GALOIS COHOMOLOGY OF FIELDS WITHOUT ROOTS OF UNITY

UZI VISHNE

Abstract. There is a standard correspondence between elements of the cohomology group $\mathrm{H}^1(F,\mu_n)$ (with the trivial action of $\Gamma_F = \mathrm{Gal}(F_s/F)$ on μ_n) and cyclic extensions of dimension n over F. We extend this to a correspondence between the cohomology groups $\mathrm{H}^1(F,\mu_n)$ where the action of Γ_F on μ_n varies, and the extensions of dimension n of K which are Galois over F, where $K = F[\mu_n]$ and $[K:F]$ is prime to n. The cohomology groups are also related to eigenspaces of $\mathrm{H}^1(K,\mathbb{Z}/n)$ with respect to the natural action of $\mathrm{Gal}(K/F)$.

As a result, we extend Albert's cyclicity criterion, stated in the 1930s for division algebras of prime degree, to algebras of prime-power degree over F, under the assumption stated above. We also extend the Rosset-Tate result on the corestriction of cyclic algebras in the presence of roots of unity, to extensions in which roots of unity are present in an extension of dimension ≤ 3 over the base field. In particular if roots of unity are present in a quadratic extension of the base field, then corestriction of a cyclic algebra along a quadratic extension is similar to a product of two cyclic algebras. Another application is that F-central algebras which are split by a certain semidirect product extension of F are cyclic. In particular, if $[K:F] = 2$ then algebras over F which are split by an odd order dihedral extension are cyclic.

We also construct generic examples of algebras which become cyclic after extending scalars by roots of unity, and present elements for which most powers have reduced trace zero.

To Appear: J. Algebra.

1. Introduction

The purpose of this paper is to generalize standard constructions in Galois cohomology to fields without roots of unity. Let n be a prime power, F a field of characteristic prime to n, and $K = F[\rho]$, where ρ is

Date: Nov. 1, 2002.

1991 *Mathematics Subject Classification.* 16K20, 12G05.

I thank J.-P. Tignol and L.H. Rowen for many stimulating discussions. I gratefully acknowledge a post-doctoral grant from the Fulbright program, United States Department of State.

a primitive unity root of order n. Let F_{s} denote the separable closure of F. In [8] and [9] A. Merkurjev uses decomposition into eigenspaces of the cohomology groups of K to study the Brauer group of F in terms of the Brauer group of K, which is better understood. In the first part of this paper, Sections 2–7, we apply his technique to the first cohomology group $\mathrm{H}^1(K,\mathbb{Z}/n)$, which is easier to handle than the Brauer group, and we establish the connection to field extensions over F. The second part, Sections 8–14, is concerned with translating this explicit connection to new results on the Brauer group of F, using the cup product.

We assume throughout the paper that $[K:F]$ is prime to n. In this situation $\mathrm{Gal}(K/F)$-modules decompose into eigenspaces indexed by the characters $\mathrm{Gal}(K/F)\to U_n$, where U_n is the Euler group of prime to n residues modulo n (see Section 2). The first examples we study are the isomorphic modules $K^\times/K^{\times n}$ and $\mathrm{H}^1(K,\mathbb{Z}/n)$ (Sections 3 and 4, respectively). We derive some technical results on representatives of classes in $K^\times/K^{\times n}$, which are used frequently later.

In Section 5 we explicitly describe an isomorphism from an eigenspace of $K^\times/K^{\times n}$ to a group $\mathrm{H}^1(F,\mu_n(\chi))$, for a suitable character χ (this is the first cohomology group of $\Gamma_F=\mathrm{Gal}(F_{\mathrm{s}}/F)$ with coefficients in μ_n, where the action is twisted by χ; in particular, the restricted action of Γ_K is trivial). Also, the eigenspaces of $\mathrm{H}^1(K,\mathbb{Z}/n)$ are shown to be isomorphic to those of $\mathrm{H}^1(F,\mu_n(\chi))$. The isomorphisms are natural in the sense that they commute with the restriction map.

It is well known that the cocycles of order n in $\mathrm{H}^1(F,\mu_n)$, with the trivial action, correspond to cyclic Galois extensions of dimension n over F. In a similar manner in Section 6, we interpret the other groups $\mathrm{H}^1(F,\mu_n(\chi))$ in terms of field extensions of dimension n over K which are Galois over F. This is used to give explicit formulas for the inverses of the isomorphisms presented in earlier sections. In Section 7 we study an example with $[K:F]$ not prime to n and explain how the constructions fail in this case.

Recall that $\mathrm{Br}(F)$, the Brauer group of F, consists of classes of central simple F-algebras (where $A\sim B$ if they have the same underlying division algebra), where the product in the group is the tensor product (of representatives). The n-torsion part is denoted ${}_n\mathrm{Br}(F)$. The celebrated theorem of Merkurjev-Suslin is often quoted as saying that if K contains n roots of unity, then ${}_n\mathrm{Br}(K)\cong \mathrm{K}_2(K)/n$ (where $\mathrm{K}_2(K)$ is the second Milnor K-group of K), thus giving generators and relations to ${}_n\mathrm{Br}(K)$ via Matsumoto's theorem. In fact, the theorem holds in greater generally, giving the isomorphism $\mathrm{H}^2(F,\mu_n^{\otimes 2})\cong \mathrm{K}_2(F)/n$ whenever the

characteristic of F is prime to n (see [17, Sec. 8]). Here, $\mathrm{H}^2(F,\mu_n^{\otimes 2})$ is the cohomology group with Γ_F acting diagonally on $\mu_n\otimes\mu_n$, which is the natural action 'twisted by 2'. Since we always have ${}_n\mathrm{Br}(F)\cong\mathrm{H}^2(F,\mu_n)$ (with the natural action), this is useful (from the point of view of Brauer group theory) mainly when the two actions coincide, i.e. when $\mu_n\subseteq F$.

In the second part of the paper, we combine the results on 1-cocycles which were obtained in the first part via the cup product, to study the second cohomology groups $\mathrm{H}^2(F,\mu_n)$ (again for various actions of Γ_F on μ_n). The first step is completed in Section 8, where we compute the corestriction of cyclic algebras from K to F and show that the various restriction maps take the groups $\mathrm{H}^2(F,\mu_n)$ to distinct eigenspaces of $\mathrm{H}^2(K,\mathbb{Z}/n)\cong{}_n\mathrm{Br}(K)$. These eigenspaces are further studied in Section 9. The action of $\mathrm{Gal}(K/F)$ on K is extended to cyclic K-algebras of degree n in Section 10. The fixed subalgebra is then a central F-algebra of the same degree, which is related to the corestriction of the original algebra.

Using a projection formula for the corestriction of cyclic algebras from K to F, we show that if D is a division algebra of degree n over F, which restricts to a cyclic algebra $(a,\beta)_K$ with $a\in K$ and $\beta\in F$, then D is cyclic over F. One application is a generalization of Albert's cyclicity criterion, that a central simple algebra of prime degree n with n-central elements is cyclic, to prime power degree, assuming $[K:F]$ is prime to n (Section 11).

An algorithm due to Rosset and Tate shows that the corestriction of a cyclic algebra from K_2 to K_1, when K_1 has enough roots of unity, is similar to the product of at most $[K_2:K_1]$ cyclic algebras over K_1. In Section 12 we derive a similar result for separable extensions L/F when we assume $[K:F]\leq 3$. In this case the corestriction of a cyclic algebra over L is similar to the product of at most $[K:F]\cdot([L:F]-1)+1$ cyclic algebras over F. If $[K:F]=2$ and L/F is a quadratic extension, then the corestriction is a product of two (and not three) cyclic algebras.

A third application is to semidirect product algebras, discussed in Section 13. If roots of unity are present in the base field, then it is known [13] that algebras with certain semidirect product splitting fields are cyclic. It is easy to show that ${}_n\mathrm{Br}(F)$ is generated by what we call *quasi-symbols* (these are algebras of degree n over F, which are cyclic of some special form when restricted to K). We show that a cyclicity result for algebras with semi-direct product splitting fields is equivalent to every quasi-symbol of that type being cyclic (it is still not known if every such quasi-symbol is indeed cyclic). We find splitting fields of smaller dimension for certain quasi-symbols, and in particular

we show that algebras with splitting fields containing K whose Galois group is $G = \langle \sigma, \tau | \, \sigma^n = \tau^d = 1, \tau\sigma\tau^{-1} = \sigma^t \rangle$ (where τ is a generator of $\mathrm{Gal}(K/F)$ such that $\tau(\rho) = \rho^t$) are cyclic. In a similar way, we extend the theorem of Rowen and Saltman [14] that dihedral algebras are cyclic, assuming the base field contains n-roots of unity. We show that the same result still holds if roots of unity are present in a quadratic extension of the base field. Moreover, F-algebras with dihedral splitting fields which intersect K non-trivially are quasi-symbols.

Finally in Section 14 we present a candidate for a non-cyclic algebra of prime degree over fields without roots of unity. We also show that some generic algebras of this type have elements w for which the reduced trace $\mathrm{Tr}(w^\ell)$ is zero for most values of $\ell < n$.

The approach of this paper is similar to that of [6], where the authors study cohomology groups twisted by quadratic extensions of F. They handle arbitrary quadratic extensions, while here the focus is on the extension of F by the n-roots of unity; however, the main technique here, decomposition into eigenspaces of characters (from the Galois group to U_n), should work for arbitrary Abelian Galois extensions with dimension prime to n. The generality in [6] forces the characteristic of F to be different than 2, while the results here are valid in any characteristic (in particular, see Theorem 13.6 below). More recently, decomposition into eigenspaces with respect to the action of $\mathrm{Gal}(K/F)$ is used in [19] to study cohomology groups. The main focus of this paper is in the Galois groups of maximal p-extensions, and the authors also develop methods to avoid the assumption that $[K:F]$ is prime to n. Our Theorem 11.4 is Theorem 3.6 in [19].

We use the notation suggested by J.-P. Tignol and S.A. Amitsur [18], that a central simple algebra A is *split by* a group G if A is similar (in the Brauer sense) to a crossed product with respect to a subgroup of G. In particular A is split by the cyclic group C_n iff it is similar to a cyclic algebra of degree dividing n.

Frequent use is made of the fact that if the index $[G:H]$ is prime to n and M is a G-module of exponent n, then the restriction of cohomology groups (in particular Brauer groups) from G to H is injective, and the corestriction (from H to G) is onto.

2. Decomposition into Eigenspaces

Let G be a finite Abelian group, and M a faithful G-module of finite torsion n (i.e. $n \cdot M = 0$). In this preparatory section introduce some general notation related to decomposition of G-modules. The primary

partition is well understood, so we assume that $n = p^m$ is a prime power.

Let $U_n = (\mathbb{Z}/n)^\times$ denote the Euler group, consisting of invertible residues modulo n. For a multiplicative character $\phi\colon G \to U_n$, we define a homomorphism $\mathrm{tr}_\phi\colon M \to M$ of G-modules, by

$$\mathrm{tr}_\phi(a) = \sum_{\tau \in G} \phi(\tau)^{-1}\tau(a). \tag{1}$$

Let

$$M^{(\phi)} = \{a \in M : \tau(a) = \phi(\tau) \cdot a\}$$

be the eigenspace of ϕ, and observe that $\mathrm{Im}(\mathrm{tr}_\phi) \subseteq M^{(\phi)}$. Note that for $a \in M^{(\phi)}$ we have $\mathrm{tr}_\phi(a) = |G| \cdot a$, so in particular if $|G|$ is prime to n, $\mathrm{tr}_\phi\colon M \to M^{(\phi)}$ is onto.

The following easy observation will be frequently used.

Remark 2.1. *If $1 \neq g \in U_n$ has order prime to p, then $g \not\equiv 1 \pmod p$.*

Proof. The kernel of the mod p projection $U_n \to U_p$ is of order n/p which is a p-power, and by assumption g is not in this kernel. □

Corollary 2.2. *If $H \leq U_n$ is a non-trivial subgroup and $d = |H|$ is prime to p, then $s = \sum_{h \in H} h \equiv 0 \pmod n$.*

Proof. Choose some $1 \neq g \in H$, then $gs = \sum gh = s$, so $(g-1)s \equiv 0 \pmod n$, but $g - 1$ is prime to p by the last remark. □

Suppose that $\exp(G) \mid \exp(U_n) = \phi(n)$, so that G has $|G|$ distinct characters.

Proposition 2.3. *If $d = |G|$ is prime to n, then*

$$M = \bigoplus_\phi M^{(\phi)}.$$

Proof. Applying the above corollary to the subgroups $\{\phi(\tau)\}_\phi$ (for every $\tau \in G$), we have for arbitrary $a \in M$ that

$$\begin{aligned} d^{-1}\sum_\phi \mathrm{tr}_\phi(a) &= d^{-1}\sum_\phi\sum_\tau \phi(\tau)\tau(a) \\ &= d^{-1}\sum_\tau(\sum_\phi \phi(\tau))\tau(a) \\ &= \sum_\tau(\delta_{\tau,1})\tau(a) = a, \end{aligned}$$

where $\mathrm{tr}_\phi(a) \in M^{(\phi)}$ as we noted above. □

3. The module $K^\times/K^{\times n}$

For the rest of this paper, let F be a field of characteristic prime to n, where $n = p^m$ is a prime power, and let $K = F[\rho]$ where $\rho = \rho_n$ is a primitive root of unity of order n. Our first step is to apply the decomposition of the previous section to $K^\times/K^{\times n}$.

The dimension $d = [K:F]$ obviously divides $|U_n| = (p-1)p^{m-1}$. As in Section 2, we assume throughout the paper that d is prime to n. In particular, p is odd, and $G = \mathrm{Gal}(K/F)$ is cyclic. For every $n = p^m$, by setting $K = F[\rho_n]$, the dimension $[K:F[\rho_p]]$ is a power of p, so the following holds:

Remark 3.1. *$[K:F]$ is prime to n iff $K = F[\rho_n] = F[\rho_p]$.*

Note that for a given field F, there is a maximal $\alpha \leq \infty$ such that the dimension of $K = F[\rho_{p^\alpha}]$ over F is prime to p.

The decomposition given in the last section applies to $M = K^\times/K^{\times n}$, which is an n-torsion module over $G = \mathrm{Gal}(K/F)$. For a character $\varphi\colon G \to U_n$, the eigenspace $(K^\times/K^{\times n})^{(\varphi)}$ defined in Section 2, lifted to $K^\times$, is

$$K^{(\varphi)} = \{a \in K^\times : \forall \tau, \quad \tau(a) \equiv a^{\varphi(\tau)} \pmod{K^{\times n}}\}.$$

The twisted norm

$$\mathrm{N}^{(\varphi)}\colon K^\times \to K^{(\varphi)}/K^{\times n}$$

is defined by

$$\mathrm{N}^{(\varphi)}a = \prod_{\tau\in G} \tau(a)^{\varphi(\tau^{-1})}. \tag{2}$$

For every $a \in K^\times$, Proposition 2.3 gives a decomposition

$$a = \Pi a_\varphi \tag{3}$$

where φ runs over the characters of $\mathrm{Gal}(K/F)$, and each $a_\varphi \in K^{(\varphi)}$ is unique modulo $K^{\times n}$.

It is obvious that $F^\times \subseteq K^{(1)}$. On the other hand,

Proposition 3.2. *$K^{(1)} = F^\times K^{\times n}$.*

Proof. The inclusion $F^\times K^{\times n} \subseteq K^{(1)}$ is obvious. Fix a generator τ of $\mathrm{Gal}(K/F)$ and let $a \in K^{(1)}$, then by assumption there is some $\mu \in K$ such that $\tau(a) = \mu^n a$. Taking norms, we see that $\mathrm{N}_{K/F}(\mu)^n = 1$. However, since the norm is in F which does not contain roots of unity even of order p (Remark 3.1), we must have $\mathrm{N}_{K/F}(\mu) = 1$. Thus, there is some $g \in K$ such that $\mu = \tau(g)g^{-1}$. Let $\alpha = g^{-n}a$. Then $\tau(\alpha) = \tau(g)^{-n}\tau(a) = \mu^{-n}g^{-n}\mu^n a = \alpha$, so that $\alpha \in F$ and $a \in F^\times K^{\times n}$, as asserted. □

The following observation is of a similar nature:

Remark 3.3. $F^\times \cap K^{\times n} = F^{\times n}$.

Proof. Let $a \in K^\times$ be an element such that $a^n \in F$. Let τ be a generator of $\mathrm{Gal}(K/F)$. Since $\tau(a^n) = a^n$, $\tau(a) = \rho^i a$ for some i. Write $\tau(\rho) = \rho^t$. Since $\langle t \rangle$ is a subgroup of order d of U_n, $t-1$ is prime to p (Remark 2.1). Let $b = \rho^{i/(1-t)}a$ (where the inverse is taken mod n), and compute that $\tau(b) = \rho^{it/(1-t)+i}a = \rho^{i(t/(1-t)+1)}a = b$. This shows that $b \in F$, and therefore $a^n = b^n \in F^{\times n}$. □

Since K has n roots of unity, the cyclic extensions of dimension n over K are classified by elements of $K^\times/K^{\times n}$, by the Kummer correspondence. In a similar manner, the subspaces $K^{(\psi)}$ classify cyclic extensions of dimension n over K, which are Galois over F. In the following proposition the condition that $[K:F]$ is prime to n is not needed.

Proposition 3.4 ([1, p. 211])**.** *Let $a \in K$, $\alpha = \sqrt[n]{a}$, and assume $K_1 = K[\alpha]$ is a field. Then K_1 is Galois over F iff $a \in K^{(\varphi)}$ for some character φ.*

Proof. Let ϖ denote the generator of $\mathrm{Gal}(K_1/K)$, defined by $\varpi(\alpha) = \rho\alpha$. Assume K_1/F is Galois; then every $\tau \in \mathrm{Gal}(K/F)$ extends to K_1. Fix τ. Since $\tau(\alpha)^n = \tau(\alpha^n) = \tau(a) \in K$, we have that $\varpi(\tau(\alpha))^n = \tau(\alpha)^n$, and $\varpi(\tau(\alpha)) = \rho^{\varphi(\tau)}\tau(\alpha)$ for some $\varphi(\tau) \in \mathbb{Z}/n$. Now $\varpi(\frac{\tau(\alpha)}{\alpha^{\varphi(\tau)}}) = \frac{\varpi\tau(\alpha)}{\varpi(\alpha)^{\varphi(\tau)}} = \frac{\rho^{\varphi(\tau)}\tau(\alpha)}{(\rho\alpha)^{\varphi(\tau)}} = \frac{\tau(\alpha)}{\alpha^{\varphi(\tau)}}$, so that $\tau(\alpha)\alpha^{-\varphi(\tau)} \in K^\times$ and $\tau(a) \in K^{\times n}a^{\varphi(\tau)}$. It then follows immediately that φ is multiplicative mod n, so that φ is a character and $a \in K^{(\varphi)}$.

