



The Schur group of an abelian number field

Allen Herman^a, Gabriela Olteanu^{b,c}, Ángel del Río^{d,*}

^a Department of Mathematics, University of Regina, Regina, Canada

^b Department of Mathematics and Computer Science, North University of Baia Mare, Victoriei 76, 430122 Baia Mare, Romania

^c Faculty of Mathematics and Computer Science, Babeş-Bolyai University, M. Kogalniceanu 1, 400084 Cluj-Napoca, Romania

^d Departamento de Matemáticas, Universidad de Murcia, 30100 Murcia, Spain

ARTICLE INFO

Article history:

Received 23 November 2007

Received in revised form 16 March 2008

Available online 2 July 2008

Communicated by C. Kassel

MSC:

Primary: 20C05

secondary: 12A60

16A26

16S35

ABSTRACT

We characterize the maximum r -local index of a Schur algebra over an abelian number field K in terms of global information determined by the field K for an arbitrary rational prime, r . This completes and unifies previous results of Janusz in [G.J. Janusz, The Schur group of an algebraic number field, *Ann. of Math. (2)* 103 (1976) 253–281] and Pendergrass in [J.W. Pendergrass, The 2-part of the Schur group, *J. Algebra* 41 (1976) 422–438].

© 2008 Elsevier B.V. All rights reserved.

1. Introduction and preliminaries

Let K be a field. A *Schur algebra* over K is a central simple K -algebra which is generated over K by a finite group of units. The *Schur group* of K is the subgroup $S(K)$ of the Brauer group of K formed by classes containing a Schur algebra. By the Brauer–Witt theorem (see e.g. [8]), each class in $S(K)$ can be represented by a cyclotomic algebra, i.e. a crossed product of the form $(L/K, \alpha)$ in which L/K is a cyclotomic extension and the factor set α takes values in the group of roots of unity $W(L)$ of L .

In the case when K is an abelian number field, i.e. K is contained in a finite cyclotomic extension of \mathbb{Q} , Benard–Schacher theory [2] gives a partial characterization of the elements of $S(K)$. According to this theory, if n is the Schur index of a Schur algebra over K , then $W(K)$ contains an element of order n . This is known as the Benard–Schacher theorem. Furthermore, if $\frac{L}{K}$ (in lowest terms) is the local invariant of A at a prime \mathcal{R} of K that lies over a rational prime r , then each of the fractions $\frac{L}{K}$ with $1 \leq c \leq n$ and c coprime to n will occur equally often among the local invariants corresponding to the primes of K lying above r . In particular, these local invariants all have the same denominator n for all the primes of K lying above r , which we call the r -local index $m_r(A)$ of A . Only finitely many of the $m_r(A)$ are greater than 1, and the Schur index of A is the least common multiple of the $m_r(A)$ as r runs over all rational primes.

The goal of this article is to characterize the maximum r -local index of a Schur algebra over an abelian number field K in terms of global information determined by K . The existence of this maximum is a consequence of the Benard–Schacher Theorem. Since $S(K)$ is a torsion abelian group, it is enough to compute the maximum of the r -local indices of Schur algebras over K with index a power of p for every prime p dividing the order of $W(K)$. We will refer to this number as $p^{\beta_p(r)}$. In [3], Janusz gave a formula for $p^{\beta_p(r)}$ when either p is odd or K contains a primitive 4-th root of unity. The remaining cases were considered by Pendergrass in [5]. However, some of the calculations involving factor sets in [5] are not correct, and as a

* Corresponding author. Tel.: +34 968 36 35 37; fax: +34 968 36 41 82.

E-mail addresses: aherman@math.uregina.ca (A. Herman), olteanu@math.ubbcluj.ro, golteanu@um.es (G. Olteanu), adelrio@um.es (Á. del Río).

consequence the formulas for $2^{\beta_2(r)}$ for odd primes r that appear there are inaccurate. This article was motivated in part by the need to find a correct formula for $p^{\beta_p(r)}$ in this remaining case, and also because of the need to apply the formula in an upcoming work of the authors in [4], where the gap between the Schur subgroup of an abelian number field and its subgroup generated by classes containing cyclic cyclotomic algebras is studied. Since the local index at ∞ will be 2 when K is real and will be 1 otherwise, the only remaining case is that of $r = 2$. In this case, p must be equal to 2 and we must have $\zeta_4 \notin K$. The characterization of fields K for which $S(K_2)$ is of order 2 is given in [5, Corollary 3.3].

