q_{i+1}) \qquad \text{for } i = 1,\dots,n \pmod n.$$

Eliminating $Q_2,\dots,Q_n$, we get

$$\alpha^{a(1)+\cdots+a(n)}(Q_1) = \left[\prod_{\ell=1}^{n}\alpha^{a(\ell+1)+\cdots+a(n)}\beta^{b(1)+\cdots+b(\ell-1)}(r_\ell)\right]\beta^{b(1)+\cdots+b(n)}(Q_1).$$

Let

$$\begin{aligned} r &= \alpha^{a(1)+\cdots+a(n)}(Q_1)\,\beta^{b(1)+\cdots+b(n)}(Q_1)^{-1} \\ &= \prod_{\ell=1}^{n}\alpha^{a(\ell+1)+\cdots+a(n)}\beta^{b(1)+\cdots+b(\ell-1)}(r_\ell) \end{aligned} \tag{8}$$

* If $n = 1$, the identity is regarded as a cycle.

and $\gamma = \alpha^{a(1)+\cdots+a(n)}\beta^{-(b(1)+\cdots+b(n))} \in G$; then

$$r = \gamma(Q)Q^{-1} \quad \text{for } Q = \beta^{b(1)+\cdots+b(n)}(Q_1),$$

hence $N_\gamma(r) = 1$. Moreover, (8) shows that $r \in D^\times$; therefore, condition $(*)$ yields $u \in D^\times$ such that $N_\alpha(u) = N_\alpha(r)$ and $N_\beta(u) = 1$.

Solving for r_n in (8) yields

$$\begin{aligned} r_n =& \beta^{-(b(1)+\cdots+b(n-1))}\left[\prod_{\ell=1}^{n-1}\alpha^{a(\ell+1)+\cdots+a(n)}\beta^{b(1)+\cdots+b(\ell-1)}(r_\ell)\right]^{-1} \\ & \times \beta^{-(b(1)+\cdots+b(n-1))}(r) \\ =& \left[\prod_{\ell=1}^{n-1}\alpha^{a(\ell+1)+\cdots+a(n)}\beta^{-(b(\ell)+\cdots+b(n-1))}(r_\ell)\right]^{-1}\beta^{-(b(1)+\cdots+b(n-1))}(r). \end{aligned}$$

Applying N_α and multiplying both sides by $N_\alpha(r_1\cdots r_{n-1})$ yields

$$\begin{aligned} N_\alpha(r_1\cdots r_n) = & \left[\prod_{\ell=1}^{n-1} N_\alpha(r_\ell)\,\beta^{-(b(\ell)+\cdots+b(n-1))}(N_\alpha(r_\ell))^{-1}\right] \\ & \times \beta^{-(b(1)+\cdots+b(n-1))}(N_\alpha(r)). \end{aligned}$$

Let then

$$v = \left[\prod_{\ell=1}^{n-1} r_\ell\,\beta^{-(b(\ell)+\cdots+b(n-1))}(r_\ell)^{-1}\right]\beta^{-(b(1)+\cdots+b(n-1))}(u).$$

Since $N_\alpha(r) = N_\alpha(u)$, we have $N_\alpha(v) = N_\alpha(r_1\cdots r_n)$; on the other hand, since $N_\beta(u) = 1$ it follows that $N_\beta(v) = 1$.

Consider then

$$x = v\frac{P_1\cdots P_n}{Q_1\cdots Q_n} \in M^\times.$$

Clearly, x is a representative of ξ in $M^\times$. From (6), it follows that

$$N_\beta(x) = N_\beta(v)\frac{N_\beta(P_1)\cdots N_\beta(P_n)}{N_\beta(Q_1)\cdots N_\beta(Q_n)} = 1,$$

and from (7)

$$N_\alpha(u) = N_\alpha(v)\frac{N_\alpha(P_1)\cdots N_\alpha(P_n)}{N_\alpha(Q_1)\cdots N_\alpha(Q_n)} = \frac{N_\alpha(v)}{N_\alpha(r_1\cdots r_n)} = 1. \qquad \blacksquare$$