Now assume that $a \in K^{(\varphi)}$. Then for every $\tau \in \mathrm{Gal}(K/F)$, we have $\tau(a) = k^n a^{\varphi(\tau)}$ for some $k \in K^\times$. For every $i \in \mathbb{Z}/n$, $\alpha \mapsto \rho^i k \alpha^{\varphi(\tau)}$ is a well defined extension of τ to K_1 (since it preserves the defining relation $\alpha^n = a$), so there are $n \cdot |\mathrm{Gal}(K/F)| = [K_1:F]$ distinct automorphisms. This shows that K_1/F is Galois. □

We remark that the assumption that K_1 is a field can be omitted. If the order n' of a in $K^\times/K^{\times n}$ is a proper divisor of n, then $K_1 = K[\lambda]/\langle \lambda^n - a \rangle$ is a direct product of n/n' copies of the field $K[\sqrt[n']{a}]$. Letting $\varphi' \colon \mathrm{Gal}(K/F) \to U_{n'}$ denote the composition of φ with the projection $U_n \to U_{n'}$, we see that K_1 is a Galois ring over F iff $a \in K^{(\varphi')}$ for some character φ.

The following remark allows us to choose $a \in K^{(\varphi)}$ with the convenient property that $\mathrm{N}_{K/F}(a) = 1$. The case $[K:F] = 2$ is covered in [6, Prop. 25].

Remark 3.5. *Let $\varphi \neq 1$. Every class in $K^{(\varphi)}/K^{\times n}$ has a representative a such that $\mathrm{N}_{K/F}(a) = 1$.*

Proof. Let $\mathrm{N} = \mathrm{N}_{K/F}$ denote the usual norm. Let τ be a generator of $\mathrm{Gal}(K/F)$, and $r \equiv \varphi(\tau) \pmod n$. By Remark 2.1 there are $i, j \in \mathbb{Z}$ such that $i(r-1) + jn = 1$. Let $a \in K^{(\varphi)}$, then by assumption, $\tau(a) = \mu^n a^r$ for some $\mu \in K^\times$. The equivalent element $a_1 = (\mu^i a^{-j})^n a$ satisfies $\mathrm{N}(a_1) = \mathrm{N}(\mu)^{ni}\mathrm{N}(a)^{1-jn} = (\mathrm{N}(\mu)^n \mathrm{N}(a)^{r-1})^i = (\mathrm{N}(\tau(a))/\mathrm{N}(a))^i = 1$. □

If $d = [K:F]$ is even and K_0/F is the quadratic intermediate field, let ϵ denote the character of order 2 of $\mathrm{Gal}(K/F)$. A similar argument proves the following:

Remark 3.6. *Let $\varphi \neq 1, \epsilon$. Every class in $K^{(\varphi)}/K^{\times n}$ has a representative a such that $\mathrm{N}_{K/K_0}(a) = 1$.*

Proof. As in the previous remark let τ be a generator of $\mathrm{Gal}(K/F)$, $r \equiv \varphi(\tau) \pmod n$, and denote $\mathrm{N}'(a) = \mathrm{N}_{K/K_0}(a) \cdot \tau\mathrm{N}_{K/K_0}(a)^{-1}$. Since $r \not\equiv -1$ by assumption, there are $i', j' \in \mathbb{Z}$ such that $i'(r+1) + j'n = 1$. Given an element $a \in K^{(\varphi)}$, write $\tau(a) = \mu^n a^r$, so that $\tau(\mathrm{N}'(a)) = \mathrm{N}'(\mu)^n \mathrm{N}'(a)^r$. Now the element $a_1 = (\mu^{i'} a^{-j'})^n a$ satisfies $\mathrm{N}'(a_1) = \mathrm{N}'(\mu)^{ni'}\mathrm{N}'(a)^{1-j'n} = (\mathrm{N}'(\mu)^n \mathrm{N}'(a)^{r+1})^{i'} = (\tau\mathrm{N}'(a)\mathrm{N}'(a))^{i'} = 1$, so that $\mathrm{N}_{K/K_0}(a_1) \in F$.

Since $\varphi \neq 1$ we can by the previous remark assume $\mathrm{N}(a) = 1$ to begin with, then $\mathrm{N}(\mu)^n = \mathrm{N}(a)^{1-r} = 1$, so that $\mathrm{N}(\mu) = 1$, and $\mathrm{N}_{K/K_0}(a_1)^2 = \mathrm{N}_{K_0/F}\mathrm{N}_{K/K_0}(a_1) = \mathrm{N}(a_1) = 1$. Finally if $\mathrm{N}_{K/K_0}(a_1) = -1$, we can replace a_1 by a_1^{n+1}, which will have norm 1. □

4. Decomposition of $\mathrm{H}^1(K, \mu_n)$

In this section we show that the eigenspaces of $\mathrm{H}^1(K, \mathbb{Z}/n)$ with respect to the $\mathrm{Gal}(K/F)$ action are $\mathrm{H}^1(K, \mathbb{Z}/n)^{(\varphi)} = K^{(\varphi)}/K^{\times n}$. Let F_{s} denote the separable closure of F, and let

$$\Gamma_F = \mathrm{Gal}(F_{\mathrm{s}}/F)$$

denote the absolute Galois group of F. As usual, we denote the cohomology groups of Γ_F by $\mathrm{H}^i(F, M) = \mathrm{H}^i(\Gamma_F, M)$.

The long exact sequence of cohomology groups applied to the Kummer sequence

$$1 \longrightarrow \mu_n \longrightarrow {F_{\mathrm{s}}}^\times \longrightarrow {F_{\mathrm{s}}}^\times \longrightarrow 1, \tag{4}$$

gives an isomorphism

$$j_F \colon F^\times/F^{\times n} \longrightarrow \mathrm{H}^1(F, \mu_n) \tag{5}$$

sending $aF^{\times n}$ to (a), which is defined by $(a)\colon \sigma \mapsto \sigma(\alpha)\alpha^{-1}$ where $\alpha = \sqrt[n]{a}$ is a fixed root.

As before, let $K = F[\rho]$ where ρ is a primitive n-root of unity. The action of Γ_K on μ_n is always taken to be the trivial action; this is often expressed by writing $\mathrm{H}^1(K, \mathbb{Z}/n)$ instead of $\mathrm{H}^1(K, \mu_n)$. Considering (4) as a sequence of Γ_K-modules (rather than Γ_F-modules), gives an isomorphism

$$j_K\colon K^\times/K^{\times n} \longrightarrow \mathrm{H}^1(K, \mathbb{Z}/n)$$

defined similarly to j_F. Of course, j_K carries the decomposition of $K^\times/K^{\times n}$ of the previous section to a similar decomposition of $\mathrm{H}^1(K, \mathbb{Z}/n)$. For the sake of later applications, we describe the latter decomposition in details.

Let $a \in K^\times$ and $\alpha = \sqrt[n]{a}$. Since K has enough roots of unity, $K[\alpha]$ is Galois over K, and the value $(a)_\sigma$ is determined by the restriction of σ to $K[\alpha]$. In other words, (a) is an element of $\mathrm{H}^1(K, \mathbb{Z}/n)$ induced from $\mathrm{H}^1(\mathrm{Gal}(K[\alpha]/K), \mathbb{Z}/n)$.

The Galois group $G = \mathrm{Gal}(K/F)$ acts on $\mathrm{H}^1(K, \mathbb{Z}/n)$ by

$$\tau(a)\colon \sigma \mapsto \tau((a)_{\tau^{-1}\sigma\tau}).$$

Since the Kummer sequence (4) is a sequence of G-modules, j_K is an isomorphism of G-modules. Indeed, let $a \in K^\times$ with $\alpha = \sqrt[n]{a}$, $\tau \in \mathrm{Gal}(K/F)$ and $\sigma \in \Gamma_K$, then by definition

$$\begin{aligned} \tau(a)\colon \sigma &\mapsto \tau((a)_{\tau^{-1}\sigma\tau}) \\ &= \tau(\tau^{-1}\sigma\tau(\alpha)\alpha^{-1}) \\ &= \sigma\tau(\alpha)\tau(\alpha)^{-1} \\ &= (\tau a)_\sigma. \end{aligned}$$

In particular, j_K is compatible with the decomposition of $K^\times/K^{\times n}$ and $\mathrm{H}^1(K, \mathbb{Z}/n)$ into eigenspaces which is given in Proposition 2.3, and restricts to an isomorphism

$$j_K\colon K^{(\varphi)}/K^{\times n} \longrightarrow \mathrm{H}^1(K, \mathbb{Z}/n)^{(\varphi)}$$

for every character $\varphi\colon \mathrm{Gal}(K/F) \to U_n$. Since $\mathrm{N}^{(\varphi)}$ of Equation (2) is the twisted trace function defined on $K^\times/K^{\times n}$, the following diagram commutes:

$$\begin{array}{ccccc} K^{(\varphi)}/K^{\times n} & \hookrightarrow & K^\times/K^{\times n} & \xrightarrow{\mathrm{N}^{(\varphi)}} & K^{(\varphi)}/K^{\times n} \\ \downarrow{\scriptstyle j_K} & & \downarrow{\scriptstyle j_K} & & \downarrow{\scriptstyle j_K} \\ \mathrm{H}^1(K, \mathbb{Z}/n)^{(\varphi)} & \hookrightarrow & \mathrm{H}^1(K, \mathbb{Z}/n) & \xrightarrow{\mathrm{tr}_\varphi} & \mathrm{H}^1(K, \mathbb{Z}/n)^{(\varphi)} \end{array} \tag{6}$$

5. First Cohomologies of F

Let F be a field of characteristic prime to n, where $n = p^m$. Let μ_n denote the group of roots of unity of order n in F_{s}. Fix a primitive root $\rho \in \mu_n$.

In this section we study the Galois groups $\mathrm{H}^1(F, \mu_n)$ for various actions of Γ_F on μ_n, which restrict to the trivial action of Γ_K. We shall see that these groups correspond to the eigenspaces of $\mathrm{H}^1(K, \mathbb{Z}/n)$, computed in the previous section. One case is well understood: taking the natural action of Γ_F on $\mu_n \subseteq {F_{\mathrm{s}}}^{\times}$, as a group of automorphisms, we have $\mathrm{H}^1(F, \mu_n) \cong F^{\times}/F^{\times n}$ by the Kummer sequence mentioned earlier.

Let $K = F[\rho]$. A character $\chi\colon \mathrm{Gal}(K/F) \to U_n$ determines an action of Γ_F on μ_n by $\sigma_*(\rho) = \rho^{\chi(\sigma)}$ (the star reminds us that this is not the usual action); and of course every extension of the trivial action of Γ_K to Γ_F has this form. We use $\mathrm{H}^1(F, \mu_n(\chi))$ to denote the cohomology group with respect to the action determined by χ. Since the action of Γ_K is trivial, we use $\mathrm{H}^1(K, \mathbb{Z}/n)$ for the cohomology group with respect to Γ_K, and we have the restriction map $\mathrm{res}\colon \mathrm{H}^1(F, \mu_n(\chi)) \to \mathrm{H}^1(K, \mathbb{Z}/n)$.

Denote $G = \mathrm{Gal}(K/F)$, and view μ_n as a Γ_F-module with the action via χ. As a subgroup, $\Gamma_K \leq \Gamma_F$ acts trivially on μ_n, and the short exact sequence

$$1 \longrightarrow \Gamma_K \longrightarrow \Gamma_F \longrightarrow G \longrightarrow 1$$

gives rise to the Serre-Hochshild spectral sequence

$$\mathrm{H}^1(G, \mu_n) \longrightarrow \mathrm{H}^1(F, \mu_n(\chi)) \longrightarrow \mathrm{H}^1(K, \mu_n)^G \longrightarrow \mathrm{H}^2(G, \mu_n).$$

Since $|\Gamma_F/\Gamma_K| = [K\colon F]$ is prime to n by assumption, we have that

$$\mathrm{H}^1(G, \mu_n) = \mathrm{H}^2(G, \mu_n) = 0,$$

so we obtain an isomorphism

$$\mathrm{H}^1(F, \mu_n(\chi)) \cong \mathrm{H}^1(K, \mu_n)^G,$$

which we will explicitly describe below. In particular we will see that for the action of G on $\mathrm{H}^1(K, \mu_n)$ via χ, the invariant subgroup $\mathrm{H}^1(K, \mu_n)^G$ is the component $\mathrm{H}^1(K, \mathbb{Z}/n)^{(\nu\chi^{-1})}$ of the previous section (where ν is defined in Equation (8) below).

From Proposition 3.2 and Remark 3.3 we see that

$$K^{(1)}/K^{\times n} = K^{\times n}F^{\times}/K^{\times n} \cong F^{\times}/F^{\times n},$$

so that $K^{(1)}/K^{\times n} \cong \mathrm{H}^1(F, \mu_n(\nu))$. This motivates an attempt to express other cohomology groups in terms of the components $K^{(\varphi)}/K^{\times n}$.

Identify U_n with $\mathrm{Aut}(\mu_n)$ is the usual way (where the action is by exponentiation). Fix a character

$$\varphi\colon \mathrm{Gal}(K/F)\to U_n,$$

and let $a \in K^{(\varphi)}$ be an element such that $K_1 = K[\alpha]$ is a field, where $\alpha = \sqrt[n]{a}$ is a fixed root (the assumption that K_1 is a field will eventually be removed). By Proposition 3.4, K_1/F is a Galois extension, and so every $\sigma \in \Gamma_F$ restricts to an automorphism of K_1/F. The idea is to use this restriction to define the value of the cocycle at σ, making the cocycle induced from $\mathrm{H}^1(\mathrm{Gal}(K_1/F), \mu_n)$ (with an action which is yet to be determined), just as $(c) \in \mathrm{H}^1(K, \mathbb{Z}/n)$ is induced from $\mathrm{H}^1(\mathrm{Gal}(K[\sqrt[n]{c}]/F), \mathbb{Z}/n)$ for $c \in K^\times$. The analogy to the special case $\varphi = 1$ still holds: if $a \in K^{(1)}$ then by Proposition 3.2 we can assume that $a \in F^\times$, and then the value of $(a) \in \mathrm{H}^1(F, \mu_n)$ (with the natural action) at $\sigma \in \Gamma_F$ is determined by the restriction of σ to $K_1 = K \otimes F[\alpha]$, where $\alpha = \sqrt[n]{a}$ is a fixed root.

Let ϖ denote a generator of $\mathrm{Gal}(K_1/K)$ defined by

$$\varpi(\alpha) = \rho\alpha. \tag{7}$$

Let $\nu\colon \mathrm{Gal}(K/F)\to U_n$ be the distinguished character defined by

$$\tau(\rho) = \rho^{\nu(\tau)}. \tag{8}$$

Note that ν is uniquely determined by F, and that ν extends to a character $\nu\colon \Gamma_F \to U_n$ in the obvious way. The natural action of Γ_F on μ_n is the action via ν.

Consider the short exact sequence

$$1 \longrightarrow \mathrm{Gal}(K_1/K) \longrightarrow \mathrm{Gal}(K_1/F) \longrightarrow \mathrm{Gal}(K/F) \longrightarrow 1. \tag{9}$$

Since $\mathrm{Gal}(K/F)$ is Abelian, the action of

$$H = \mathrm{Gal}(K_1/F)$$

on $\mathrm{Gal}(K_1/K)$ by conjugation reduces to an action of $\mathrm{Gal}(K/F)$. Let

$$\chi\colon \mathrm{Gal}(K/F)\to U_n$$

be the character associated to this action, namely

$$\tau\varpi\tau^{-1} = \varpi^{\chi(\tau)}. \tag{10}$$

The three characters φ, ν, χ are related by the following equation:

Remark 5.1. $\chi\varphi = \nu$.

Proof. Writing $\tau^{-1}(\alpha) = k\alpha^{\varphi(\tau^{-1})}$ for some $k \in K^\times$, we obtain

$$\begin{aligned}
\rho^{\chi(\tau)}\alpha &= \varpi^{\chi(\tau)}(\alpha) \\
&= \tau\varpi(\tau^{-1}(\alpha)) \\
&= \tau\varpi(k\alpha^{\varphi(\tau^{-1})}) \\
&= \tau(k\rho^{\varphi(\tau^{-1})}\alpha^{\varphi(\tau^{-1})}) \\
&= \tau(\rho)^{\varphi(\tau^{-1})}\tau(k\alpha^{\varphi(\tau^{-1})}) \\
&= \rho^{\nu(\tau)\varphi(\tau^{-1})}\alpha.
\end{aligned}$$

□

Let $N = \mathrm{Gal}(K_1/K) = \langle\varpi\rangle$. Repeating the spectral sequence argument, we obtain an isomorphism

$$\mathrm{H}^1(F, \mu_n(\chi)) \cong \mathrm{H}^1(K, \mu_n)^{H/N},$$

which we will use to construct the co-cycle in $\mathrm{H}^1(F, \mu_n(\chi))$ associated to the element a. The group

$$\mathrm{H}^1(N, \mu_n) = \mathrm{Hom}(N, \mu_n)$$

is cyclic of order n, generated by an element c which is defined by $c(\varpi^s) = \rho^s$. Moreover, the action of

$$H/N = \mathrm{Gal}(K/F)$$

on this group is trivial: for every $\tau \in \mathrm{Gal}(K/F)$, we have $(\tau c)(\varpi^s) = \tau_*(c(\tau^{-1}\varpi^s\tau)) = \tau_*(c(\varpi^{s\chi(\tau)^{-1}})) = \tau_*(\rho^{s\chi(\tau)^{-1}}) = \rho^s = c(\varpi^s)$, where we used the definition $\tau_*(\rho) = \rho^{\chi(\tau)}$.

We will now define a map

$$J^\varphi\colon K^{(\varphi)}/K^{\times n} \to \mathrm{H}^1(F, \mu_n(\chi))$$

where φ and $\chi = \nu\varphi^{-1}$ are the characters fixed above.

Definition 5.2. *Let F, n, K be as above, $G = \mathrm{Gal}(K/F)$, $\varphi\colon G \to U_n$ a character, and $a \in K^{(\varphi)}$. Let ν be the character defined in (8), and $\chi = \nu\varphi^{-1}$.*

First assume that a is of order n in $K^\times/K^{\times n}$, and let $\alpha = \sqrt[n]{a} \in F_{\mathrm{s}}$, $K_1 = K[\alpha]$ and $H = \mathrm{Gal}(K_1/K)$. Choose a splitting of (9) which maps $\tau \mapsto \tau' \in \mathrm{Gal}(K_1/F)$ (this is possible since $\mathrm{H}^2(G, H(\chi)) = 0$).