Note that the converse of Lemma 9 holds: if $r \in D^\times$ is such that $N_\gamma(r) = 1$ with $\gamma = \alpha^s\beta^t$, then Hilbert's Theorem 90 yields an element $x \in M^\times$ such that $r = x\gamma(x)^{-1}$. Let then

$$y = \frac{\gamma(x)}{\alpha^s(x)} = \frac{\beta^t\alpha^s(x)}{\alpha^s(x)} = \frac{x}{\alpha^s(x)}r^{-1};$$

we have $N_\alpha(y) = N_\alpha(r^{-1}) \in D^\times$ and $N_\beta(y) = 1$, so

$$N_\alpha(\overline{y}) = N_\beta(\overline{y}) = 1 \qquad \text{in } M^\times/D^\times.$$

If one can find a representative z of y in $M^\times$ such that $N_\alpha(z) = N_\beta(z) = 1$, then $z = uy$ for some $u \in D^\times$ such that $N_\alpha(u) = N_\alpha(r)$ and $N_\beta(u) = 1$. Therefore, condition $(*)$ holds.

6. Brauer algebras

Interesting examples of cyclic algebras were constructed by Brauer in [2]. We investigate their possible decomposition.

We first recall Brauer's construction, following [7, §7.3]. Throughout this section, q, n and t denote powers of a prime p. We let $\zeta_q = e^{2i\pi/q} \in \mathbb{C}$ and consider the field of rational fractions:

$$E_{q,t} = \mathbb{Q}(\zeta_q)(\mu_1, \ldots, \mu_t),$$

where $\mu_1, \ldots, \mu_t$ are independent indeterminates. Let σ denote the automorphism of $E_{q,t}$ which permutes $\mu_1, \ldots, \mu_t$ cyclically and leaves ζ_q invariant. If $n \leq t$, we denote by $K_{q,n,t}$ the subfield of $E_{q,t}$ elementwise invariant under σ^n, and we set

$$R_{q,n,t} = (K_{q,n,t}/K_{q,1,t}, \sigma, \zeta_q).$$

According to [7, Theorem 7.3.8], the cyclic algebra $R_{q,n,t}$ is a division algebra of degree n and exponent qn/t, whenever $n \leq t < qn$.

Our main result is the following:

THEOREM 10: *If p is odd and $q \geq p$, the cyclic algebra $R_{q,p^2,pq}$ does not satisfy property $D(p)$. The cyclic algebra $R_{2,8,8}$ does not satisfy property $D(2)$.*

Proof: Suppose first that p is odd. For convenience of notation, we simply denote $K = K_{q,p^2,pq}$, $L = K_{q,p,pq}$ and $F = K_{q,1,pq}$, so that

$$F \subset L \subset K$$

is a tower of extensions of degree p. Let also $L^\sharp = L(\sqrt[p]{\zeta_q}) = K_{pq,p,pq}$ and $F^\sharp = F(\sqrt[p]{\zeta_q}) = K_{pq,1,pq}$. In order to show that $R_{q,p^2,pq}$ does not satisfy property $D(p)$, it suffices by Proposition 8 to show that there is no $z \in L^\sharp$ such that

$$N_{L^\sharp/F^\sharp}(z) = \zeta_p \qquad \text{and} \qquad N_{L^\sharp/L}(z) = 1. \tag{9}$$

(Note that if $q = p = 2$ we have $N_{L^\sharp/F^\sharp}(\zeta_4) = \zeta_2$ and $N_{L^\sharp/L}(\zeta_4) = 1$.)

The following notation will enable us to describe explicitly the field $L^\sharp$: for $i = 1, \dots, p$ and $j = 0, \dots, q-1$, let

$$\lambda_i(\zeta_q^j) = \mu_i + \zeta_q^j \mu_{i+p} + \zeta_q^{2j} \mu_{i+2p} + \cdots + \zeta_q^{(q-1)j} \mu_{i+(q-1)p} \in E_{q,pq}$$

and

$$x_{ij} = \lambda_i(\zeta_q^j)\lambda_1(\zeta_q)^{-j}.$$

We have

$$\sigma^p(\lambda_i(\zeta_q^j)) = \zeta_q^{-j}\lambda_i(\zeta_q^j),$$

hence $x_{ij} \in L$ for $i = 1, \dots, p$ and $j = 0, \dots, q-1$. Let

$$X = \{x_{ij} \mid 1 \le i \le p,\ 0 \le j \le q-1,\ (i,j) \ne (1,1)\}.$$

(Observe that $x_{1,1} = 1$.) For $i = 1, \dots, p$ and $k = 0, \dots, q-1$, we have

$$\mu_{i+kp} = \frac{1}{q} \sum_{j=0}^{q-1} \zeta_q^{-jk} \lambda_i(\zeta_q^j),$$

hence

$$E_{q,pq} = \mathbb{Q}(\zeta_q)(\lambda_i(\zeta_q^j) \mid 1 \le i \le p,\ 0 \le j \le q-1) = \mathbb{Q}(\zeta_q)(X, \lambda_1(\zeta_q))$$

and

$$\begin{aligned} L &= \mathbb{Q}(\zeta_q)(X, \lambda_1(\zeta_q)^q), \\ L^\sharp &= \mathbb{Q}(\zeta_{pq})(X, \lambda_1(\zeta_q)^q). \end{aligned} \tag{10}$$

Let β denote the automorphism of $E_{pq,pq}/E_{q,pq}$ defined by

$$\beta(\zeta_{pq}) = \zeta_{pq}^{1+q}.$$

We also denote by β the restriction of this automorphism to $L^\sharp$ and we let $\alpha = \sigma|_{L^\sharp}$. The automorphisms α and β are of order p and generate the Galois group $\mathrm{Gal}(L^\sharp/F) \simeq (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$. Direct computations yield:

$$\sigma(\lambda_i(\zeta_q^j)) = \begin{cases} \lambda_{i+1}(\zeta_q^j) & \text{for } i = 1, \dots, p-1, \\ \zeta_q^{-j}\lambda_1(\zeta_q^j) & \text{for } i = p, \end{cases}$$

hence

$$\alpha(x_{ij}) = \begin{cases} x_{i+1,j}x_{2,1}^{-j} & \text{for } i = 1, \dots, p-1 \\ \zeta_q^{-j}x_{1,j}x_{2,1}^{-j} & \text{for } i = p \end{cases}$$

and

$$\alpha(\lambda_1(\zeta_q)^q) = x_{2,1}^q \lambda_1(\zeta_q)^q.$$

Let

$$y_\ell = x_{1+\ell,1} \qquad \text{for } \ell = 1, \dots, p-1$$

and

$$X' = \{x_{ij} \mid 1 \le i \le p,\ 0 \le j \le q-1,\ j \ne 1\};$$

let also

$$D = \mathbb{Q}(\zeta_{pq})[X', y_1^{\pm 1}, \dots, y_{p-1}^{\pm 1}, \lambda_1(\zeta_q)^q].$$

This ring is a (Laurent) polynomial ring over $\mathbb{Q}(\zeta_{pq})$; it is therefore a unique factorization domain. Moreover, (10) shows that $L^\sharp$ is the field of fractions of D, and the calculations above show that it is stable under α. Since the indeterminates are in L, the ring D is also clearly preserved under β.

We proceed to show that condition $(*)$ of the preceding section holds. We have

$$D^\times = \{c y_1^{n_1} \cdots y_{p-1}^{n_{p-1}} \mid c \in \mathbb{Q}(\zeta_{pq})^\times,\ n_1, \dots, n_{p-1} \in \mathbb{Z}\}.$$

Suppose $\gamma \in \mathrm{Gal}(L^\sharp/F)$ and $r = c y_1^{n_1} \cdots y_{p-1}^{n_{p-1}}$ are such that

$$N_\gamma(r) = 1. \tag{11}$$

We have to show that there exists $u \in D^\times$ such that $N_\alpha(u) = N_\alpha(r)$ and $N_\beta(u) = 1$. As observed in the preceding section, this is easy if γ is in the subgroup generated by α or in the subgroup generated by β. If it is not in any of these subgroups, then $N_\gamma(c) = N_\beta(c)$ and $N_\gamma(y_i) = N_\alpha(y_i) = \zeta_q^{-i}$. Therefore, equation (11) yields

$$N_\beta(c) = \zeta_q^{n_1 + 2n_2 + \cdots + (p-1)n_{p-1}}.$$

Since p is odd, we have $N_\beta(\zeta_{pq}) = \zeta_q = \zeta_{pq}^p$; therefore, for

$$u = c\,\zeta_{pq}^{-(n_1+2n_2+\cdots+(p-1)n_{p-1})}$$

we have

$$N_\alpha(u) = c^p N_\alpha(y_1)^{n_1} \cdots N_\alpha(y_{p-1})^{n_{p-1}} = N_\alpha(r)$$

and

$$N_\beta(u) = N_\beta(c)\,\zeta_q^{-(n_1+2n_2+\cdots+(p-1)n_{p-1})} = 1,$$

as required.