Let $\sigma \in \Gamma$ be given, and let $\tau \in \mathrm{Gal}(K/F)$ be the restriction of σ to K. Then for a unique $s \in \mathbb{Z}/n$, the restriction of σ to K_1 is $\sigma = \varpi^s\tau'$. Now, define $c_a \in \mathrm{H}^1(F, \mu_n(\chi))$ by

$$c_a(\sigma) = \rho^s. \tag{11}$$

If the order n' of a in $K^\times/K^{\times n}$ strictly divides n, then repeating the argument for $b = \sqrt[n']{a} \in K$ and n/n' (noting that $b \in K^{(\varphi)}$ when φ is viewed as a character modulo n/n'), we define

$$c_a(\varpi^s\tau') = \rho^{n's}.$$

Finally, $J^\varphi\colon K^{(\varphi)}/K^{\times n}\to \mathrm{H}^1(F,\mu_n(\nu\varphi^{-1}))$ is defined by

$$J^\varphi(a) = c_a.$$

We need to show that the definition does not depend on the splitting of (9). Indeed, since $\mathrm{H}^1(G,H(\chi))=0$, every other splitting $\tau\mapsto\tau''$ is of the form

$$\tau'' = \tau_*(\varpi^i)\varpi^{-i}\tau' = \varpi^{i(\chi(\tau)-1)}\tau'$$

for some i. Let c'_a be the cocycle defined using this splitting. If $\sigma = \varpi^s\tau' = \varpi^{s-i(\chi(\tau)-1)}\tau''$, then $c_a(\sigma)=\rho^s$ and $c'_a(\sigma)=\rho^{s-i(\chi(\tau)-1)}$. The quotient

$$g(\sigma) = \rho^{i(\chi(\tau)-1)} = \tau_*(\rho^i)\rho^{-i} = \sigma_*(\rho^i)\rho^{-i},$$

which is cohomologous to 1.

Theorem 5.3. *The following diagram commutes:*

$$\begin{array}{ccccc} K^{(\varphi)}/K^{\times n} & \hookrightarrow & K^\times/K^{\times n} & \xrightarrow{\mathrm{N}^{(\varphi)}} & K^{(\varphi)}/K^{\times n} \\ \downarrow{\scriptstyle J^\varphi} & & \downarrow{\scriptstyle j_K} & & \downarrow{\scriptstyle J^\varphi} \\ \mathrm{H}^1(F,\mu_n(\chi)) & \xrightarrow{\mathrm{res}} & \mathrm{H}^1(K,\mathbb{Z}/n) & \xrightarrow{\mathrm{cor}} & \mathrm{H}^1(F,\mu_n(\chi)) \end{array} \tag{12}$$

Proof. Let $a\in K^{(\varphi)}$, and let $\alpha, K_1, \varpi, \chi$ be as above. Then $j_K\colon a\mapsto (a)$, where $(a)_\sigma = \sigma(\alpha)\alpha^{-1}$ for every $\sigma\in\Gamma_K$. On the other hand, if $\sigma=\varpi^s$ on K_1, then

$$J^\varphi(a) = c_a \in \mathrm{H}^1(F,\mu_n(\chi))$$

has value ρ^s at σ by definition, and $\sigma(\alpha)\alpha^{-1}=\rho^s=c_a(\sigma)$.

Now consider the right hand square. Since $K^\times$ is generated by the subgroups $K^{(\varphi')}$, it is enough to check that $J^\varphi\circ\mathrm{N}^{(\varphi)} = \mathrm{cor}\circ j_K$ on an element $a\in K^{(\varphi')}$. The corresponding element in $\mathrm{H}^1(K,\mathbb{Z}/n)$ is by definition $\sigma\mapsto\frac{\sigma(\alpha)}{\alpha}$ where α is a fixed nth root of a. Let $K_1=K[\alpha]$, and $\tau\mapsto\tau'$ a splitting of (9) for this K_1. Define ϖ by (7), and set

$$\chi' = \nu{\varphi'}^{-1},$$

so that $G=\mathrm{Gal}(K/F)$ acts on $\langle\varpi\rangle$ via χ'.

We need to show that $J^{\varphi}(\mathrm{N}^{(\varphi)}(a))$ and $\mathrm{cor}(a)$ agree on every $\sigma \in \Gamma_F$. Let $\varpi^s\tau_0'$ be the restriction of σ to K_1. Since $\Gamma_F = \cup_{\tau\in G}\Gamma_K\tau$, we have by definition of the corestriction that

$$\begin{aligned}
\mathrm{cor}(a)\colon \sigma &\mapsto \prod_{\tau} \tau_*^{-1}((a)_{\tau\sigma(\tau\tau_0)^{-1}}) \\
&= \prod_{\tau} \tau_*^{-1}((a)_{\tau\varpi^s\tau^{-1}}) \\
&= \prod_{\tau} \tau_*((a)_{\varpi^{s\chi'(\tau)^{-1}}}) \\
&= \prod_{\tau} \tau_*(\rho^{s\chi'(\tau)^{-1}}) \\
&= \prod_{\tau} \rho^{s\chi(\tau)\chi'(\tau)^{-1}},
\end{aligned}$$

where $\tau_*(\rho) = \rho^{\chi(\tau)}$ since the computation is in $\mathrm{H}^1(F, \mu_n(\chi))$.

If $\chi \neq \chi'$, then

$$\sum_{\tau} \chi(\tau)\chi'(\tau)^{-1} = 0$$

by Remark 2.2, so that $\mathrm{cor}(a) = 1$. This is what we need since $\mathrm{N}^{(\varphi')}(a) \equiv 1$ modulo $K^{\times n}$, again by the same remark.

Now assume $\chi' = \chi$ (i.e. $\varphi' = \varphi$), then $\mathrm{cor}(a)\colon \sigma \mapsto \rho^{sd}$ (where $d = [K:F]$), and likewise $\mathrm{N}^{(\varphi)}(a) \equiv a^d$ so that

$$J^{\varphi}(\mathrm{N}^{(\varphi)}(a)) = J^{\varphi}(a)^d,$$

while

$$J^{\varphi}(a) = c_a\colon \sigma \mapsto \rho^s,$$

and the maps coincide. □

Corollary 5.4. *For* $\varphi\colon \mathrm{Gal}(K/F) \to U_n$ *and* $\chi = \nu\varphi^{-1}$,

$$J^{\varphi}\colon K^{(\varphi)}/K^{\times n} \longrightarrow \mathrm{H}^1(F, \mu_n(\chi))$$

is an isomorphism.

Proof. Since

$$\mathrm{cor} \circ \mathrm{res}\colon \mathrm{H}^1(F, \mu_n(\chi)) \to \mathrm{H}^1(F, \mu_n(\chi))$$

is multiplication by $d = [K:F]$ which is prime to n, res is injective and cor is surjective. Our claim then follows from the commutativity of (12). □

Corollary 5.5. *If $\chi \neq \chi'$, then the composition*

$$\mathrm{H}^1(F, \mu_n(\chi)) \xrightarrow{\mathrm{res}} \mathrm{H}^1(K, \mathbb{Z}/n) \xrightarrow{\mathrm{cor}} \mathrm{H}^1(F, \mu_n(\chi'))$$

is the zero map.

Proof. Use the left hand square of (12) for $\varphi = \nu\chi^{-1}$ and χ, and the right hand square for $\varphi' = \nu\chi^{-1}$ and χ', with the fact (following from Proposition 2.3) that $\mathrm{N}^{(\varphi')}$ is zero on $K^{(\varphi)}/K^{\times n}$. □

Notice that Equation (12) provides an expression for J^φ in terms of the restriction and corestriction, namely $J^\varphi = d^{-1} \cdot \mathrm{cor} \circ j_K$, where the corestriction here is $\mathrm{cor}\colon \mathrm{H}^1(K, \mathbb{Z}/n) \to \mathrm{H}^1(F, \mu_n(\chi))$.

For $\varphi = 1$ we have $\chi = \nu$, so that $\mathrm{H}^1(F, \mu_n(\chi)) = \mathrm{H}^1(F, \mu_n)$ is the group with usual action. In this case the isomorphism J^1 is the composition of $K^{(1)}/K^{\times n} \cong F^\times/F^{\times n}$ with j_F, which was discussed at the beginning of this section. In particular, if $K = F$, then $J^1 = j_K$.

Corollary 5.6. *For every character $\varphi\colon \mathrm{Gal}(K/F) \to U_n$,*

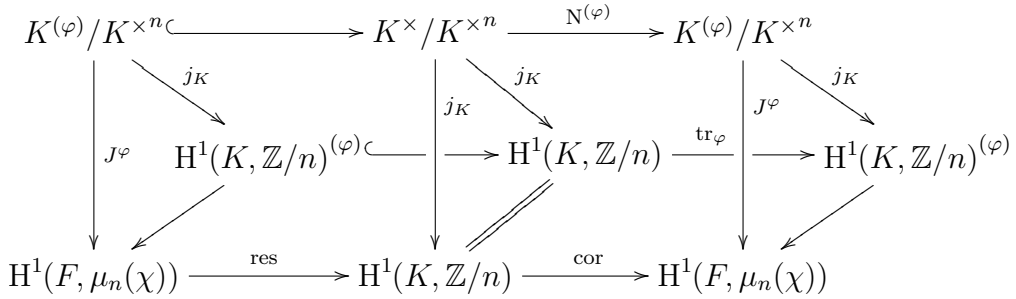
$$\mathrm{H}^1(K, \mathbb{Z}/n)^{(\varphi)} \cong \mathrm{H}^1(F, \mu_n(\chi)),$$

where $\chi = \nu\varphi^{-1}$. Moreover, the following diagram commutes:

$$\begin{array}{ccccc} \mathrm{H}^1(K, \mathbb{Z}/n)^{(\varphi)} & \hookrightarrow & \mathrm{H}^1(K, \mathbb{Z}/n) & \xrightarrow{\mathrm{tr}_\varphi} & \mathrm{H}^1(K, \mathbb{Z}/n)^{(\varphi)} \\ \downarrow & & \| & & \downarrow \\ \mathrm{H}^1(F, \mu_n(\chi)) & \xrightarrow{\mathrm{res}} & \mathrm{H}^1(K, \mathbb{Z}/n) & \xrightarrow{\mathrm{cor}} & \mathrm{H}^1(F, \mu_n(\chi)) \end{array} \tag{13}$$

where the left and right arrows are $J^\varphi \circ j_K^{-1}$.

Proof. Apply the commutativity of (6) and (12) to the following diagram:



□

In general, if M is a G-module and $H \trianglelefteq G$, then the image of the restriction $\mathrm{H}^1(G,M)\to\mathrm{H}^1(H,M)$ is invariant under the action of G/H; one might thus expect that the image of

$$\mathrm{res}\colon \mathrm{H}^1(F,\mu_n(\chi))\to\mathrm{H}^1(K,\mu_n)$$

would be contained in $\mathrm{H}^1(K,\mu_n)^{(1)}$, and not $\mathrm{H}^1(K,\mu_n)^{(\varphi)}$ as the corollary indicates. In fact, every character χ defines a different action of $\mathrm{Gal}(K/F)$ on $\mathrm{H}^1(K,\mu_n)$, compatible with μ_n being a Γ_F-module with the action induced by χ (and indeed $\mathrm{Im}(\mathrm{res})$ is invariant under this action). However, notice that we decompose $\mathrm{H}^1(K,\mu_n)$ to eigenspaces with respect to a fixed action of Γ_F on μ_n, namely the natural one, and $\mathrm{Im}(\mathrm{res})$ is invariant under this action iff $\chi=\nu$.

We end this section by showing that the maps J^φ commute with restriction when F is being changed. For that, we need to express eigenspaces of $K^\times/K^{\times n}$ with respect to the action of $\mathrm{Gal}(K/F)$, in terms of the eigenspaces with respect to the action of a subgroup.

Lemma 5.7. *Let $F\subseteq L\subseteq K$ be an intermediate field, and $\varphi_0:\mathrm{Gal}(K/L)\to U_n$ a character. Let $K^{(\varphi_0)}$ be the φ_0-component of $K^\times$ with respect to the action of $\mathrm{Gal}(K/L)$.*

Then $K^{(\varphi_0)}$ is the product of the components $K^{(\varphi')}$ for all the extensions of φ_0 to characters $\varphi'\colon \mathrm{Gal}(K/F)\to U_n$.

Proof. Let τ be a generator of $\mathrm{Gal}(K/F)$, so that $L=K^{\tau^e}$ and $\mathrm{Gal}(K/L)=\langle\tau^e\rangle$. When viewed as a $\mathrm{Gal}(K/L)$-module, the eigenspace of $K^\times$ with respect to φ_0 is

$$K^{(\varphi_0)}=\{a\in K^\times : \tau^e(a)\equiv a^{\varphi_0(\tau^e)} \pmod{K^{\times n}}\}.$$

Now let $\varphi'\colon \mathrm{Gal}(K/F)\to U_n$ be an arbitrary character, and compare $K^{(\varphi')}$ and $K^{(\varphi_0)}$: if a belongs to the intersection, then $\tau^e(a)\equiv a^{\varphi_0(\tau^e)}\equiv a^{\varphi'(\tau^e)}$, so if φ' restricts to φ_0 we get $K^{(\varphi')}\subseteq K^{(\varphi_0)}$, while otherwise the intersection is $K^{\times n}$. □

Let L be a separable extension of F (viewed as a subfield of F_s), and $L_0=L\cap K$. Let

$$G_0=\mathrm{Gal}(K/L_0)$$

be the corresponding subgroup of $G=\mathrm{Gal}(K/F)$, and φ_0 the restriction of $\varphi\colon G\to U_n$ to G_0. By the lemma, $K^{(\varphi)}\subseteq K^{(\varphi_0)}$. Since $T=L[\rho]=L\otimes_{L_0}K$, there is a natural identification

$$\mathrm{Gal}(T/L)\xrightarrow{\cong}\mathrm{Gal}(K/L_0),$$

which makes φ_0 a character on $\mathrm{Gal}(T/L)$. Likewise let χ_0 be the restriction of $\chi=\nu\varphi^{-1}$ to $\mathrm{Gal}(T/L)$.

Proposition 5.8. *Let L/F be a separable extension, $T = L[\rho]$, and let $\varphi_0, \chi_0 \colon \mathrm{Gal}(T/L) \to U_n$ be defined as above. Then the following diagram commutes.*

$$\begin{array}{ccc} T^{(\varphi_0)}/T^{\times n} & \xrightarrow{J^{\varphi_0}} & \mathrm{H}^1(L, \mu_n(\chi_0)) \\ \uparrow & & \uparrow{\scriptstyle \mathrm{res}} \\ K^{(\varphi)}/K^{\times n} & \xrightarrow{J^{\varphi}} & \mathrm{H}^1(F, \mu_n(\chi)) \end{array} \tag{14}$$

Proof. It is enough to treat the extensions L/L_0 and L_0/F, that is, to show that the following diagram commutes.

$$\begin{array}{ccc} T^{(\varphi_0)}/T^{\times n} & \xrightarrow{J^{\varphi_0}} & \mathrm{H}^1(L, \mu_n(\chi_0)) \\ \uparrow & & \uparrow{\scriptstyle \mathrm{res}} \\ K^{(\varphi_0)}/K^{\times n} & \xrightarrow{J^{\varphi_0}} & \mathrm{H}^1(L_0, \mu_n(\chi_0)) \\ \uparrow & & \uparrow{\scriptstyle \mathrm{res}} \\ K^{(\varphi)}/K^{\times n} & \xrightarrow{J^{\varphi}} & \mathrm{H}^1(F, \mu_n(\chi)) \end{array}$$

For the square at the bottom, let $a \in K^{(\varphi)}$, $K_1 = K[\sqrt[n]{a}\,]$, and assume K_1 is a field (the general case easily follows). We need to prove that the restriction of $J^{\varphi}(a)$ to Γ_{L_0} coincides with $J^{\varphi_1}(a)$. Recall that $c_a = J^{\varphi}(a)$ is not well defined as a function on Γ_F, as it depends on the splitting of (9). Choose a splitting $G \to \mathrm{Gal}(K_1/F)$ which maps $\tau \mapsto \tau'$. Let $\sigma \in \Gamma_{L_0}$, and write the restriction of σ to K_1 as $\varpi^s \tau'$ where $\tau \in \mathrm{Gal}(K/L_0) \subseteq \mathrm{Gal}(K/F)$; then $c_a(\sigma) = s$ either as a cocycle on Γ_F or on Γ_{L_0}.

Next, for the top square, let $a \in K^{(\varphi_0)}$. Again, it is enough to assume that $T_1 = T[\sqrt[n]{a}\,]$ is a field. Let $\tau \mapsto \tau'$ be a splitting of (9) (for K/L_0 instead of K/F), and extend each τ' to $T = L \otimes_{L_0} K$ as $1 \otimes \tau'$. For $\sigma \in \Gamma_L$, write the restriction to T_1 as $\varpi^s \tau'$ where ϖ is defined as usual. Then σ restricts to $\varpi^s \tau'$ on K_1, so $J^{\varphi_0}(\sigma) = \rho^s$ either over the extension T/L, or over K/L_0. □

Note that for the special case $L = K$, (14) is the left hand side of (12).

6. Subfields of K_1

As before, let F be a field of characteristic prime to $n = p^m$, $K = F[\rho]$ where ρ is a primitive root of unity of order n. We assume that $[K : F]$ is prime to n.

Let $\varphi\colon \mathrm{Gal}(K/F)\to U_n$ be a character, $\chi=\nu\varphi^{-1}$ (where ν is defined by (8)) and $a\in K^{(\varphi)}$ an element such that $K_1=K[\alpha]$ is a field for $\alpha=\sqrt[n]{a}$. We inspect some subfields of K_1, and give an explicit computation of the inverse of the map J^φ of Definition 5.2. This will later be used to construct Galois splitting fields of central simple algebras.

Let ϖ be the generator of $\mathrm{Gal}(K_1/K)$ defined by $\varpi(\alpha)=\rho\alpha$. By Proposition 3.4, K_1 is Galois over F, with $\mathrm{Gal}(K_1/F)$ the semidirect product of

$$\mathrm{Gal}(K/F)=\mathbb{Z}/d$$

acting (via χ, by Remark 5.1) on

$$\mathrm{Gal}(K_1/K)=\langle\varpi\rangle\cong\mathbb{Z}/n.$$

Let $\tau\mapsto\tau'$ be a splitting of (9), and G' the copy of $G=\mathrm{Gal}(K/F)$ in $\mathrm{Gal}(K_1/F)$ under this map. Let F_1 denote the invariant subfield of K_1 under G', so that $[F_1\colon F]=n$. Notice that $K_1=F_1\otimes_F K$ as the dimensions are co-prime. The following is essentially in [16, Sec. 2].

Proposition 6.1. *If $\chi=1$ then $F_1=K_1^{G'}$ is cyclic over F. Every cyclic extension of dimension n over F has this form.*

Proof. If $\chi=1$ then

$$\mathrm{Gal}(K_1/F)=\mathbb{Z}/n\times\mathrm{Gal}(K/F)$$

by Equation (10), so that G' is normal in $\mathrm{Gal}(K_1/F)$, with cyclic quotient.