Suppose now that $z \in L^\sharp$ satisfies (9). Then

$$N_\alpha(z \cdot D^\times) = N_\beta(z \cdot D^\times) = 1 \quad \text{in } L^{\sharp\times}/D^\times,$$

hence Lemma 9 shows that $z \cdot D^\times = z' \cdot D^\times$ for some $z' \in L^\sharp$ such that $N_\alpha(z') = N_\beta(z') = 1$. Let $z' = zv$ with $v \in D^\times$; then v satisfies

$$N_\alpha(v) = N_\alpha(z')N_\alpha(z)^{-1} = \zeta_q^{-1} \qquad \text{and} \qquad N_\beta(v) = N_\beta(z')N_\beta(z)^{-1} = 1.$$

But $v = cy_1^{n_1} \cdots y_{p-1}^{n_{p-1}}$ for some $c \in \mathbb{Q}(\zeta_{pq})^\times$ and some $n_1, \ldots, n_{p-1} \in \mathbb{Z}$, hence

$$N_\alpha(v) = c^p \zeta_q^{-(n_1+2n_2+\cdots+(p-1)n_{p-1})} \qquad \text{and} \qquad N_\beta(v) = N_\beta(c) y_1^{pn_1} \cdots y_{p-1}^{pn_{p-1}}.$$

Therefore, we must have $n_1 = \cdots = n_{p-1} = 0$,

$$c^p = \zeta_q^{-1} \qquad \text{and} \qquad N_\beta(c) = 1.$$

This is impossible, since the condition $c^p = \zeta_q^{-1}$ implies $N_\beta(c) = c^p$. This completes the proof in the case where p is odd.

Suppose next $p = 2$. For convenience of notation, denote $K = K_{2,8,8}$, $L = K_{2,4,8}$ and $F = K_{2,1,8}$, so that L is the intermediate extension of codimension 2 in K/F. Let also $L^\sharp = L(\sqrt{-1}) = K_{4,4,8}$ and $F^\sharp = F(\sqrt{-1}) = K_{4,1,8}$. In order to show that $R_{2,8,8}$ does not have property $D(2)$, Proposition 8 shows that it suffices to prove that there is no $z \in L^\sharp$ such that

$$N_{L^\sharp/F^\sharp}(z) = -1 \qquad \text{and} \qquad N_{L^\sharp/L}(z) = 1. \tag{12}$$

We again give an explicit description of $L^\sharp$. For $i = 1, \ldots, 4$, let

$$x_i = \mu_i + \mu_{i+4} \in L, \qquad \lambda_i = \mu_i - \mu_{i+4} \in K$$

and let

$$y_i = \lambda_{i+1}\lambda_1^{-1} \qquad \text{for } i = 1, 2, 3.$$

Since $\sigma^4(\lambda_i) = -\lambda_i$, we have $y_i \in L$. Clearly,

$$K = \mathbb{Q}(x_1, \ldots, x_4, \lambda_1, \ldots, \lambda_4) = \mathbb{Q}(x_1, \ldots, x_4, y_1, y_2, y_3, \lambda_1),$$

$$L = \mathbb{Q}(x_1, \ldots, x_4, y_1, y_2, y_3, \lambda_1^2) \quad \text{and} \quad L^\sharp = \mathbb{Q}(\zeta_4)(x_1, \ldots, x_4, y_1, y_2, y_3, \lambda_1^2).$$

Let $\alpha = \sigma|_{L^\sharp}$ and let β be the non-trivial automorphism of $L^\sharp/L$. The orders of α and β are 4 and 2 respectively, and these automorphisms generate $\mathrm{Gal}(L^\sharp/F)$. Straightforward computations show that

$$\alpha(x_i) = x_{i+1} \qquad \text{for } i = 1, \ldots, 4 \pmod 4,$$

$$\alpha(y_1) = y_2 y_1^{-1}, \qquad \alpha(y_2) = y_3 y_1^{-1}, \qquad \alpha(y_3) = -y_1^{-1}$$

and

$$\alpha(\lambda_1^2) = y_1^2 \lambda_1^2.$$

Therefore, the ring

$$D = \mathbb{Q}(\zeta_4)[x_1, \ldots, x_4, y_1^{\pm 1}, y_2^{\pm 1}, y_3^{\pm 1}, \lambda_1^2]$$

is a unique factorization domain which is preserved under α and β and whose field of fractions is $L^\sharp$.