Now let F_1/F be cyclic extension of dimension n. Let $K_1=F_1\otimes_F K$, then K_1 is Galois over F (since $F_1\cap K=F$ as the dimensions are co-prime) and thus of the form $K_1=K[\alpha]$ where $\alpha^n=a$ and $a\in K^{(\varphi)}$ for some character $\varphi\colon G\to U_n$. Let $\chi=\nu\varphi^{-1}$ (where ν is defined by Equation (8)). Let ϖ be the automorphism defined by $\varpi(\alpha)=\rho\alpha$. Let $1\neq\tau\in\mathrm{Gal}(K/F)$, and let τ' be the extension of τ to K_1. By the normality of G' in $\mathrm{Gal}(K_1/F)$, $\varpi\tau'\varpi^{-1}=\varpi^{1-\chi(\tau)}\tau'$ is in G', so that $\chi(\tau)=1$ (otherwise $1-\chi(\tau)$ is prime to n by Remark 2.1). □

Example 6.2. *When $[K\colon F]=2$ we can, by Remark 3.5, choose a representative of $[a]\in K^{(\nu)}/K^{\times n}$ such that $\tau(a)=a^{-1}$. Let $\alpha=\sqrt[n]{a}$, then $K_1=K[\alpha]$ with $\tau(\alpha)=\alpha^{-1}$ and $\varpi(\alpha)=\rho\alpha$. Then*

$$F_1=F[\alpha+\alpha^{-1}].$$

Writing $a=a_0+a_1\rho$ for $a_0,a_1\in F$, the condition $\tau(a)=a^{-1}$ is equivalent to

$$a_0^2+(\rho+\rho^{-1})a_0a_1+a_1^2=1.$$

Of course the general solution to this quadratic equation is obtained by taking $a = b\tau(b)^{-1}$ *for arbitrary* $b = b_0 + b_1\rho \in K$*, namely*

$$a_0 = (b_0^2 - b_1^2)/N \quad \textit{and} \quad a_1 = (2b_0b_1 + (\rho + \rho^{-1})b_1^2)/N$$

where $b_0, b_1 \in F$ *and* $N = b_0^2 + (\rho + \rho^{-1})b_0b_1 + b_1^2 = \mathrm{N}_{K/F}(b_0 + b_1\rho)$*.*

Since $\mathrm{H}^1(G, \mathbb{Z}/n(\chi)) = 0$, the splitting of (9), and hence G', is unique up to conjugation by elements of $\langle\varpi\rangle$.

Remark 6.3. *If* $\chi \neq 1$*, then there are* $d = [K:F]$ *distinct conjugates of* G' *in* $\mathrm{Gal}(K/F)$*.*

Proof. Let τ be a generator of $\mathrm{Gal}(K/F)$. Applying Remark 2.1 to $\chi(\tau)$, we see from the equality $\varpi^i\tau'\varpi^{-i} = \varpi^{i(\chi(\tau')-1)}\tau'$ that $\langle\tau'\rangle$ is its own normalizer in $\mathrm{Gal}(K_1/K)$, and the result follows. □

The various copies G' of G correspond to d isomorphic subfields of K_1, all having dimension n over F. This can be used to invert the map

$$J^\varphi\colon K^{(\varphi)}/K^{\times n} \to \mathrm{H}^1(F, \mu_n(\chi))$$

in the following way. Suppose we are given a cocycle $c \in \mathrm{H}^1(F, \mu_n(\chi))$. By assumption $c(\sigma_1\sigma_2) = \sigma_{1*}(c(\sigma_2))c(\sigma_1)$, so that

$$H = \{\sigma \in \Gamma_F : c(\sigma) = 1\}$$

is a subgroup of Γ_F (though in general not a normal subgroup). It also follows that c is well defined on right cosets of H, so that $[\Gamma_F : H]$ divides n. Adjusting n if necessary, we may assume H is of index n. Now, $F_1 = {F_\mathrm{s}}^H$ has dimension n over F, and

$$K_1 = F_1 \otimes K$$

is a cyclic extension, generated by some $\alpha \in K$ such that $a = \alpha^n \in K$. Choosing α so that ϖ defined by (7) will satisfy $c(\varpi) = 1$, it is immediate that $a \in K^{(\varphi)}$ and $c = J^\varphi(a)$.

We now describe explicitly how the action of $\mathrm{Gal}(K/F)$ on K extends to K_1. Let τ be a generator of $\mathrm{Gal}(K/F)$, and fix $a \in K^{(\varphi)}$. Let

$$r \equiv \varphi(\tau) \pmod{n}$$

be an integer. By the assumption $\tau(a) \equiv a^r \pmod{K^{\times n}}$, so for some $\mu \in K^\times$ we have $\tau(a) = \mu^n a^r$. Let $\alpha = \sqrt[n]{a}$ be a generator of K_1 over K. For every j, $\tau_1(\alpha) = \rho^j\mu\alpha^r$ is a well defined automorphism of K_1. The fact that (9) splits ensures that j can be chosen so that $\tau_1^d(\alpha) = \alpha$. Changing μ accordingly, we may assume that

$$\tau'(\alpha) = \mu\alpha^r, \tag{15}$$

where $\tau \mapsto \tau'$ splits (9). In particular, choosing $F_1 = K_1^{\tau'}$, we can decompose $K_1 = K \otimes_F F_1$. The action of $\mathrm{Gal}(K/F)$ on K_1 will be used in Section 10 to define an action of $\mathrm{Gal}(K/F)$ on cyclic K-algebras.

The action of $\mathrm{Gal}(K/F)$ on K_1 which we just described can be refined in some cases, namely when φ does not generate the full character group $\mathrm{Gal}(K/F)^{\#}$. This refinement will be used in the construction of generic examples in Section 14.

Lemma 6.4. *Let $F \subseteq L \subseteq K$ be an intermediate subfield and $e = [L:F]$, a divisor of $d = [K:F]$. Then*

$$L^\times K^{\times n} = K^{(1)} K^{(\nu^{d/e})} \dots K^{(\nu^{(e-1)d/e})}.$$

Proof. Using Proposition 3.2, this is a special case of Lemma 5.7 with $\varphi_0 = 1$. □

Let $a \in K^{(\varphi)}$ as before, and let e denote the order of φ in the character group $\mathrm{Gal}(K/F)^{\#}$; equivalently, $\mathrm{Ker}(\varphi) = \langle \tau^e \rangle$; or, e is minimal such that $\varphi \in \left\langle \tau^{d/e} \right\rangle$. From the lemma it then follows that a can be taken to be an element of $L = K^{\tau^e}$.

Proposition 6.5. *Let $L = K^{\tau^e}$, and assume $a \in K^{(\varphi)} \cap L^\times$ for a character φ of order e, a proper divisor of $d = [K:F]$. Let $\alpha = \sqrt[n]{a}$ and $K_1 = K[\alpha]$. Then the action of $\mathrm{Gal}(K/F)$ can be extended to K_1 such that $\tau^e(\alpha) = \alpha$. Moreover, if $\tau(\alpha) = \mu\alpha^c$ for $\mu \in K$ and $c \equiv \varphi(\tau) \pmod n$, then $\mu \in L$.*

If $e = 2$, then we can choose $c = -1$, and then $\mu \in F$.

Proof. Choose $c = \varphi(\tau)$, and let $\mu \in K^\times$ be an element such that $\tau(a) = \mu^n a^c$. Extend τ to K_1 by setting $\tau(\alpha) = \mu\alpha^c$. Since $\tau^e(a) = a$, $(\tau^e(\alpha)\alpha^{-1})^n = 1$. Replacing α by $\rho^j\alpha$, we still have $\alpha^n = a$, but $\tau^e(\alpha)\alpha^{-1}$ is now multiplied by $\tau^e(\rho)\rho^{-1} = \rho^{j(\varphi(\tau^e)-1)}$. By Remark 2.1, $\varphi(\tau)^e - 1$ is invertible mod n, so there is a (unique) j for which $\tau^e(\alpha) = \alpha$.

Now compute that

$$\tau^{e-1}(\mu)\tau^{e-2}(\mu)^c \dots \mu^{c^{e-1}} \alpha^{c^e-1} = \tau^e(\alpha)\alpha^{-1} = 1,$$

so applying τ and dividing by the c-power of this equality, we find that $\tau^e(\mu) = \mu$.

Finally, assume $c = -1$, so that $\tau(\alpha) = \mu\alpha^{-1}$. Then $\mu = \alpha\tau(\alpha)$ which is a norm from K^{τ^2} to F. □

This proposition can be viewed (in the case $e = n$) as a direct proof that Equation (9) is a split extension.

7. An example

Many of the statements in this paper hold only if $d = [K:F]$ is prime to n, and providing counterexamples in this direction is an interesting and worthy task. In this section, which concludes the first part, we give one such example, and hint on some of the problems it arises.

Let $F = \mathbb{Q}[\sqrt{-2}]$, and $n = 4$. Adding the forth root of unity $\rho = \sqrt{-1}$, we obtain the field $K = F[\rho]$, where of course $d = [K:F] = 2$. Let τ denote the non-trivial automorphism of K over F. Notice that K contains an eighth root of unity, namely $\rho_8 = \frac{\sqrt{-2}}{2}(1-\rho)$ (and $\tau(\rho_8) = -\rho_8^{-1}$).

Let $a = 1+\sqrt{2}$, then $\mathrm{N}_{K/F}(a) = -1$ and $\tau(a) = -a^{-1} = \rho^2 a^{-1}$, so that $a \in K^{(\nu)}$ (where ν is the non-trivial character from $\mathrm{Gal}(K/F) = \langle\tau\rangle$ to $U_4 = \{\pm 1\}$). Let α be the forth root of a. Then by Proposition 3.4, $K_1 = K[\alpha]$ is Galois over F. Indeed, $\tau(\alpha) = \rho_8\alpha^{-1}$ preserves the defining relation $\alpha^4 = a$, and so extends from K to an automorphism of K_1 over F. In fact, $\tau^2(\alpha) = \tau(\rho_8\alpha^{-1}) = -\rho_8^{-1}(\rho_8\alpha^{-1})^{-1} = \rho\alpha$, $\tau^4(\alpha) = \tau^2(\rho\alpha) = -\alpha$, and $\tau^8(\alpha) = \alpha$; thus, $\mathrm{Gal}(K_1/F) = \langle\tau\rangle$ is a cyclic group of order 8.

In particular, the short exact sequence (9) does not split in this case, and there is no subfield F_1 of K_1 such that $K = K\otimes_F F_1$. Also, The character χ, which comes from the action of $\mathrm{Gal}(K/F)$ on $\mathrm{Gal}(K_1/K)$, is trivial.

Finally, suppose $c \in \mathrm{H}^1(F, \mu_4(\chi)) = \mathrm{Hom}(\Gamma_F, \mathbb{Z}/4)$ is defined with the basic properties of Section 5, namely that $c(\sigma)$ only depends on $\sigma|_{K_1}$, and that $c(\sigma) = 1$ for $\sigma \in \Gamma_K$. Since τ^2 is the identity on K we have that $c(\tau^2) = 1$, so c has order at most 2, and cannot be of order $n = 4$.

For the rest of the paper we again assume that $d = [K:F]$ is prime to n.

8. Central Simple Algebras

In the remaining sections we apply the results obtained so far on the first cohomology groups of F, to the theory of central simple algebras. Denote by ${}_n\mathrm{Br}(F)$ the exponent n part of the Brauer group of F.

Applying the long exact sequence of cohomology groups to the Kummer sequence (4), and using the identification $\mathrm{H}^2(F, {F_\mathrm{s}}^\times) = \mathrm{Br}(F)$ of the crossed products construction [7], we obtain the isomorphism $\mathrm{H}^2(F, \mu_n(\nu)) = {}_n\mathrm{Br}(F)$, where ν is the natural action of Γ_F on μ_n, defined in Equation (8). In general the action of G on tensor products

$M\otimes N$ is diagonal, so the cup product

$$\cup\colon \mathrm{H}^i(G,M)\otimes\mathrm{H}^j(G,N)\to\mathrm{H}^{i+j}(G,M\otimes N)$$

is in our notation a map

$$\mathrm{H}^1(F,\mu_n(\varphi))\otimes\mathrm{H}^1(F,\mu_n(\varphi'))\ \xrightarrow{\cup}\ \mathrm{H}^2(F,\mu_n(\varphi\varphi')).$$

In particular, for every character φ, letting $\chi=\nu\varphi^{-1}$, we have a map

$$\mathrm{H}^1(F,\mu_n(\varphi))\otimes\mathrm{H}^1(F,\mu_n(\chi))\ \xrightarrow{\cup}\ {}_n\mathrm{Br}(F),$$

which we explicitly describe below. The case $\varphi=1$ is well known (e.g. [15, p. 555]): an element $\gamma\in\mathrm{H}^1(F,\mu_n(1))=\mathrm{Hom}(\Gamma_F,\mathbb{Z}/n)$ has kernel $\Gamma_1=\mathrm{Ker}(\gamma)$, of index equal to the order of γ. Assuming γ has order n, let $F_1=F_{\mathrm{s}}^{\Gamma_1}$ be the invariant subfield, then F_1 is a cyclic extension of dimension n over F. Now, given $(b)\in\mathrm{H}^1(F,\mu_n(\nu))$ (which corresponds to an element $b\in F^\times$ by the isomorphism (5)), $\gamma\cup(b)$ is the Brauer class of the cyclic algebra

$$(F_1/F,\varpi,b)=F_1[z|\,zfz^{-1}=\varpi(f),\ z^n=b],$$

where ϖ is the generator of $\mathrm{Gal}(F_1/F)$ specified by $\gamma(\varpi)=1$. This is always an F-central simple algebra of degree n. When the construction is applied to $K=F[\rho_n]$ instead of F, we get what is called a symbol algebra,

$$(a)\cup(b)=(a,b)_K=K[x,y|\,x^n=a,\ y^n=b,\ yxy^{-1}=\rho x],$$

which is another notation for $(K[\sqrt[n]{a}\,]/K,\varpi,b)$.

We call a pair of generators x,y of (a,b) a *standard pair* if $x^n=a$, $y^n=b$ and $yxy^{-1}=\rho x$. The symbol $(a,b)_K$ is multiplicative in both variables, that is

$$(a,b_1b_2)_K\sim(a,b_1)_K\otimes(a,b_2)_K,$$
$$(a_1a_2,b)_K\sim(a_1,b)_K\otimes(a_2,b)_K.$$

By Merkurjev-Suslin theorem the symbol algebras of degree n generate ${}_n\mathrm{Br}(K)$. Strictly speaking, not every algebra of the form $(a,b)_K$ is a cyclic algebra, since $K[x]=K[\sqrt[n]{a}\,]$ need not be a field. However it is always split by the cyclic group C_n (in the sense of [18], as stated at the end of the introduction).

Let $\varphi,\varphi'\colon\mathrm{Gal}(K/F)\to U_n$ be characters such that $\varphi\varphi'=\nu$. To describe the cup product $\mathrm{H}^1(F,\mu_n(\varphi))\cup\mathrm{H}^1(F,\mu_n(\varphi'))$, recall that the maps

$$J^{\varphi}\colon K^{(\varphi)}/K^{\times n}\to\mathrm{H}^1(F,\mu_n(\varphi')),$$
$$J^{\varphi'}\colon K^{(\varphi')}/K^{\times n}\to\mathrm{H}^1(F,\mu_n(\varphi))$$

are onto (Corollary 5.4).

Proposition 8.1. *Let $\varphi, \varphi' \colon \mathrm{Gal}(K/F) \to U_n$ be characters such that $\varphi\varphi' = \nu$. Then for every $a \in K^{(\varphi)}$ and $b \in K^{(\varphi')}$, we have that*

$$J^{\varphi}(a) \cup J^{\varphi'}(b) \sim \mathrm{cor}_{K/F}(a,b)_K^{\otimes d'},$$

where d' is the inverse of d modulo n.

Proof. From Theorem 5.3 we have that $(a) = \mathrm{res}_{K/F} J^{\varphi}(a)$ and $(b) = \mathrm{res}_{K/F} J^{\varphi'}(b)$, where $(a), (b) \in \mathrm{H}^1(K, \mathbb{Z}/n)$. Thus, the projection formula gives

$$\begin{aligned} \mathrm{cor}(a,b)_K &= \mathrm{cor}((a) \cup (b)) \\ &= \mathrm{cor}(\mathrm{res} J^{\varphi}(a) \cup \mathrm{res} J^{\varphi'}(b)) \\ &= J^{\varphi}(a) \cup \mathrm{cor}(\mathrm{res} J^{\varphi'}(b)) \\ &= d \cdot J^{\varphi}(a) \cup J^{\varphi'}(b). \end{aligned}$$

□

Notice that if D has degree n over K, then $\mathrm{cor}_{K/F} D$ has degree $n^{[K:F]}$ over F. From time to time we will use a degree argument to write that the corestriction is equal (and not just similar) to a given algebra.

Corollary 8.2. *Under the assumptions of Proposition 8.1,*

$$\mathrm{res}_{K/F} \mathrm{cor}_{K/F}(a,b) = (a,b)^{\otimes d}.$$

Proof. By the commutativity of the restriction with the cup product,

$$\begin{aligned} \mathrm{res}\ \mathrm{cor}(a,b)_K &= d \cdot \mathrm{res}(J^{\varphi}(a) \cup J^{\varphi'}(b)) \\ &= d \cdot (a) \cup (b) \\ &= [(a,b)_K^{\otimes d}]. \end{aligned}$$

□

We now want to compute the algebra $\mathrm{cor}_{K/F}(a,b)_K$ for $a \in K^{(\varphi)}$ and $b \in K^{(\varphi')}$, without the assumption $\varphi\varphi' = \nu$. Just as above, the general projection formula yields

$$\mathrm{cor}((a) \cup (b)) = d \cdot J^{\varphi}(a) \cup J^{\varphi'}(b),$$

but the corestriction here is from ${}_n\mathrm{Br}(K) = \mathrm{H}^2(K, \mathbb{Z}/n)$ to $\mathrm{H}^2(F, \mu_n(\varphi\varphi'))$, which is in general *not* the corestriction of central simple algebras. To compute the algebra $\mathrm{cor}_{K/F}(a,b)_K$, we need to know what are the conjugate algebras $\tau(a,b)$ for $\tau \in \mathrm{Gal}(K/F)$ (see [11, p. 220]).

If $\sigma \in \Gamma_K$, then $\sigma(a,b)_{n;K} = (\sigma a, \sigma b)_{n;K}$. More generally, let $\sigma \in \Gamma_F$ be an automorphism. Letting

$$D = K[x, y |\, x^n = \sigma a,\ y^n = \sigma b,\ yxy^{-1} = \sigma\rho = \rho^t]$$

where $t = \nu(\sigma)$ and $tt' \equiv 1 \pmod{n}$, we see that $x^{t'}, y$ generate D with $yx^{t'}y^{-1} = \rho$, so by our definition $\sigma(a,b)_K = D$ is the symbol algebra $\left(\sigma a^{t'}, \sigma b\right)_K$.

Proposition 8.3. *Suppose $a \in K^{(\varphi)}$ and $b \in K^{(\varphi')}$, where $\varphi\varphi' \neq \nu$. Then the corestriction of algebras is*

$$\mathrm{cor}_{K/F}(a,b)_K \sim F.$$

Proof. Let $\phi = \varphi\varphi'\nu^{-1}$ ($\phi \neq 1$ by the assumption). For $a \in K^{(\varphi)}, b \in K^{(\varphi')}$ we have $\sigma(a,b)_K \sim (\sigma a, \sigma b)_K{}^{\otimes \nu(\sigma)^{-1}} \sim (a,b)_K{}^{\otimes \phi(\sigma)}$.

It is known (e.g. [17]) that

$$\mathrm{res}_{K/F}\mathrm{cor}_{K/F}(a,b) = \prod_{\tau \in \mathrm{Gal}(K/F)} \tau(a,b),$$

so we have

$$\begin{aligned} \mathrm{res}_{K/F}\mathrm{cor}_{K/F}(a,b) &= \prod (a,b)^{\otimes \phi(\tau)} \\ &= (a,b)^{\otimes \sum \phi(\tau)} \end{aligned}$$

and the result follows from Corollary 2.2, and the injectivity of $\mathrm{res}_{K/F}$. □

Let $\mathrm{R}_{n,K} \colon \mathrm{K}_2(K)/n \to {}_n\mathrm{Br}(K)$ denote the norm residue map

$$\mathrm{R}_{n,K} \colon \{a,b\} \mapsto (a,b)_K.$$

Corollary 8.4. *There is no map making the diagram (16) commutative, unless $\mathrm{K}_2(F)/n = 0$.*

$$\begin{array}{ccc} \mathrm{K}_2(F)/n & \xrightarrow{\mathrm{res}} & \mathrm{K}_2(K)/n \\ \vdots & & \downarrow{\scriptstyle \mathrm{R}_{n,K}} \\ {}_n\mathrm{Br}(F) & \xrightarrow{\mathrm{res}} & {}_n\mathrm{Br}(K) \end{array} \tag{16}$$

Proof. Let $\tilde{\mathrm{R}}_{n,F}$ denote a map making the diagram commute. Then for $\alpha, \beta \in F$,

$$\mathrm{res}_{K/F}\tilde{\mathrm{R}}_{n,F}\{\alpha,\beta\}_F = \mathrm{R}_{n,K}\mathrm{res}_{K/F}\{\alpha,\beta\}_F = (\alpha,\beta)_K.$$

Taking corestriction, we get

$$\left(\tilde{\mathrm{R}}_{n,F}\{\alpha,\beta\}_F\right)^{\otimes d} = \mathrm{cor}_{K/F}(\alpha,\beta)_K \sim F,$$

so that $\tilde{\mathrm{R}}_{n,F} = 0$. □

By the above computation, the $\mathrm{Gal}(K/F)$-eigenspace of ${}_n\mathrm{Br}(K)$ with respect to a character ψ is the subgroup

$$\Big\langle [(a,b)] : a \in K^{(\varphi)},\, b \in K^{(\varphi')}, \varphi\varphi' = \psi \Big\rangle.$$

Combining Corollary 8.2 and the proposition, we obtain the projection formula for K/F: given $a, b \in K^\times$, decompose $a = \prod a$ and $b = \prod b$ mod $K^{\times n}$ with $a_{,}b_{\in}K^{()}$; then

$$\mathrm{res}_{K/F}\mathrm{cor}_{K/F}(a,b) \sim \otimes_{\varphi\varphi'=\nu}(a_\varphi, b_{\varphi'})^{\otimes d}. \tag{17}$$

Corollary 8.5. *Let φ, φ' be characters with $\varphi\varphi' = \nu$, and let $a \in K^{(\varphi)}$, $b \in K^{(\varphi')}$, and $D = (a,b)_{n,K}$.*

Let D_0 be a central simple algebra of degree n over F. The following conditions are equivalent.

a. $\mathrm{res}_{K/F} D_0 = D$.

b. $D_0 \sim \mathrm{cor}_{K/F} D^{\otimes d'}$ *where d' is an inverse of d modulo n.*

Corollary 8.6. *Let D be a central simple algebra of degree n over F. If $D \otimes_F K = (a,b)_K$ and $a \in K^{(\varphi)}$, then we can assume $b \in K^{(\varphi')}$ where $\varphi\varphi' = \nu$.*

Proof. Let $b_{\varphi'}$ be the component of b in $K^{(\varphi')}$, then $\mathrm{cor}_{K/F}(a,b)_K = \mathrm{cor}_{K/F}(a, b_{\varphi'})_K$ by Proposition 8.3. By the previous corollary $D \sim \mathrm{cor}_{K/F}(a,b)_K{}^{\otimes d'} = \mathrm{cor}_{K/F}(a, b_{\varphi'})_K{}^{\otimes d'}$, and then also $\mathrm{res}_{K/F} D = (a, b_{\varphi'})_K$. □

9. Second cohomologies of F

In this section we consider eigenspaces of the second cohomology group $\mathrm{H}^2(K, \mu_n)$ for $K = F[\rho]$. The remarks we make here are not needed for later sections, where we focus on applications to central simple algebras.

The 'onto' part of the Merkurjev-Suslin Theorem [17, Thm 8.5], applied to K, shows that $\mathrm{H}^1(K,\mu_n) \cup \mathrm{H}^1(K,\mu_n) = \mathrm{H}^2(K,\mu_n)$, so in fact

$$\mathrm{H}^2(K,\mu_n) = \oplus_\psi \Big(\sum_{\varphi\varphi'=\psi} \mathrm{H}^1(K,\mu_n)^{(\varphi)} \cup \mathrm{H}^1(K,\mu_n)^{(\varphi')} \Big). \tag{18}$$

and in particular for every ψ,

$$\mathrm{H}^2(K,\mu_n)^{(\psi)} = \sum_{\varphi\varphi'=\psi} \mathrm{H}^1(K,\mu_n)^{(\varphi)} \cup \mathrm{H}^1(K,\mu_n)^{(\varphi')}. \tag{19}$$

Similarly to Corollary 5.6, we have the following isomorphism:

Theorem 9.1. *For every character* $\psi\colon \mathrm{Gal}(K/F)\to U_n$,

$$\mathrm{H}^2(K,\mu_n)^{(\psi)} \cong \mathrm{H}^2(F,\mu_n(\theta)),$$

where $\theta = \nu^2\psi^{-1}$.

Proof. We will show that the restriction $\mathrm{res}\colon \mathrm{H}^2(F,\mu_n(\theta))\to\mathrm{H}^2(K,\mu_n)$ (which is obviously injective) covers $\mathrm{H}^2(K,\mu_n)^{(\psi)}$.

Recall the general projection formula for cohomology groups: let M,N be Γ_F-modules, $a\in\mathrm{H}^1(F,M)$ and $b\in\mathrm{H}^1(K,N)$. Then

$$\mathrm{cor}(\mathrm{res}(a)\cup b) = a\cup\mathrm{cor}(b),$$

where the restriction is $\mathrm{H}^1(K,M)\to\mathrm{H}^1(F,M)$, the corestriction at the left hand side is $\mathrm{H}^2(F,M\otimes N)\to\mathrm{H}^2(K,M\otimes N)$ and the one at the right hand side is $\mathrm{H}^1(F,N)\to\mathrm{H}^1(K,N)$.

Let φ,φ' be arbitrary characters. We choose $M=N=\mu_n$ with the actions of Γ_F on M,N via $\chi=\nu\varphi^{-1}$ and $\theta\chi^{-1}$, respectively, so our restriction and corestriction are the maps

$$\begin{aligned}
\mathrm{res}_\chi &: \mathrm{H}^1(F,\mu_n(\chi))\to\mathrm{H}^1(K,\mu_n),\\
\mathrm{cor}_\theta &: \mathrm{H}^2(K,\mu_n)\to\mathrm{H}^2(F,\mu_n(\theta)),\\
\mathrm{cor}_{\theta\chi^{-1}} &: \mathrm{H}^1(K,\mu_n)\to\mathrm{H}^1(F,\mu_n(\theta\chi^{-1})).
\end{aligned}$$

We apply the projection formula to an element

$$u = c\cup c' \in \mathrm{H}^1(K,\mu_n)^{(\varphi)}\cup\mathrm{H}^1(K,\mu_n)^{(\varphi')}$$

in the decomposition (18). From Corollary 5.6 we have that

$$\mathrm{res}_\chi\mathrm{H}^1(F,\mu_n(\chi)) = \mathrm{H}^1(K,\mu_n)^{(\varphi)} \tag{20}$$

and similarly

$$\mathrm{res}_{\chi'}\mathrm{H}^1(F,\mu_n(\chi')) = \mathrm{H}^1(K,\mu_n)^{(\varphi')} \tag{21}$$

for $\chi'=\nu{\varphi'}^{-1}$, so we can write $c=\mathrm{res}_\chi a$ and $c'=\mathrm{res}_{\chi'}a'$ where $a\in\mathrm{H}^1(F,\mu_n(\chi))$ and $a'\in\mathrm{H}^1(F,\mu_n(\chi'))$. It follows that

$$\mathrm{cor}_\theta(c\cup c') = \mathrm{cor}_\theta(\mathrm{res}_\chi(a)\cup\mathrm{res}_{\chi'}(a')) = a\cup\mathrm{cor}_{\theta\chi^{-1}}\mathrm{res}_{\chi'}(a').$$

If $\chi\chi'=\theta$, then we find that $\mathrm{cor}_\theta(c\cup c') = d\cdot(a\cup a')$ since $\mathrm{cor}_{\chi'}\mathrm{res}_{\chi'}$ is multiplication by d. On the other hand if $\chi\chi'\neq\theta$ then by Corollary 5.5 we have that $\mathrm{cor}_{\theta\chi^{-1}}\mathrm{res}_{\chi'}(a')=0$, so that $\mathrm{cor}_\theta(c\cup c')=0$.

Applying cor_θ to (18) and recalling that cor_θ is onto $\mathrm{H}^2(F,\mu_n(\theta))$, we find that

$$\mathrm{H}^2(F,\mu_n(\theta)) = \sum_{\chi\chi'=\theta}\mathrm{H}^1(F,\mu_n(\chi))\cup\mathrm{H}^1(F,\mu_n(\chi')). \tag{22}$$

Finally applying $\mathrm{res}_\theta = \mathrm{res}_\chi \cup \mathrm{res}_{\chi'}$ (for every $\chi\chi' = \theta$), and using Equations (19), (20) and (21), we obtain

$$\mathrm{res}_\theta \mathrm{H}^2(F, \mu_n(\theta)) = \sum_{\varphi\varphi'=\psi} \mathrm{H}^1(K, \mu_n)^{(\varphi)} \cup \mathrm{H}^1(K, \mu_n)^{(\varphi')} = \mathrm{H}^2(K, \mu_n)^{(\psi)}.$$

□

The onto part of Merkurjev-Suslin for the field F gives the equality $\mathrm{H}^2(F, \mu_n(\nu^2)) = \mathrm{H}^1(F, \mu_n(\nu)) \cup \mathrm{H}^1(F, \mu_n(\nu))$, which is of course much better than Equation (22) for $\psi = 1$ (and $\theta = \nu^2$). It is not known if $\mathrm{H}^2(F, \mu_n(\nu)) = \mathrm{H}^1(F, \mu_n(\nu)) \cup \mathrm{H}^1(F, \mu_n(1))$ in general (see Question 10.6 below). A somewhat related negative result is given in the remark after Lemma 29 in [6].

10. Action of $\mathrm{Gal}(K/F)$ on $(a, b)_K$

In Section 8 we have seen that if $a \in K^{(\varphi)}$ and $b \in K^{(\varphi')}$ where $\varphi\varphi' = \nu$, then $\tau(a, b)_K = (a, b)_K$ for every $\tau \in \mathrm{Gal}(K/F)$.

Proposition 10.1. *Let φ, φ' be characters such that $\varphi\varphi' = \nu$, $a \in K^{(\varphi)}$ and $b \in K^{(\varphi')}$.*

There is a natural extension of the action of $\mathrm{Gal}(K/F)$ on K to an action on $D = (a, b)_K$.

Proof. As in Section 6, fix a generator τ of $\mathrm{Gal}(K/F)$, let $r \equiv \varphi(\tau)$, $r' \equiv \varphi'(\tau)$, and $t = rr' \equiv \nu(\tau)$. By the assumption on a, b, there exist $\mu, \eta \in K^\times$ such that

$$\tau(a) = \mu^n a^r \qquad \text{and} \qquad \tau(b) = \eta^n b^{r'}.$$

Define τ on

$$D = K[x, y |\, x^n = a,\ y^n = b,\ yxy^{-1} = \rho x]$$

by

$$\tau(x) = \mu x^r,$$
$$\tau(y) = \eta y^{r'},$$

where μ, η are chosen (i.e. multiplied by appropriate powers of ρ) so that $\tau^d(x) = x$ and $\tau^d(y) = y$. Since $\tau(yxy^{-1}) = \mu y^{r'} x^r y^{-r'} = \mu\rho^{rr'} x^r = \tau(\rho x)$, this action respects the defining relations, and is thus well defined on D. Finally, τ^d is the identity on $K[x, y] = D$. □

Lemma 10.2. *Let φ, φ' be characters with $\varphi\varphi' = \nu$, and let $a \in K^{(\varphi)}$, $b \in K^{(\varphi')}$. Let $D = (a, b)_{n,K}$ be a cyclic algebra over K.*

Let D_0 be a central simple algebra of degree n over F. The following conditions are equivalent.

a. $\mathrm{res}_{K/F} D_0 = D$.

b. $D_0 \sim \mathrm{cor}_{K/F} D^{\otimes d'}$ *where* d' *is an inverse of* d *modulo* n.

c. D_0 *is the invariant subalgebra* $D^{\mathrm{Gal}(K/F)}$ *under the action defined in Proposition 10.1.*

Proof. The equivalence of a. and b. is Corollary 8.5.

Let $G = \mathrm{Gal}(K/F)$. In general the invariant subalgebra D^G is central simple of degree n over $F = K^G$ [11, Cor. 7.2.15]. Since $\mathrm{res}_{K/F} D^G = D^G \otimes_F K = D$ and the restriction ${}_n\mathrm{Br}(F) \to {}_n\mathrm{Br}(K)$ is injective, a. is equivalent to c. □

The following theorem is proved in [8] for n prime.

Theorem 10.3. *Let* F *be a field of characteristic prime to* $n = p^m$, $K = F[\rho_n]$, *and assume that* $d = [K:F]$ *is prime to* n.

Let D_0 *be a central simple algebra of degree* n *over* F. D_0 *is cyclic if and only if there are* $a \in K^{(\nu)}$ *and* $\beta \in F^\times$ *where* $K_1 = K[\sqrt[n]{a}\,]$ *is a field, such that* $\mathrm{res}_{K/F} D_0 = (a, \beta)_{n,K}$.

Proof. If a, β are as assumed, then G acts on $D = (a,\beta)_K$ (by Proposition 10.1), $K_1 = K[\sqrt[n]{a}\,]$ is a subfield of D, and $F_1 = K_1^G$ is a cyclic subfield of D^G (Proposition 6.1).

On the other hand, if D_0 is cyclic of degree n over F, it has a cyclic subfield F_1 of dimension n over F, which again by Proposition 6.1 has the form $F_1 = K_1^G$ where $K_1 = K[\sqrt[n]{a}\,]$ is a field, for some $a \in K^{(\nu)}$. As D_0 is cyclic, we can write $D_0 = (F_1/F, \varpi, \beta)$ for some $\beta \in F$, and then $D = D_0 \otimes K = (K_1/K, \varpi, \beta) = (a,\beta)_K$. □

Definition 10.4. *An algebra* D_0 *of degree* n *over* F *which satisfies the conditions of Lemma 10.2, is called a quasi-symbol (of type* (φ, φ')*).*

We give a description of quasi-symbols in terms of their splitting fields in Proposition 13.1 below.

Under the assumption that $[K:F]$ is prime to n, the corestriction from ${}_n\mathrm{Br}(K)$ to ${}_n\mathrm{Br}(F)$ is onto, so by the projection formula (17), ${}_n\mathrm{Br}(F)$ is generated by quasi-symbols.

Question 10.5. *Are quasi-symbols cyclic over* F*?*

By the Theorem 10.3, quasi-symbols of type $(1, \nu)$ (or $(\nu, 1)$) are cyclic, but nothing is known in general about the cyclicity of other quasi-symbols.

Merkurjev proved in [8] that ${}_n\mathrm{Br}(F)$ is generated by cyclic algebras (of degree dividing n) if $[K:F] \le 3$. This is not known if $[K:F] \ge 4$.

Question 10.6. *Is* ${}_n\mathrm{Br}(F)$ *generated by (the classes of) algebras which are split by* C_n*?*

Of course, a positive answer to the first question will answer the second. One approach is to compute the corestriction of cyclic algebras from K to F; we return to this in Section 12.

We conclude this section with a remark concerning involutions of the second kind. We touch this subject again in Proposition 11.6. In Proposition 8.3 we saw that algebras of the form $A = (a,b)_K$ where $a \in K^{(\varphi)}$ and $b \in K^{(\varphi')}$ and $\varphi\varphi' \neq \nu$, have trivial corestriction. If $[K:F] = 2$, this is known to be equivalent to the existence of an involution of the second kind on A for which the invariant subfield of the center is F. Since we assume $[K:F] = 2$, there are only two cases to consider: either $a, b \in K^{(1)} = F^\times K^{\times n}$, or $a, b \in K^{(\nu)}$. A similar configuration is studied in [4, Thm. 3.5]; it is shown there that if $[K:F] = 2$ and a cyclic algebra $A = (\alpha, b)_K$ has an involution of the second kind over F where $\alpha \in F$, then one can assume $b \in F$. This theorem covers also the case of even n (where it is assumed that $\tau(\rho) = \rho^{-1}$).

Similarly to Proposition 10.1, we now use the action of $\mathrm{Gal}(K/F)$ on $K[x]$ and $K[y]$ (where x, y are a standard pair of generators of A) to define an involution of the second kind on A.

Assume that $[K:F] = 2$, and let $\tau \in \mathrm{Gal}(K/F)$ be the non-trivial automorphism. Note that $\tau(\rho) = \rho^{-1}$. Let $\varphi(\tau) = \epsilon$ define a character, where $\epsilon = \pm 1$ is fixed. Let $a, b \in K^{(\varphi)}$ and

$$A = (a,b)_K = K[x, y |\, x^n = a,\ y^n = b,\ yx = \rho xy].$$

By assumption there are $\mu, \eta \in K^\times$ such that $\tau(a) = \mu^n a^\epsilon$ and $\tau(b) = \eta^n b^\epsilon$. Define a linear map $(*)$ on A by

$$(\sum k_{ij} x^i y^j)^* = \sum \tau(k_{ij})(y^*)^j (x^*)^i$$

where $x^* = \mu x^\epsilon$ and $y^* = \eta y^\epsilon$. The relations $x^n = a$ and $y^n = b$ are automatically preserved, and for both possible values of ϵ, $(yx)^* = (\rho xy)^* = \rho^{-1}\mu y^\epsilon \eta x^\epsilon = \mu\eta x^\epsilon y^\epsilon = x^* y^*$. Finally, $x^{**} = x$ and $y^{**} = y$ by the choice of μ, η, so that $u \mapsto u^*$ is an involution.

11. Albert's cyclicity criterion

Every cyclic algebra $D = (F_1/F, \varpi, b)$ has by definition an element $z \in D$ such that $z^n = b$ is central. In the "special results" chapter (Chapter XI) of his seminal book [2], Albert proves the converse, which is known as Albert's cyclicity criterion: a central simple algebra D of prime degree p over a field F of characteristic prime to p is cyclic, if and only if $u^p \in F$ for some non-central $u \in D$. Of course the assertion follows from Kummer theory if F has p-roots of unity. Albert remarks [2, p. 175] that the criterion fails if the degree is not a prime, and

indeed in [3] he provides an example of a non-cyclic algebra of degree (and exponent) 4, with an element u such that u^4 is central but u^2 is not. In Theorem 11.4 below we generalize Albert's criterion, and show that it holds for algebras of degree $n = p^m$ over a field F, assuming that $d = [K:F]$ is prime to n, where as always $K = F[\rho_n]$.