We check condition $(*)$: suppose $r = c y_1^{n_1} y_2^{n_2} y_3^{n_3}$ with $c \in \mathbb{Q}(\zeta_4)^\times$ and $n_1, n_2, n_3 \in \mathbb{Z}$, and $\gamma \in \mathrm{Gal}(L^\sharp/F)$ are such that $N_\gamma(r) = 1$. We have to find $u \in D^\times$ such that $N_\alpha(u) = N_\alpha(r)$ and $N_\beta(u) = 1$. As noticed in the preceding section, this is straightforward if γ is in the subgroup generated by α or in the subgroup generated by β. If $\gamma = \alpha\beta$ or $\alpha^3\beta$, then

$$N_\gamma(r) = N_\beta(c)\,(-1)^{n_1+n_3}.$$

Since β is the complex conjugation on $\mathbb{Q}(\zeta_4)$, we have $N_\beta(c) > 0$, hence the relation $N_\gamma(r) = 1$ implies $n_1 + n_3$ is even and $N_\beta(c) = 1$. We may then choose $u = c$. If $\gamma = \alpha^2\beta$, then

$$N_\gamma(r) = N_\beta(c)\,(-1)^{n_2+n_3}(y_1 y_2^{-1} y_3)^{n_1+n_3},$$

so the condition $N_\gamma(r) = 1$ implies $n_1 + n_3 = 0$, $n_2 + n_3$ even and $N_\beta(c) = 1$. Again, we may choose $u = c$.

Lemma 9 now shows that if $z \in L^\sharp$ satisfies (12), then there exists $v \in D^\times$ such that $N_\alpha(zv) = N_\beta(zv) = 1$, i.e.

$$N_\alpha(v) = -1 \qquad \text{and} \qquad N_\beta(v) = 1.$$

Letting $v = cy_1^{n_1}y_2^{n_2}y_3^{n_3}$ with $c \in \mathbb{Q}(\zeta_4)^\times$ and $n_1, n_2, n_3 \in \mathbb{Z}$, we have

$$N_\alpha(v) = c^4(-1)^{n_1+n_3} \qquad \text{and} \qquad N_\beta(v) = N_\beta(c)y_1^{2n_1}y_2^{2n_2}y_3^{2n_3}.$$

Therefore, we must have $n_1 = n_2 = n_3 = 0$ and $c^4 = -1$. This is impossible, since $\mathbb{Q}(\zeta_4)$ does not contain a primitive 8-th root of unity. ∎

Combining Proposition 8 and Theorem 10, we obtain examples which show that the cyclicity criterion of [3] for biquaternion algebras does not generalize to algebras of higher degree. Corollary 5.11 of [3] states: *Let A be a central simple F-algebra of degree 4 and exponent 2 and let L be a quadratic extension of F contained in A. Suppose L can be embedded in some cyclic extension K/F of degree 4. The algebra A is split by such a cyclic extension if and only if it is isomorphic to the corestriction $\mathrm{cor}_{L/F}(Q)$ of some quaternion algebra Q over L.*

The "only if" direction is easy to generalize: if A is a cyclic algebra of exponent p (prime) and degree p^n:

$$A = (K/F, \sigma, a)$$

and if L denotes the intermediate extension of codimension p in K/F, then by [5, Theorem 30.10],

$$A^p = (L/F, \sigma, a) \quad \text{in } \mathrm{Br}(F),$$

hence the condition that A has exponent p implies $a = N_{L/F}(\ell)$ for some $\ell \in L^\times$. Then

$$A = \mathrm{cor}_{L/F}(K/L, \sigma^{p^{n-1}}, \ell) \quad \text{in } \mathrm{Br}(F).$$

However, Brauer algebras yield examples which show that the "if" direction does not generalize to algebras of degree p^2 and exponent p if p is odd, nor to algebras of degree 8 and exponent 2, as we now show.