The following is a slightly more general version of Theorem 10.3.

Proposition 11.1. *Let n be a prime power, $K = F[\rho]$ where ρ is a primitive n-root, and assume $d = [K:F]$ is prime to n.*

Let $a \in K^\times$ and $\beta \in F^\times$. Then $A = \mathrm{cor}_{K/F}(a,\beta)_{n,K}$ is split by C_n.

Proof. Since $\beta \in F^\times \subseteq K^{(1)}$, we can by Corollary 8.6 replace a by its ν-component, so we assume $a \in K^{(\nu)}$. Let $D = \left(a, \beta^d\right)_K$. The projection formula for K/F (Equation (17)) gives $\mathrm{res}_{K/F} A \sim D$, which is an algebra of degree n. Since d is prime to n, the index of A divides n.

Let D_0 be a the central simple algebra of degree n over F which is similar to A. Then $\mathrm{res}_{K/F} D_0 = D$, so if $K[\sqrt[n]{a}]$ is a field, D_0 is cyclic by Theorem 10.3. For the general case, let n' denote the order of a in $K^\times/K^{\times n}$; equivalently, n' is the maximal divisor of n such that $a \in K^{\times n/n'}$. Write $a = c^{n/n'}$ for some $c \in K^\times$; then

$$D = \left(a, \beta^d\right)_{n,K} = \left(c^{n/n'}, \beta^d\right)_{n,K} \sim \left(c, \beta^d\right)_{n',K},$$

and $K[\sqrt[n']{c}]$ is a field. In particular,

$$A \sim \mathrm{cor}_{K/F} D^{\otimes d'} \sim \mathrm{cor}_{K/F}(c,\beta)_{n',K},$$

where d' is the inverse of d modulo n. Let D_1 be the algebra of degree n' similar to A. By Lemma 10.2 we have that $\mathrm{res}_{K/F} D_1 = \mathrm{cor}_{K/F}(c,\beta)_{n',K}$. In order to show that D_1 is cyclic, we need to know that c is in the ν-component of the decomposition of $K^\times/K^{\times n'}$. Indeed, Let τ be a generator of $\mathrm{Gal}(K/F)$, and $t = \nu(\tau)$. For some $\mu \in K^\times$ we have $\tau(a) = \mu^n a^t$, so that $\tau(c) = (\rho^i \mu)^{n'} c^t$ for some i. We are now done by Theorem 10.3. □

Example 11.2. *Assume that the p-part of the group of units in K has order n, and take $a = \rho^{n/n'}$ in the above corollary. Then a has order n' in $K^\times/K^{\times n}$, and*

$$\mathrm{cor}_{K/F}\left(\rho^{n/n'}, \beta\right)_K \sim (F_1/F, \varpi, \beta^d),$$

a cyclic algebra of degree n', with $F_1 \subseteq K_1 = F[\sqrt[n']{\rho}]$.

Corollary 11.3. *With F, n, K as in the proposition, let D_0 be a division algebra of degree n over F. If $\mathrm{res}_{K/F} D_0 = (a, \beta)$ for some $a \in K^\times$ and $\beta \in F^\times$, then D_0 is cyclic.*

Proof. Let d' be an inverse of d modulo n. By Lemma 8.5 $D_0 \sim \mathrm{cor}_{K/F}\big(a, \beta^{d'}\big)$, so by the proposition D_0 is similar to a cyclic algebra of degree dividing n, and being a division algebra it is cyclic. □

This leads directly to the general form of Albert's theorem.

Theorem 11.4. *Let F be a field as above. Let D be a central division algebra of degree n over F, with an element $u \in D$ such that $[F[u]:F] = n$ and $\beta = u^n \in F^\times$. Then D is cyclic.*

Proof. Since $F[u]$ splits D, the field $K[u] = K \otimes F[u]$ splits $K \otimes D$. Thus, there exists an element $a \in K^\times$ such that $\mathrm{res}_{K/F} D = (a, \beta)_K$, and we are done by the corollary. □

A standard argument using idempotents gives the following more general result.

Corollary 11.5. *Let F be a field as above. Let D be a central simple algebra of degree n over F, with an element $u \in D$ such that $[F[u]:F] = n$ and $\beta = u^n \in F^\times$. Then D is split by C_n.*

Proof. If $F[u]$ is a field then D is cyclic by the proof given above. Otherwise, let n' be the order of u in $F^\times / F^{\times n}$. Let $D_1 = D \otimes_F K$. The subring $K[u^{n'}]$ of D_1 is isomorphic to a direct product of n/n' copies of K. Let $C = \mathrm{Cent}_{D_1}(K[u^{n'}])$. Taking a minimal idempotent e_1 of $K[u^{n'}]$, Ce_1 is a central simple algebra of degree n' over $Ke_1 \cong K$ and $Ke_1[ue_1]$ is a subfield of dimension n' of Ce_1, so Ce_1 is cyclic. We are done since $D_1 \sim Ce_1$. □

It would be interesting to have examples of non-cyclic algebras of odd degree $n = p^2$ with an n-central element, when $[K:F]$ is divisible by p. As mentioned above, Albert gave such an example for $p = 2$.

We prove another generalization of Albert's theorem, due to N. Elkayam [4, Thm. 3.9]. We give only the version of prime degree, as the generalization to prime-power degree along the lines drawn above is easy.

Proposition 11.6. *Let D be a central division algebra of degree p over F, with an involution of the second kind over F/F_0, and assume $F_0[\rho] = F[\rho]$.*

If D has a symmetric element $u \notin F$ such that $u^p \in F$, then D contains a subfield F_1 Galois over F_0, such that $\mathrm{Gal}(F_1/F_0)$ is dihedral.

Proof. Let $d = [K:F]$, and let ϵ be the element of order 2 in the character group of $\mathrm{Gal}(K/F_0) \cong \mathbb{Z}/2d$. Let $\nu_0 \colon \mathrm{Gal}(K/F_0) \to U_p$ be the character defined by Equation (8) for the extension K/F_0, and ν the restriction to $\mathrm{Gal}(K/F)$; there are two characters of $\mathrm{Gal}(K/F_0)$ whose restriction is ν, namely ν_0 and $\nu_0\epsilon$. By Lemma 5.7 we have that $K^{(\nu)} = K^{(\nu_0)}K^{(\nu_0\epsilon)}$, where $K^{(\nu)}$ is the component with respect to the action of $\mathrm{Gal}(K/F)$ on $K^\times$, and $K^{(\nu_0)}, K^{(\nu_0\epsilon)}$ are components with respect to the action of $\mathrm{Gal}(K/F_0)$.

By the assumption, $\alpha = u^p \in F_0$. Moreover, $K[u] \subseteq D \otimes_F K$ is a cyclic subfield, and we can write $D_1 = D \otimes_F K = (\alpha, b)_K$ for some $b \in K^\times$. By Corollary 8.6, we may assume $b \in K^{(\nu)}$. Let $b = b_{\nu_0} b_{\nu_0\epsilon}$ be the decomposition to eigenvectors with respect to the action of $\mathrm{Gal}(K/F_0)$. Since $\mathrm{cor}_{F/F_0} D \sim F_0$, we have that $F_0 \sim \mathrm{cor}_{F/F_0} D^{\otimes d} = \mathrm{cor}_{F/F_0}\mathrm{cor}_{K/F} D_1 = \mathrm{cor}_{K/F_0}(\alpha, b)_K = \mathrm{cor}_{K/F_0}(\alpha, b_{\nu_0})_K$, so that in fact $D^{\otimes d} \sim \mathrm{cor}_{K/F}\mathrm{res}_{K/F} D \sim \mathrm{cor}_{K/F}(\alpha, b_{\nu\epsilon})_K$. Letting $D_2 = (a, b_{\nu\epsilon})_K$ we have that $D = D_2^{\mathrm{Gal}(K/F)}$ by Lemma 10.2.

But now, $K_1 = K[\sqrt[p]{b_{\nu\epsilon}}]$ is Galois over F_0 with Galois group $\mathbb{Z}/d \rtimes \mathbb{Z}/p$, where the action is by the character ϵ. In particular, letting τ be a generator of $\mathrm{Gal}(K/F_0)$, τ^2 is central in $\mathrm{Gal}(K/F_0)$, and $K_1^{\tau^2} \subseteq D_2^{\tau^2} = D$ is Galois over F_0, with $\mathrm{Gal}(K_1^{\tau^2}/F_0) \cong D_p$. □

12. Corestriction of cyclic algebras

Rosset and Tate proved in [10] that if K_2/K_1 is an extension of fields in which K_1 has n-roots of unity, then the corestriction of a cyclic algebra of degree n over K_2 to K_1 is similar to a product of at most $[K_2:K_1]$ cyclic algebras of the same degree. No similar result is known if K_1 does not have roots of unity (see [11], the remark after Corollary 7.2.39). A general result in this direction should not be easy to obtain, as it would imply a positive answer to Question 10.6.

In [8, Lemma 2], Merkurjev proved that if $[K:F] \leq 3$ (for an arbitrary fields extension K/F), then $\mathrm{K}_2(K)$ is generated by symbols of the form $\{K, F\}$ (i.e. with one entry in F; this is how Question 10.6 is solved in this case). We give an explicit version of this useful lemma.

Lemma 12.1. *Let K/F be any extension of fields, and let $a, b \in K$, $a, b \notin F$. Then the following identities hold in* $\mathrm{K}_2(K)$.

a. Assume $[K:F] = 2$, and write $b = \alpha + \beta a$, $\alpha, \beta \in F$. Then

$$\{a, b\} = \begin{cases} \left\{\frac{b}{\beta}, -\frac{\beta}{\alpha}\right\} + \{a, \alpha\} & \text{if } \alpha \neq 0 \\ \{a, -\beta\} & \text{if } \alpha = 0 \end{cases} \tag{23}$$

b. Assume $[K:F]=3$*, and write* $b=g(a)$*,* $g\in F[\lambda]$ *a polynomial of degree* ≤ 2*. Since the minimal polynomial of* a *is of degree* 3*, there are* $\alpha+\beta\lambda,\alpha'+\beta'\lambda\in F[\lambda]$ *such that* $(\alpha+\beta a)\cdot g(a)=\alpha'+\beta' a$*. Then we have (where in each case we only indicate the coefficients equal to zero):*

$$\{a,b\}=\begin{cases}\left\{a,-\frac{\beta'}{\alpha}\right\} & \alpha'=\beta=0\\ \left\{a,-\frac{\alpha'}{\beta}\right\} & \alpha=\beta'=0\\ \{a,-\beta'\}-\left\{b,-\frac{\beta}{\alpha}\right\}-\{\beta a,\alpha\} & \alpha'=0\\ \{a,\alpha'\}-\left\{b,-\frac{\beta}{\alpha}\right\}-\{\beta a,\alpha\} & \beta'=0\\ \left\{b,-\frac{\beta'}{\alpha'}\right\}+\{\beta' a,\alpha'\}-\{a,-\beta\} & \alpha=0\\ \left\{b,-\frac{\beta'}{\alpha'}\right\}+\{\beta' a,\alpha'\}-\{a,\alpha\} & \beta=0\\ \left\{a,\frac{\alpha'}{\alpha}\right\}+\left\{\frac{\alpha'+\beta' a}{\alpha'},\frac{-\beta'}{\alpha'}\right\}+\left\{\frac{\alpha+\beta a}{\alpha},\frac{-\alpha}{\beta}\right\} & \end{cases}$$

Proof. For the $[K:F]=2$ case, compute that

$$\begin{aligned}\{a,b\}-\{a,\alpha\} &= \left\{a,1+\frac{\beta a}{\alpha}\right\}\\ &= \left\{a,1+\frac{\beta a}{\alpha}\right\}-\left\{-\frac{\beta a}{\alpha},1+\frac{\beta a}{\alpha}\right\}\\ &= \left\{-\frac{\alpha}{\beta},\frac{b}{\alpha}\right\}=\left\{\frac{b}{\alpha},-\frac{\beta}{\alpha}\right\}=\left\{\frac{b}{\beta},-\frac{\beta}{\alpha}\right\},\end{aligned}$$

where the last equality follows from $\left\{\frac{\beta}{\alpha},-\frac{\beta}{\alpha}\right\}=0$. The case $[K:F]=3$ follows from $\{a,b\}=\{a,\alpha'+\beta' b\}-\{a,\alpha+\beta b\}$, applying the case of dimension 2 for each of these symbols. □

We can now prove a version of the Rosset-Tate theorem for the corestriction from K to F, if $[K:F]\leq 3$ (under the usual assumptions that $[K:F]$ is prime to n).

Proposition 12.2. *Let* $D=(a,b)_{n,K}$ *be a cyclic algebra over* K*. If* $[K:F]\leq 3$*, then* $\mathrm{cor}_{K/F}D$ *is similar to a product of at most* $[K:F]$ *algebras which are split by* C_n*.*

Proof. The corestriction of an algebra of the form (c,γ), $c\in K$ and $\gamma\in F$, is split by C_n by Proposition 11.1. Expressing $(a,b)_K$ as a product of at most $[K:F]$ symbols of this form (using the previous lemma), we are done by taking corestriction.

We remark that the case $[K:F]=2$ also follows from decomposing $a=a_1a_\nu$ and $b=b_1b_\nu$ as in Equation (17), for then $\mathrm{cor}(a,b)_K\sim \mathrm{cor}(a_1,b_\nu)_K\otimes\mathrm{cor}(a_\nu,b_1)_K$. □

Corollary 12.3. *Let L/F be a separable extension of fields of characteristic prime to n, such that $d = [K:F] \leq 3$ where $K = F[\rho]$. If D is cyclic of degree n over L, then $\mathrm{cor}_{L/F}D$ is similar to a product of at most*

$$d \cdot ([L:F] - 1) + 1$$

algebras which are split by C_n.

Proof. Let $m = [L:F]$. If $K \subseteq L$ then in fact we only need $[L:F]$ cyclic algebras, since $\mathrm{cor}_{L/K}D$ is similar to a product of $[L:K]$ cyclics of degree n over K, and the corestriction down to F requires $[K:F]$ cyclics to each of these by the proposition.

So suppose L does not contain K, and let $T = L[\rho] = L \otimes_F K$. Since D is cyclic over L, we can (by Proposition 10.3) write $\mathrm{res}_{T/L}D = (a, \beta)_n$ for $a \in T$ and $\beta \in L$. Let $D_2 = \left(a^{d'}, \beta\right)_n$, where $dd' \equiv 1 \pmod{n}$, and note that

$$\mathrm{cor}_{L/F}D \sim \mathrm{cor}_{L/F}\mathrm{cor}_{T/L}D_2 = \mathrm{cor}_{K/F}\mathrm{cor}_{T/K}D_2.$$

By the Rosset-Tate algorithm, $\mathrm{cor}_{T/K}D_2$ is a product of $[T:K] = m$ symbols, the first of which is $\left(c, \mathrm{N}_{T/K}(\beta)\right)_K$ for some $c \in K$ [11, Cor. 7.2.38]. Since $\mathrm{N}_{T/K}(\beta) = \mathrm{N}_{L/F}(\beta) \in F$, the corestriction from K to F of this first symbol is split by C_n (Proposition 11.1). The corestriction of each of the other $m - 1$ symbols is similar to a product of d cyclic algebras over F by the previous proposition. □

The bound $d \cdot ([L:F] - 1) + 1$ of the corollary is higher than the $[L:F]$ value suggested by the Rosset-Tate result. In the proof we write $\mathrm{res}_{T/L}D = (a, \beta)$ for $a \in T$ and $\beta \in L$, and ignore the fact that $a \in T^{(\nu)}$. This can be used to improve the bound if $[L:F] = [K:F] = 2$.

Theorem 12.4. *Suppose that $K = F[\rho]$ is quadratic over F, and let L/F be any separable quadratic extension. Let D_1 be a cyclic algebra of degree n (an odd prime power) over L.*

Then $\mathrm{cor}_{L/F}D_1$ is similar to a product of at most two algebras over F which are split by C_n.

Proof. If $L = K$ then the result follows from Proposition 12.2, and we assume this is not the case. Let

$$T = L[\rho] = L \otimes_F K,$$

a quadratic extension of K. By Theorem 10.3,

$$D_2 = \mathrm{res}_{T/L}D_1 = (a, \beta)_T$$

where $a \in T^{(\nu)}$ and $\beta \in L$; in fact we can assume $\mathrm{N}_{T/L}(a) = 1$ (see Remark 3.5). We compute $\mathrm{cor}_{T/K}D_2$ using Equation (23). If $\beta \in F \subseteq$

K then $\mathrm{cor}_{T/K} D_2 = \big(\mathrm{N}_{T/K}(a), \beta\big)_K$ is cyclic, and the corestriction from K to F is split by C_n by Proposition 11.1. We thus assume $\beta \notin F$, so that $K[\beta] = T$.

Choose $c, d \in K$ such that $a = d + c\beta$. By the above argument we may assume $a \notin K$, so that $c \neq 0$. Similarly if $d = 0$ then $(a, \beta) = (c\beta, \beta) = (-c, \beta)$, and we are back in the case $a \in K$. We thus assume $d \neq 0$.

By Equation (23) (taking the opposite of all the symbols involved),

$$D_2 = (a, \beta)_T \sim \Big(-\frac{c}{d}, \frac{a}{c}\Big)_T \otimes_T (d, \beta)_T,$$

so that

$$\mathrm{cor}_{T/K} D_2 = \Big(-\frac{c}{d}, \mathrm{N}_{T/K}(\frac{a}{c})\Big)_K \otimes_K \big(d, \mathrm{N}_{L/F}(\beta)\big)_K. \tag{24}$$

The right-hand symbol has at least one entry, namely $\mathrm{N}_{L/F}(\beta)$, in F, and so its corestriction from K to F is split by C_n. Let σ denote the non-trivial automorphism of L/F (which extends to T/K as the identity on K). We will show that $\mathrm{N}_{T/K}(a/c) \in F$. Consider the polynomial

$$g(\lambda) = \mathrm{N}_{K/F}(\lambda + \frac{d}{c}) - \mathrm{N}_{K/F}(\frac{1}{c}),$$

which is quadratic over F. Since

$$g(\beta) = \mathrm{N}_{T/L}(a/c) - \mathrm{N}_{K/F}(1/c) = 0,$$

g is the minimal polynomial of β, and $\sigma(\beta)$ is its other root. It follows that $g(\lambda) = \lambda^2 - (\beta + \sigma(\beta))\lambda + \beta \cdot \sigma(\beta)$, so comparing coefficients we obtain

$$\beta + \sigma(\beta) = -\left(\frac{\tau(d)}{\tau(c)} + \frac{d}{c}\right),$$
$$\beta \cdot \sigma(\beta) = \frac{\tau(d)d - 1}{\tau(c)c},$$

where τ generates $\mathrm{Gal}(K/F)$. We can now compute that

$$\begin{aligned} \mathrm{N}_{T/K}(a/c) &= \mathrm{N}_{T/K}(d/c + \beta) \\ &= (d/c + \beta)(d/c + \sigma(\beta)) \\ &= \frac{d^2}{c^2} - \frac{d}{c}\left(\frac{\tau(d)}{\tau(c)} + \frac{d}{c}\right) + \frac{\tau(d)d - 1}{\tau(c)c} \\ &= -\frac{1}{\tau(c)c}. \end{aligned} \tag{25}$$

It follows that $\mathrm{N}_{T/K}(a/c) \in F$, and the left-hand symbol in Equation (24) also has one entry in F. The corestriction from K to F of $\mathrm{cor}_{T/K} D_2$ is thus similar to the product of two algebras split by C_n. □

By induction, we obtain

Corollary 12.5. *Let L/F be a separable extension and assume there is a chain of quadratic extensions from F to L. Also assume that $[K:F]=2$ where $K=F[\rho]$.*

For every cyclic algebra D_1 of degree n over L, $\mathrm{cor}_{L/F}D_1$ is similar to a product of at most $[L:F]$ algebras split by C_n.