Suppose first p is odd. With the notation of the preceding section, Theorem 10 shows that the algebra $R_{q,p^2,pq} = (K_{q,p^2,pq}, \sigma, \zeta_q)$ does not satisfy property $D(p)$, hence Proposition 8 shows that the symbol algebra

$$A_{\zeta_p}(t, \zeta_q)_{K_{q,1,pq}((t))}$$

is not split by any extension of degree p of $K_{q,p,pq}((t))$ which is cyclic over $K_{q,1,pq}((t))$. Nevertheless, since $R_{q,p^2,pq}$ has exponent p, by [7, Theorem 7.3.8], ζ_q is a norm from $K^\times_{q,p,pq}$, hence $A_{\zeta_p}(t,\zeta_q)_{K_{q,1,pq}((t))}$ is Brauer-equivalent to the corestriction of a symbol over $K_{q,p,pq}((t))$.

For $p = 2$, Theorem 10 shows that $R_{2,8,8} = (K_{2,8,8}/K_{2,1,8}, \sigma, -1)$ does not satisfy property $D(2)$, hence Proposition 8 shows that the quaternion algebra

$$(t,-1)_{K_{2,1,8}((t))}$$

is not split by any quadratic extension of $K_{2,4,8}((t))$ which is cyclic over $K_{2,1,8}((t))$. This quaternion algebra is Brauer-equivalent to the corestriction of some quaternion algebra over $K_{2,4,8}((t))$ however, since the fact that $R_{2,8,8}$ has exponent 2 implies that -1 is a norm from $K_{2,4,8}$.

7. Indecomposable algebras

In this last section, we show how property $D(p)$ relates to more general decomposition properties, and use Brauer algebras to produce indecomposable division algebras of prime exponent.

We first review the general construction, which is explained in still greater generality in [7, §7.3]. Let p be a prime and

$$R = (K/F, \sigma, a)$$

be a cyclic algebra of degree p^2. Suppose F contains a primitive p-th root of unity ζ_p. Let L be the intermediate subfield of codimension p in K, so

$$K = L(\delta)$$

for some $\delta \in K$ such that $\sigma^p(\delta) = \zeta_p\delta$. As in Lemma 7, we have $\sigma(\delta) = \mu\delta$ for some $\mu \in L^\times$. Write

$$R = \bigoplus_{i=0}^{p^2-1} K \cdot z^i$$

where $z^{p^2} = a$ and $zkz^{-1} = \sigma(k)$ for $k \in K$. Let R_0 denote the (commutative) subring of R generated by L and z^p:

$$R_0 = \bigoplus_{i=0}^{p-1} L \cdot (z^p)^i = L[z^p] = L(\sqrt[p]{a}).$$

We assume throughout R_0 is a field, which simply means $a \notin L^{\times p}$.

Let λ_1, λ_2 be independent commuting indeterminates over F. In $R(\lambda_1, \lambda_2) = R \otimes_F F(\lambda_1, \lambda_2)$ we consider the elements

$$\delta^\diamond = \delta\lambda_1, \qquad z^\diamond = z\lambda_2, \qquad a^\diamond = a\lambda_2^{p^n} = z^{\diamond p^n}$$

and we let

$$F^\diamond = F(\lambda_1^p, \lambda_2^p), \qquad L^\diamond = L(\lambda_1^p, \lambda_2^p), \qquad K^\diamond = L^\diamond(\delta^\diamond).$$

We extend σ to $K(\lambda_1, \lambda_2)$ by letting λ_1, λ_2 invariant and consider the cyclic algebra

$$R^\diamond = (K^\diamond/F^\diamond, \sigma, a^\diamond) = \bigoplus_{i=0}^{p^2-1} K^\diamond \cdot z^{\diamond i},$$

which is denoted by R' in [7, p. 252]. Proposition 7.3.21 of [7] shows that $R^\diamond$ is a division algebra of degree p^n and exponent dividing the exponent of R (provided R is not split).