In the situation described in Theorem 12.4, it is obvious that $D_2 = \mathrm{res}_{T/L}D_1$ is invariant under the action of $\mathrm{Gal}(K/F)$, and that the corestriction $\mathrm{cor}_{T/K}D_2$ is a product of two symbol algebras over K. This can be improved:

Remark 12.6. *The algebra D_2 of Theorem 12.4 satisfies*

$$\mathrm{cor}_{T/K}D_2 = (\tau(c),c)_K \otimes_K (d, 1-\tau(d)d)_K, \tag{26}$$

where both symbols in this expression are invariant under $\mathrm{Gal}(K/F)$, and their corestriction to F is split by C_n.

Proof. We continue the computation from Equation (24), using the equality $\mathrm{N}_{T/K}(a/c) = -1/\tau(c)c$ proved in Equation (25) and the value $\mathrm{N}_{L/F}(\beta) = (\tau(d)d-1)/\tau(c)c$.

$$\begin{aligned}
\mathrm{cor}_{T/K}D_2 &= \left(-\frac{c}{d}, -\frac{1}{\tau(c)c}\right)_K \otimes_K \big(d, \mathrm{N}_{L/F}(\beta)\big)_K \\
&= \left(-c, -\frac{1}{\tau(c)c}\right)_K \otimes_K \big(d, -\tau(c)c\mathrm{N}_{L/F}(\beta)\big)_K \\
&= (\tau(c),c)_K \otimes_K (d, 1-\tau(d)d)_K,
\end{aligned}$$

where we use the fact that $(c,-c) \sim K$ and that -1 is an n-power in K (since n is odd). Writing $c = c_1 c_\nu$ for $c_1 \in F^\times$ and $c_1 \in K^{(\nu)}$, one can check that $(\tau(c),c) = (c_1^2, c_\nu)$; likewise $1-\tau(d)d \in F$, so the corestriction of both symbols is split by C_n by Proposition 11.1.

Recall that $\tau(\rho) = \rho^{-1}$ (since $[K:F]=2$), so in general $\tau(u,v)_K = (\tau(u),\tau(v))^{\mathrm{op}}$. Now

$$\tau(\tau(c),c)_K = (c,\tau(c))_K{}^{\mathrm{op}} = (\tau(c),c)_K,$$

and

$$\begin{aligned}
\tau(d, 1-\tau(d)d)_K &= (\tau(d), 1-\tau(d)d)_K{}^{\mathrm{op}} \\
&\sim (\tau(d)d, 1-\tau(d)d)_K{}^{\mathrm{op}} \otimes (d, 1-\tau(d)d)_K \\
&\sim (d, 1-\tau(d)d)_K.
\end{aligned}$$

□

13. Semidirect crossed products

Rowen and Saltman [13] proved that if D is a division algebra of prime degree p over a field L with p roots of unity, and D is split by a field T such that $\mathrm{Gal}(T/L) = \mathbb{Z}/e \rtimes \mathbb{Z}/p$, where $e = 2, 3, 4$ or 6 and divides $p-1$, then D is cyclic. Our version (Corollary 13.4 below) holds for any prime-power degree $n = p^k$ and arbitrary e (dividing $p-1$), and rather than assuming the base field contains roots of unity, we assume that the splitting field contains them. On the other hand, the cyclicity result only holds for specific semidirect products. To make the notation clear, if τ is a generator of $\mathbb{Z}/d$ and $\varphi\colon \mathbb{Z}/d \to U_n$ is a character defined by $\varphi(\tau) = t$, then we set

$$\mathbb{Z}/d \rtimes_\varphi \mathbb{Z}/n = \left\langle \varpi, \tau \,|\, \varpi^n = \tau^d = 1,\ \tau\varpi\tau^{-1} = \varpi^t \right\rangle.$$

The cyclicity of semidirect crossed products is strongly related to Question 10.5, as the following observation on quasi-symbols (see Definition 10.4) shows.

Proposition 13.1. *A central simple algebra D of degree n over F is a quasi-symbol, iff it has a splitting field $S \supset K$ which is Galois over F with Galois group a semidirect product $\mathbb{Z}/d \rtimes \mathbb{Z}/n$.*

The splitting field S has $\mathrm{Gal}(S/F) = \mathbb{Z}/d \rtimes_\varphi \mathbb{Z}/n$ iff D is of type $(\varphi, \nu\varphi^{-1})$.

Proof. If $\mathrm{res}_{K/F} D = (a, b)$ for $a \in K^{(\varphi)}$ and $b \in K^{(\varphi')}$, then $S = K[\sqrt[n]{a}\,]$ is a splitting field satisfying the assumptions (by Proposition 3.4).

On the other hand, let S be a splitting field satisfying the assumptions. Then S is Galois over K, and $\mathrm{Gal}(S/K) \cong \mathbb{Z}/n$ since this is the unique normal subgroup of order n of $\mathbb{Z}/d \rtimes \mathbb{Z}/n$. We can thus write $S = K[\alpha]$ where $\alpha^n = a \in K$, and again by Proposition 3.4, $a \in K^{(\varphi)}$ for some character φ. By Corollary 8.6 there is an element $b \in K^{(\varphi')}$ such that $D \otimes_F K = (a, b)_K$, where $\varphi\varphi' = \nu$. Finally, in this case $\mathrm{Gal}(S/F) = \mathbb{Z}/d \rtimes_{\varphi'} \mathbb{Z}/n$ by Remark 5.1. □

It follows that semidirect product splitting fields come in pairs:

Corollary 13.2. *Let φ, φ' be characters with $\varphi\varphi' = \nu$. A central simple algebra of degree n over F has a splitting field containing K with Galois group $\mathbb{Z}/d \rtimes_\varphi \mathbb{Z}/n$ iff it has a splitting field containing K with Galois group $\mathbb{Z}/d \rtimes_{\varphi'} \mathbb{Z}/n$.*

Proposition 13.1 can be extended to characterize quasi-symbols with splitting fields of smaller dimension.

Proposition 13.3. *Let $F \subseteq L \subseteq K$ be an intermediate field of dimension $e = [L:F]$, and let D be a central simple algebra of degree n over F.*

Then D has a splitting field $S \supset L$ such that $\mathrm{Gal}(S/F) = \mathbb{Z}/e \rtimes \mathbb{Z}/n$, iff D is a quasi-symbol of type (φ, φ') for φ of order e in $\mathrm{Gal}(K/F)^{\#}$.

Proof. Let $S \supset L$ be a splitting field which is Galois over F. We want to check that $S_1 = S \otimes_L K$ is also Galois over F, and for that we need to count automorphisms of S_1 over F.

Let ϖ denote a generator for $\mathrm{Gal}(S/L)$, and let τ be a generator of $\mathrm{Gal}(K/L)$. Since S/F is Galois, τ extends to an automorphism (of order e) of S. But τ is also defined on K, and thus on S_1. Likewise ϖ extends to S_1 as the identity on K. Finally, we have that $\tau\varpi\tau^{-1} = \varpi^r$ on S for some r, and the same relation trivially holds on K (since ϖ is the identity on K) and thus on S_1. It follows that $|\langle \varpi, \tau \rangle| = nd$ and S_1/F is Galois. In particular $S = S_1^{\tau^e}$.

Now let φ denote the character defining the action of $\mathrm{Gal}(K/F)$ on $\mathrm{Gal}(S_1/K)$. Since S/F is Galois, $\langle \tau^e \rangle$ is normal in $\mathrm{Gal}(S_1/F)$; as easily seen, this is equivalent to τ^e being central; which is equivalent to $\varphi^e = 1$.

Writing $S_1 = K[\alpha]$ for $\alpha^n = a \in K^\times$, we have by Proposition 3.4 that $a \in K^{(\nu\varphi^{-1})}$, and when we write $D \otimes_F K = (a,b)_K$ by Corollary 8.6 we have $b \in K^{(\varphi)}$, so that D is a quasi-symbol of type $(\varphi, \nu\varphi^{-1})$. □

In particular, for the case $e = 1$, we have

Corollary 13.4. *Let D be a central simple algebra of degree n over F. If D is split by a Galois extension $S \supset K$ such that $\mathrm{Gal}(S/F) = \mathbb{Z}/d \rtimes_\nu \mathbb{Z}/n$, then D is split by C_n.*

Proof. By the above proposition $\mathrm{res}_{K/F} D = (a,b)$ for $a \in K^{(\nu)}$ and $b \in K^{(1)}$, so we are done by Proposition 11.1. □

Though essentially the same, we can formulate the result more generally for $[K:F] = 2$.

Proposition 13.5. *Let m be an arbitrary odd number, F a field of characteristic prime to m, $\rho \in F_{\mathrm{s}}$ a primitive m-root of unity and $K = F[\rho]$, and assume that $[K:F]$ is prime to m.*

Let D be a division algebra of degree m over F. If D is split by a field $S \supset K$ which is dihedral of dimension $2m$ over F, then D is cyclic.

Proof. The only normal subgroups of the dihedral group

$$D_m = \left\langle \sigma, \tau \,|\, \sigma^m = \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^{-1} \right\rangle$$

are contained in $\langle\sigma\rangle$, so from S being dihedral over F it follows that $[K:F]=2$, $K=S^\sigma$ and S is cyclic over K.

Let $m=n_1\dots n_t$ be the factorization of m into prime power factors. Decompose $S=K_1\otimes_K\dots\otimes_K K_t$ where $[K_i:K]=n_i$, and $D=D_1\otimes_F\dots\otimes_F D_t$ where $\deg D_i=n_i$. The fields K_i are Galois over F, and since $[K:F]=2$, there are only two possibilities for every $i=1,\dots,t$: $\mathrm{Gal}(K_i/F)$ is either the dihedral group of order $2n_i$, or the direct product $\mathbb{Z}/2\times\mathbb{Z}/n_i$. Applying the proposition in the first case and standard arguments in the second, we see that every D_i is cyclic, and (tensoring the cyclic splitting fields over F) D is cyclic as well. □

Our final result on dihedral algebras is to remove the assumption that the splitting field contains roots of unity, made in the last proposition. For that we need to assume that $[K:F]=2$. This theorem is proved in [6, Cor. 30] under the assumption $\mathrm{char}\,F\neq 2$.

Theorem 13.6. *Let n be an odd prime power, $K=F[\rho]$ where ρ is an n-root of unity, and assume $[K:F]\leq 2$. Let D be a central simple algebra of degree n over F.*

If D is split by a dihedral extension of dimension $2n$ over F, then D is cyclic.

Proof. The result was proved under the assumption $K=F$ in [14], so we assume $[K:F]=2$. Let S be the dihedral splitting field. The case $K\subseteq S$ is covered by Proposition 13.5, so we assume S does not contain K.

Let ϖ,σ be generators of the Galois group $\mathrm{Gal}(S/F)$, such that $\varpi^n=\sigma^2=1$ and $\sigma\varpi\sigma^{-1}=\varpi^{-1}$. Let $L=S^\varpi$ be the quadratic subfield, over which S is cyclic. By our assumption K is linearly independent with L, and we let $T=L\otimes_F K=L[\rho]$.

Since $D_1=D\otimes_F L$ is split by S and thus cyclic, Theorem 10.3 shows that

$$D_2=\mathrm{res}_{T/L}D_1=(a,\beta)_T$$

for some $a\in T$ and $\beta\in L$, which is the situation analyzed in Theorem 12.4. In fact (Section 6), letting $\alpha=\sqrt[n]{a}$ we have that $S_1=T[\alpha]$ decomposes as $S_1=S\otimes_L T$. Moreover, letting τ be the non-trivial automorphism of T/L (so that $\tau(\rho)=\rho^{-1}$), we may by Remark 3.5 assume that $\tau(a)=a^{-1}$, and then τ extends to S_1 by $\tau(\alpha)=\alpha^{-1}$. We can also extend ϖ to S_1 by $\varpi(\alpha)=\rho\alpha$, and then $T=S_1^\varpi$.

The main feature of the proof is that to understand D, we first take the restriction to L and from there to T, and then the corestriction to K and down back to F. Indeed, we will apply the computations of Theorem 12.4 to $\mathrm{res}_{T/L}D_1$; from this it will follow that $D^{\otimes 4} \sim \mathrm{cor}_{T/F}\mathrm{res}_{T/L}D_1$ is split by C_n, which proves the claim.

For that we need to know more about a. Since $S_1 = K \otimes_F S$, it is Galois over F (with $\mathrm{Gal}(S_1/F) = D_n \times \mathbb{Z}/2$), and σ is extended to S_1 as the identity on K. Since the relations $\sigma^2 = 1$ and $\varpi\sigma = \sigma\varpi^{-1}$ hold both in K and S, they also hold in S_1. Now let $\alpha' = \sigma(\alpha)$ and note that $\sigma(\alpha') = \alpha$. We have that

$$\varpi(\alpha') = \varpi\sigma(\alpha) = \sigma\varpi^{-1}(\alpha) = \sigma(\rho^{-1}\alpha) = \rho^{-1}\alpha'.$$

It follows that $g = \alpha\alpha' \in S_1^{\sigma,\varpi} = K$, and then $a\sigma(a) = g^n$. Checking that $\tau(\alpha') = \tau\sigma(\alpha) = \sigma\tau(\alpha) = \sigma(\alpha^{-1}) = \alpha'^{-1}$, we see that $\tau(g) = g^{-1}$. Now, consider the element $a_1 = (g^{(n-1)/2}a^{-1})^n a$: since $\tau(a_1) = a_1^{-1}$ and $K[\sqrt[n]{a_1}\,] = K[\sqrt[n]{a}\,]$ we can replace a by a_1; but $\sigma(a_1) = a_1^{-1}$, so from now on we may assume $\sigma(a) = a^{-1}$ and $g = 1$.

Recall that $D_2 = \mathrm{res}_{T/F}D = (a,\beta)_T$. If $\beta \in F$ then

$$\mathrm{cor}_{T/K}D_2 \sim \left(\mathrm{N}_{T/K}a, \beta\right)_K = (1,\beta)_K \sim K,$$

so D is already split. We thus assume $\beta \notin F$, and in particular $T = K[\beta]$. As in Theorem 12.4, let $c, d \in K$ be such that $a = c\beta + d$. We proved in Equation (25) that $\mathrm{N}_{T/K}(a/c) = -1/\mathrm{N}_{K/F}(c)$, and adding the fact that $\mathrm{N}_{T/K}(a) = 1$, we obtain the equality $\tau(c) = -c$. Plugging this in Equation (26), we immediately obtain

$$\mathrm{cor}_{T/K}D_2 \sim (d, 1 - \tau(d)d)_K,$$

and since $1 - \tau(d)d \in F$, we have that $D^{\otimes 4} \sim \mathrm{cor}_{T/F}\mathrm{res}_{T/F}D = \mathrm{cor}_{T/F}D_2 = \mathrm{cor}_{K/F}\mathrm{cor}_{T/K}D_2 = \mathrm{cor}_{K/F}(d, 1-\tau(d)d)_K$ is split by C_n. □

We end this section with a curious property of ${}_n\mathrm{Br}(F)$ when $[K:F] = 6$, which is related to the fact that in the equation

$$3 + 4 \equiv 1 \pmod 6,$$

the common divisor with 6 with each of the summands is greater than 1. Let $F \subseteq L_2, L_3 \subseteq K$ be the intermediate subfields (with $[L_t:F] = t$). Since $[K:L_t] \leq 3$ $(t = 2, 3)$, we have from [8] that ${}_n\mathrm{Br}(L_t)$ is generated by (classes of) cyclic algebras of degree n. Since $\mathrm{cor}_{L_t/F}$ is onto, we immediately get that ${}_n\mathrm{Br}(F)$ is generated by algebras which become cyclic after extending scalars to L_2, and also by algebras which become cyclic after extending scalars to L_3. But in fact ${}_n\mathrm{Br}(F)$ is generated by algebras with a better set of splitting fields:

Proposition 13.7. *Assume that $[K:F]=6$ and let L_2, L_3 be as above. Then ${}_n\mathrm{Br}(F)$ is generated by (the classes of) algebras which are split by both $\mathbb{Z}/2 \rtimes \mathbb{Z}/n$ and $\mathbb{Z}/3 \rtimes \mathbb{Z}/n$.*

Proof. By Lemma 12.1, ${}_n\mathrm{Br}(K)$ is generated by cyclic algebras of the form (a,b) where $a \in K^\times$ and $b \in L_2^\times$. We can decompose $a = a_0 a_1 \dots a_5$ and $b = b_0 b_3$ where $a_i, b_i \in K^{(\nu^i)}$ (see Lemma 6.4). By Proposition 8.3,

$$\mathrm{cor}_{K/F}(a,b) \sim \mathrm{cor}_{K/F}(a_1,b_0) \otimes \mathrm{cor}_{K/F}(a_4,b_3).$$

The algebras $\mathrm{cor}_{K/F}(a_1,b_0)$ are split by C_n, by Proposition 11.1.

By Lemma 6.4 we may assume that $a_4 \in L_3$ and $b_3 \in L_2$, so the same argument works for $\mathrm{res}_{L_t/F}\mathrm{cor}_{K/F}(a_4,b_3)$, and the result follows from Corollary 13.2. □

A similar result holds by the same proof whenever $d = [K:F]$ is divisible by 6: ${}_n\mathrm{Br}(F)$ is generated by algebras which are split by both $\mathbb{Z}/(d/2) \rtimes \mathbb{Z}/n$ and $\mathbb{Z}/(d/3) \rtimes \mathbb{Z}/n$.

14. Generic constructions

In Section 8 we have seen that ${}_n\mathrm{Br}(F)$ is generated by quasi-symbols, which are algebras D_0 such that $D_0 \otimes_F K = (a,b)_K$ for $a \in K^{(\varphi)}$ and $b \in K^{(\varphi')}$, where φ, φ' range over the pairs of characters with product ν. If either $\varphi = 1$ or $\varphi' = 1$, then D_0 is cyclic, and we will assume this is not the case. In this final section we describe a generic construction for quasi-symbols, and present elements w with the property that $\mathrm{Tr}(w^i) = 0$ for most values of i.

According to Theorem 10.3, D_0 is split by C_n iff there are $\alpha \in F^\times$ and $c \in K^{(\nu)}$ of order n, such that $J^\varphi(a) \cup J^{\varphi'}(b) = (\alpha) \cup J^\nu(c)$. It is generally believed that there exist non-cyclic algebras of prime degree $p \geq 5$, though no one was yet able to construct such an algebra. Based on the experience with other types of extensions (e.g. Amitsur's construction of non-crossed products), it seems even more plausible that non-cyclic algebras exist over fields without roots of unity of order p, and the equation given above suggests that a generic quasi-symbol is a reasonable candidate to be non-cyclic.

Let $n = p^m$ be a prime power, and k_0 a field of characteristic prime to n. Let ρ be an n-root of unity in the separable closure $(k_0)_\mathrm{s}$, and $k = k_0[\rho]$. We assume that $d = [k:k_0]$ is prime to n. We then define

$$K = k(a, b, \mu_0, \dots, \mu_{d-2}, \eta_0, \dots, \eta_{d-2}),$$

a transcendental extension of degree at most $2d$ (in some cases there are equations on the μ_i, η_i, which we describe below). Let τ be a generator

of $\mathrm{Gal}(k/k_0)$. The extension of τ to K will depend on our choice of characters. Define $\nu\colon \mathrm{Gal}(k/k_0)\to U_n$ by Equation (8), and let φ,φ' be two characters such that $\varphi\varphi'=\nu$. Let

$$r=\varphi(\tau),\qquad r'=\varphi'(\tau).$$

We extend τ to K by setting

$$\begin{aligned}\tau(a) &= \mu_0^n a^r\\ \tau(b) &= \eta_0^n b^{r'}\\ \tau(\mu_i) &= \mu_{i+1} \pmod d\\ \tau(\eta_i) &= \eta_{i+1} \pmod d,\end{aligned}$$

where μ_{d-1} and η_{d-1} are defined in K by the following formulas:

$$\begin{aligned}\mu_{d-1} &= \mu_{d-2}^{-r}\mu_{d-3}^{-r^2}\cdots\mu_1^{-r^{d-2}}\mu_0^{-r^{d-1}}a^{-\frac{r^d-1}{n}},\\ \eta_{d-1} &= \eta_{d-2}^{-r'}\eta_{d-3}^{-r'^2}\cdots\eta_1^{-r'^{d-2}}\eta_0^{-r'^{d-1}}b^{-\frac{r'^d-1}{n}}.\end{aligned}$$

This definition makes τ an automorphism of order d of K, and $F=K^\tau$ satisfies $F[\rho]=K$.

If the order e of φ is strictly less than n, then we can apply Lemma 6.4 and Proposition 6.5 to simplify K, without losing the generality of the construction. Specifically, if $L=K^{\mathrm{Ker}(\varphi)}$, we can have $a\in L$ and $\mu_0\in L$, so that $\mu_{e+i}=\mu_i$. In particular if $\varphi^2=1$ we choose $r=-1$ and $\mu_i=1$, and then $\tau(a)=a^{-1}$. More generally we can alter the definition so that $\mathrm{N}_{K/F}(a)=1$ (Remark 3.5), which can be used to express μ_{d-2} in terms of $\mu_0,\dots,\mu_{d-3},a$, and similarly η_{d-2} in terms of $\eta_0,\dots,\eta_{d-3},b$. If $d=[K:F]$ is even (and $F\subset K_0\subseteq K$ the intermediate quadratic extension), we can have $\mathrm{N}_{K/K_0}(a)=a\tau^2(a)\dots\tau^{d-2}(a)=1$ by Remark 3.6, and this can be used to express μ_{d-3} in terms of $\mu_0,\dots,\mu_{d-4},a$.

After τ is defined on K, we let

$$D=(a,b)_K=K[x,y|\, x^n=a,\ y^n=b,\ yxy^{-1}=\rho x], \tag{27}$$

and extend τ to D by

$$\tau(x)=\mu_0x^r,\qquad \tau(y)=\eta_0y^{r'}.$$

The generic quasi-symbol $D_0=D^G$ is, according to Lemma 10.2, similar to $\mathrm{cor}_{K/F}(D)$.

Example 14.1. *Consider the case $d=[K:F]=4$ (so in particular $n\equiv 1 \pmod 4$). There are only two options (up to order) for the pair φ,φ': either they are $(1,\nu)$ (in which case the quasi-symbol is surely cyclic), or $\varphi=\nu^2$, $\varphi'=\nu^{-1}$.*

We construct a generic quasi-symbol of type (ν^2,ν^{-1}). Let k,k_0 be as above, $\mathrm{Gal}(k/k_0)=\langle\tau\rangle$, and $t\equiv\nu(\tau) \pmod n$. We then choose

$r = -1$ and $r' = -t$; if $\tau(b) = \eta_0^n b^{-t}$ and $\tau(\eta_0) = \eta_1$ then the condition $b\tau^2(b) = 1$ gives $\eta_1 = \eta_0^t b^{-(t^2+1)/n}$. We thus set

$$K = k(a, b, \eta)$$

and define τ on K by

$$\begin{aligned} \tau(a) &= a^{-1}, \\ \tau(b) &= \eta^n b^{-t}, \\ \tau(\eta) &= \eta^t b^{-(t^2+1)/n}. \end{aligned}$$

Now define $D = (a, b)_K$ by Equation (27), and extend τ to D by $\tau(x) = x^{-1}$, $\tau(y) = \eta y^{-t}$. Notice that $\tau^2(\eta) = \eta^{-1}$ and $\tau^2(y) = y^{-1}$.

The problem we already stated (Question 10.5) is whether or not D^τ is cyclic. By Theorem 11.4, this is equivalent to the existence of $u \in D^\tau$ such that $[F[u]:F] = n$ and $u^n \in F$. Naturally, we view the candidate u as an element of $D \otimes_F K = (a, b)_K$, and multiplying by a central element we can assume u is in the subring of polynomials of K. However, even in this setup, it seems difficult to determine whether or not such an element exits.

We now change perspective, and study some special elements of quasi-symbols. Let w be an element in a central simple algebra. If the characteristic of the field is zero, the coefficients of the minimal polynomial of w are expressed by Newton formulas in terms of the reduced traces $\mathrm{Tr}(w^i)$. In particular, assuming $[F[w]:F] = n$, $w^n \in F$ iff $\mathrm{Tr}(w) = \cdots = \mathrm{Tr}(w^{n-1}) = 0$. One traditional approach to cyclicity problems is to find elements w for which $\mathrm{Tr}(w^i) = 0$ for as many values of i as possible. There is no need to assume roots of unity in the base field: by Theorem 11.4 $D_0 = D^G$ is cyclic over F iff there is $u \in D$ such that $\tau(u) = u$ and $u^n \in K$ (in which case $u^n \in F$). Rowen has shown [12] that in an algebra of odd degree, there always exist an element u such that $\mathrm{Tr}(u) = \mathrm{Tr}(u^2) = 0$. A similar result was obtained by Haile [5]: in any division algebra there exists an element u with $\mathrm{Tr}(u) = \mathrm{Tr}(u^{-1}) = 0$. The technique of power traces was effectively used by Rowen and Saltman [14] to prove their above mentioned result on cyclicity of dihedral algebras. Our computations can be viewed as a partial analog to fields without roots of unity.

From now on, assume $d = [K:F]$ is even, and let $\epsilon = \nu^{d/2}$ denote the character of order 2 in $\mathrm{Gal}(K/F)^\#$. Consider a quasi-symbol D_0 of type $(\epsilon, \nu\epsilon)$. There exist $a \in K^{(\epsilon)}$ and $b \in K^{(\nu\epsilon)}$ such that $\mathrm{res}_{K/F} D_0 = (a, b)$; letting τ be a generator of $\mathrm{Gal}(K/F)$, we set $t = \nu(\tau)$, so that $\tau(a) \equiv a^{-1}$ and $\tau(b) \equiv b^{-t}$.

Let $W = \{\mathrm{tr}_\tau(kxy) : k \in K\}$. This is a subspace of dimension d of D_0 ($\mathrm{tr}_\tau(kxy)$ determines k, which is the coefficient of xy). We will show that powers of elements $w \in W$ often have reduced trace zero. To this end, note that the reduced trace in D_0 is the same as in D, which is easily computed: writing $D = \sum_{i,j=0}^{n-1} Kx^iy^j$, the reduced trace of an element is n times the free coefficient (as the minimal polynomial of kx^iy^j, $(i,j) \neq (0,0)$, is of the form $\lambda^n - c$ for some $c \in K$).

Proposition 14.2. *Let W be as above. Then for every $w \in W$,*

$$\mathrm{Tr}(w) = \mathrm{Tr}(w^3) = \mathrm{Tr}(w^5) = \mathrm{Tr}(w^7) = \cdots = \mathrm{Tr}(w^{n-2}) = 0,$$

and

$$\mathrm{Tr}(w^2) = 0.$$

If, moreover, $\mathrm{char}\, F = 2$*, then* $\mathrm{Tr}(w^\ell) = 0$ *for every* $\ell = 0, \ldots, n-1$.

Proof. Write $D = K[x,y]$ for a standard pair of generators. Let $w = \mathrm{tr}_\tau(kxy) \in \sum_{i=0}^{d-1} Kx^{(-1)^i}y^{s^i}$ where $s = -\nu(\tau)$ and $k \in K$ is arbitrary. For odd $\ell < n$, $w^\ell \in \sum_{i=1,3,\ldots,n-2}(K[y]x^i + K[y]x^{-i})$, so that $\mathrm{Tr}(w^\ell) = 0$.

To see that $\mathrm{Tr}(w^2) = 0$, notice that

$$w^2 \in K[y]x^{-2} + K[y] + K[y]x^2,$$

and the component in $K[y]$ is in $\sum Ky^{s^i+s^j}$ where the sum is over $i = 0, 2, \ldots, d-2$ and $j = 1, 3, \ldots, d-1$. To have non-zero reduced trace there must be a pair i, j such that $s^i + s^j \equiv 0 \pmod{n}$, but then $(-s)^i \equiv (-s)^j$, which is impossible since $(-s)$ is of order d in U_n.

Finally, if $\mathrm{char}\, F = 2$, the claim follows by induction on ℓ from Lemma 14.3 below, whose easy proof was pointed out to me by A. Wadsworth. □

Lemma 14.3. *Let D be a central simple algebra over a field of characteristic 2. The reduced trace satisfies* $\mathrm{Tr}(u^2) = \mathrm{Tr}(u)^2$.

Proof. Extending scalars to the separable closure of F, every element of D is conjugate to an upper triangular matrix, where the reduced trace is the sum of diagonal entries. But if $u_{11}, \ldots, u_{nn}$ is the diagonal of u, the diagonal of u^2 is $u_{11}^2, \ldots, u_{nn}^2$ and $\mathrm{Tr}(u^2) = \sum u_{ii}^2 = (\sum u_{ii})^2 = \mathrm{Tr}(u)^2$. □

The result $\mathrm{Tr}(w^2) = 0$ of the proposition can be significantly improved if $[K:F] = 4$. Note that if $[K:F] = 4$, then ${}_n\mathrm{Br}(F)$ is generated by algebras which are split by C_n, and the quasi-symbols of type $(\epsilon, \nu\epsilon)$.

Proposition 14.4. *Let W be the space defined above, where we assume $d = 4$. Let $\ell \geq 1$ be odd. If $n > \ell^2$, then for every $w \in W$,*

$$\mathrm{Tr}(w^{2\ell}) = 0.$$

Proof. Let τ be a generator of $\mathrm{Gal}(K/F)$ and let t be a number such that $\tau(\rho) = \rho^t$. Since

$$w = \mathrm{tr}_\tau(kxy) \in Kxy + Kx^{-1}y^{-t} + Kxy^{-1} + Kx^{-1}y^t,$$

we have that

$$w^2 \in (Ky^{\pm 2t} + K)x^{-2} + Ky^{\pm 1 \pm t} + (Ky^{\pm 2} + K)x^2.$$

The trace $\mathrm{Tr}(w^{2\ell})$ can be non-zero only if there is a product of ℓ monomials of w^2 which is in K. Let $g_{i,j}$ denote the number of monomials coming from Kx^iy^j in such a product, so that $\sum g_{ij} = \ell$. Let h_i denote the sum of $g_{i,j}$ over all possible values of j. Since the exponent of x in the product is $2(h_2 - h_{-2})$, we have that $h_{-2} = h_2$, and in particular $h_0 = \ell - 2h_2$ is odd.

It then follows that the exponent of y in the product is of the form $d_1t + d_2$, where the only condition on the d_i is that they are odd and $|d_i| \le \ell$. We thus have that $d_1t \equiv -d_2 \pmod{n}$, and since $t^2 \equiv -1$, we obtain $n \mid d_1^2 + d_2^2$, which is even. But n is odd, so $n \mid (d_1^2+d_2^2)/2 \le \ell^2$. □

Example 14.5. *Let D be the algebra of Example 14.1, and let*

$$w = \mathrm{tr}_\tau(kxy) = kxy + \tau(k)\eta x^{-1}y^{-t} + \tau^2(k)xy^{-1} + \tau^3(k)\eta^{-1}x^{-1}y^t.$$

We proved that

$$\mathrm{Tr}(w) = \mathrm{Tr}(w^3) = \mathrm{Tr}(w^5) = \cdots = \mathrm{Tr}(w^{n-2}) = 0$$

and

$$\mathrm{Tr}(w^2) = \mathrm{Tr}(w^6) = \mathrm{Tr}(w^{10}) = \cdots = \mathrm{Tr}(w^{2\ell}) = 0$$

for $\ell \le \sqrt{n}$ odd.

The only way to combine four monomials of w so that the product is in K, is if they are different. Summing all the possible products, we obtain

$$\mathrm{Tr}(w^4) = 4n((\rho + \rho^{-1})(\rho^t + \rho^{-t}) + 2) \cdot \mathrm{N}_{K/F}(k).$$

This coefficient is never zero by the final proposition below, so that $\mathrm{Tr}(w^4) \ne 0$ whenever $w \ne 0$.

Remark 14.6. *A similar computation shows that if $[K:F] = 6$ and $n > 7$, and D_0 is a quasi-symbol of type (ν^3, ν^4), then for every $w \in W$,*

$$\mathrm{Tr}(w^4) = 0.$$

We end this paper with a bit of trigonometry (which is needed for Example 14.5).

Proposition 14.7. *Let n be an odd prime power and t an integer such that $t^2 \equiv -1 \pmod{n}$, and let ρ be an n-root of unity. Then*

$$(\rho + \rho^{-1})(\rho^t + \rho^{-t}) + 2 \ne 0.$$

Proof. Let $\theta_1 = \frac{2(t-1)\pi}{n}$ and $\theta_2 = \frac{2(t+1)\pi}{n}$. Since $(\rho+\rho^{-1})(\rho^t+\rho^{-t}) = \rho^{t+1}+\rho^{t-1}+\rho^{1-t}+\rho^{-1-t} = 2\cos\theta_1 + 2\cos\theta_2$, we need to show that $\cos\theta_1+\cos\theta_2 \neq -1$. Otherwise, the average of $\cos\theta_1, \cos\theta_2$ is $-1/2$, so for some $\{i,j\} = \{1,2\}$ we have $-1/2 \leq \cos\theta_i \leq 0$ and $\cos\theta_j \leq -1/2$; in other words

$$\theta_i \in [\pi/2, 2\pi/3] \cup [4\pi/3, 3\pi/2],$$

$$\theta_j \in [2\pi/3, 4\pi/3].$$

First assume $j < i$. Then since $\theta_1 < \theta_2$ we have $4\pi/3 \leq \theta_2$, and (changing t to $n-t$ if necessary) $\theta_1 < \pi$. It follows that $4\pi/n = \theta_2 - \theta_1 > 4\pi/3 - \pi = \pi/3$, so $n < 12$ and $n \in \{5, 9\}$.

Now assume $i < j$: again since $\theta_1 < \theta_2$, we have that $\theta_1 \leq 2\pi/3 < \theta_2$, so substituting we obtain $n - 3 < 3t \leq n + 3$. Writing $n = 3p + u$ for $u = 0, 1, 2$, we get $t \in \{p, p+1\}$. Recall that by assumption $n \mid t^2+1$. If $t = p$, then $n \mid 9(t^2+1) - n(3p-u) = 9+u^2$; otherwise $t = p+1$, and $n \mid 9(t^2+1) - (3p+6-u)n = 9+(3-u)^2$. In both cases $n \in \{5, 9, 13\}$.

A direct computation now excludes the few possible values of (n, t). Note that for $n = 5$, $(\rho+\rho^{-1})(\rho^2+\rho^{-2}) = -1$. □

References

[1] A.A. Albert, Modern Higher Algebra, Chicago Univ. Press, 1937.

[2] A.A. Albert, Structure of Algebras, Amer. Math. Soc. Coll. Publ., Vol. XXIV, Providence.1961

[3] A.A. Albert, *Non-cyclic algebras with pure maximal subfields*, A. M. S. Bull. **44**, 576–579, (1938).

[4] N. Elkayam, Central simple algebras with involution of the second kind, MSc thesis, Bar-Ilan University, Israel, 2001.

[5] D.E. Haile, *A useful proposition for division algebras of small degree*, Proc. Amer. Math. Soc. **106**(2), 317–319, (1989).

[6] D.E. Haile, M.-A. Knus, M. Rost, and J.-P. Tignol, *Algebras of odd degree with involution, trace forms and dihedral extensions*, Israel J. Math. **96** B, 299–340, (1996).

[7] N. Jacobson, Finite Dimensional Division Algebras Over Fields, Springer, 1996.

[8] A.S. Merkurjev, *Brauer groups of fields*, Comm. Alg. **11**(22), 2611-2624, (1983).

[9] A.S. Merkurjev, *On the structure of the Brauer group of fields*, Math. USSR. Izvestya **27**(1), 141–157, (1986).

[10] S. Rosset and J. Tate, *A reciprocity law for* K_2*-traces*, Comment. Math. Helvetici **58**, 38–47, (1983).

[11] L.H. Rowen, Ring Theory, Volume II, Academic Press, 1988.

[12] L.H. Rowen, *Brauer factor sets and simple algebras*, Trans. Amer. Math. Soc. **282**(2), 765–772, (1984).

[13] L.H. Rowen and D.J. Saltman, *Semidirect product division algebras*, Isr. J. Math. **96**, 527–551, (1996).

[14] L.H. Rowen and D.J. Saltman, *Dihedral algebras are cyclic*, Proc. Amer. Math. Soc. **84**(2), 162–164, (1982).

[15] L.H. Rowen and J.-P. Tignol, *On the decomposition of cyclic algebras*, Israel J. Math. **96**, 553–578, (1996).
[16] D.J. Saltman, *Generic galois extensions and problems in field theory*, Advances Math. **43**(3), 250–282, (1982).
[17] V. Srinivas, Algebraic K_2-Theory, Progress in Math. **90**, Birkhauser, 1991.
[18] J.-P. Tignol and S.A. Amitsur, *Kummer subfields of Malcev-Neumann division algebras*, Israel J. Math **50**, 114–144, (1985).
[19] B. Kahn, J. Minác and A. Wadsworth, *The first two cohomology groups of some Galois extensions*, preprint, (2002).

Department of Mathematics, Yale University, 10 Hillhouse Avenue, New-Haven CT 06520, USA
E-mail address: uv2@math.yale.edu