PROPOSITION 11: *If $R^\diamond$ decomposes into a tensor product of two subalgebras of degree p, then R has property $D(p)$.*

Proof: Proposition 7.3.26 of [7] shows that if $R^\diamond$ decomposes, then

$$z^p = f\, N_{R_0/F(z^p)}(r)$$

for some $f \in F^\times$ and some $r \in R_0^\times$. Letting τ denote the automorphism of R_0/L such that $\tau(z^p) = \zeta_p z^p$, we then have

$$\zeta_p = \tau(z^p)z^{-p} = N_{R_0/F(z^p)}(\tau(r)r^{-1}).$$

Therefore, the element $x = \tau(r)r^{-1} \in R_0^\times$ satisfies

$$N_{R_0/F(z^p)}(x) = \zeta_p \qquad \text{and} \qquad N_{R_0/L}(x) = 1,$$

hence Proposition 8 shows that R satisfies property $D(p)$. (In the notation of that proposition, $R_0 = L^\sharp$ and $F(z^p) = F^\sharp$.) ∎

Remark: The converse of Proposition 11 also holds.

COROLLARY 12: *Let q be a power of p, with $q \geq p$, and let $R_{q,p^2,pq}$ denote the Brauer algebra constructed in the preceding section. If p is odd, the algebra $R^\diamond_{q,p^2,pq}$ is an indecomposable division algebra of degree p^2 and exponent p.*

Proof: Indecomposability of $R^{\diamond}_{q,p^2,pq}$ readily follows from Theorem 10 and Proposition 11. The other properties follow from general results about the $^{\diamond}$ construction. ∎

Remark: Corollary 12 is already announced in [6, Theorem 4] and [7, Theorem 7.3.28]. The proofs given there contained gaps, however. Specifically, the proof of Proposition 5 in [6] is not sufficient, because (in the notation of that paper) the automorphism σ does not necessarily preserve the rings H, H_1. Similarly, the proof of Proposition 7.3.27 in [7] uses the hypothesis that f_1 is relatively prime to $N(h_2)$ to derive that it divides a_2, whereas it is only assumed that f_1 is relatively prime to h_2. We are indebted to Al Sethuraman and Adrian Wadsworth for pointing out these gaps to us. Note however that Proposition 7.3.27 of [7] is correct as stated; a proof can be given on the same lines as Lemma 9 above.

On the other hand, we do not know how to patch the gaps in the proofs of the noncrossed product results ([6, Theorem 4(ii)], [7, Theorem 7.3.30]). Another open question is whether the Brauer algebra $R_{q,p^2,pq}$ itself is indecomposable (as opposed to the generic construction $R^{\diamond}_{q,p^2,pq}$ based on it).

The indecomposable algebras $R^{\diamond}_{q,p^2,pq}$ have the property that the algebraic closure of $\mathbb{Q}$ in their center is $\mathbb{Q}(\zeta_q)$. However, an ultraproduct construction also yields examples where the base field contains all the p^n-th roots of unity for all n: let $I = \mathbb{N} \setminus \{0\}$ and, for $i \in I$, let

$$D_i = R_{p^i,p^2,p^{i+1}}.$$

Let $\mathcal{F}$ be any ultrafilter on I containing the cofinite filter. The ultraproduct

$$D = \prod_{i \in I} D_i / \mathcal{F}$$

is a ring such that any elementary sentence holding in almost all D_i holds in D (see [7]). In particular, D is a division algebra; its degree is p^2 since this condition is determined by the standard polynomial identity S_{2p^2} (and nonidentity S_{2p^2-1}), which is an elementary sentence. Since decomposability is elementary, D is indecomposable. Moreover, for all integers n, the center of D_i contains a primitive p^n-th root of unity if $i \geq n$, hence the center of D contains a primitive p^n-th root of unity for all n.

References

[1] A. A. Albert, *Modern Higher Algebra*, University of Chicago Press, Chicago, 1937.

[2] R. Brauer, *Über den Index und den Exponent von Divisionsalgebren*, Tôhoku Mathematical Journal **37** (1933), 77–87.

[3] T. Y. Lam, D. B. Leep and J.-P. Tignol, *Biquaternion algebras and quartic extensions*, Publications Mathématiques de l'IHES **77** (1993), 63–102.

[4] J. W. Milnor, *Introduction to Algebraic K-theory*, Annals of Mathematics Studies 72, Princeton University Press, Princeton, 1971.

[5] I. Reiner, *Maximal Orders*, Academic Press, London, 1975.

[6] L. H. Rowen, *Cyclic division algebras*, Israel Journal of Mathematics **41** (1982), 213–234; correction **43** (1982), 277–280.

[7] L. H. Rowen, *Ring Theory* (Volumes I and II), Academic Press, San Diego, 1988.

[8] J-P. Serre, *Corps locaux*, Hermann, Paris, 1968.