The main result of the paper (Theorem 13) characterizes $p^{\beta_p(r)}$ in terms of the position of K relative to an overlying cyclotomic extension F that is determined by K and p . The formulas for $p^{\beta_p(r)}$ are stated in terms of elements of certain Galois groups in this setting. The main difference between our approach and that of Janusz and Pendergrass is that the field F that we use is slightly larger, which allows us to present some of the somewhat artificial-looking calculations in [3] in a more conceptual fashion. Another highlight of our approach is the treatment of calculations involving factor sets. In Section 2 we generalize a result from [1] which describes the factor sets for a given action of an abelian group G on another abelian group W in terms of some data. In particular, we give necessary and sufficient conditions that the data must satisfy in order to be induced by a factor set. Because of the applications we have in mind, extra attention is paid to the case when W is a cyclic p -group.

2. Factor set calculations

In this section W and G are two abelian groups and $\Upsilon : G \rightarrow \text{Aut}(W)$ is a group homomorphism. A group epimorphism $\pi : \bar{G} \rightarrow G$ with kernel W is said to induce Υ if, given $u_g \in \bar{G}$ such that $\pi(u_g) = g$, one has $u_g w u_g^{-1} = \Upsilon(g)(w)$ for each $w \in W$. If $g \mapsto u_g$ is a crossed section of π (i.e. $\pi(u_g) = g$ for each $g \in G$) then the map $\alpha : G \times G \rightarrow W$ defined by $u_g u_h = \alpha_{g,h} u_{gh}$ is a factor set (or 2-cocycle) $\alpha \in Z^2(G, W)$. We always assume that the crossed sections are normalized, i.e. $u_1 = 1$ and hence $\alpha_{g,1} = \alpha_{1,g} = 1$. Since a different choice of crossed section for π would be a map $g \mapsto w_g u_g$ where $w : G \rightarrow W$, π determines a unique cohomology class in $H^2(G, W)$, namely the one represented by α .

Given a list g_1, \dots, g_n of generating elements of G , a group epimorphism $\pi : \bar{G} \rightarrow G$ inducing Υ , and a crossed section $g \mapsto u_g$ of π , we associate the elements β_{ij} and γ_i of W , for $i, j \leq n$, by the equalities:

$$u_{g_j} u_{g_i} = \beta_{ij} u_{g_i} u_{g_j}, \quad \text{and} \quad u_{g_i}^{q_i} = \gamma_i u_{g_1}^{t_1^{(i)}} \cdots u_{g_{i-1}}^{t_{i-1}^{(i)}}, \tag{1}$$

where the integers q_i and $t_j^{(i)}$ for $1 \leq i \leq n$ and $0 \leq j < i$ are determined by

$$q_i = \text{order of } g_i \text{ modulo } \langle g_1, \dots, g_{i-1} \rangle, \quad g_i^{q_i} = g_1^{t_1^{(i)}} \cdots g_{i-1}^{t_{i-1}^{(i)}}, \quad \text{and} \quad 0 \leq t_j^{(i)} < q_j. \tag{2}$$

If α is the factor set associated to π and the crossed section $g \mapsto u_g$, then we say that α induces the data (β_{ij}, γ_i) . The following proposition gives necessary and sufficient conditions for a list (β_{ij}, γ_i) of elements of W to be induced by a factor set.

The order of an element g of a group is denoted by $|g|$.

Proposition 1. *Let W and $G = \langle g_1, \dots, g_n \rangle$ be abelian groups and let $\Upsilon : G \rightarrow \text{Aut}(W)$ be an action of G on W . For every $1 \leq i, j \leq n$, let q_i and $t_j^{(i)}$ be the integers determined by (2). For every $w \in W$ and $1 \leq i \leq n$, let*

$$\Upsilon_i = \Upsilon(g_i), \quad N_i^t(w) = w \Upsilon_i(w) \Upsilon_i^2(w) \cdots \Upsilon_i^{t-1}(w), \quad \text{and} \quad N_i = N_i^{q_i}.$$

For every $1 \leq i, j \leq n$, let β_{ij} and γ_i be elements of W . Then the following conditions are equivalent:

- (1) There is a factor set $\alpha \in Z^2(G, W)$ inducing the data (β_{ij}, γ_i) .
- (2) The following equalities hold for every $1 \leq i, j, k \leq n$:

(C1) $\beta_{ii} = \beta_{ij} \beta_{ji} = 1$.

(C2) $\beta_{ij} \beta_{jk} \beta_{ki} = \Upsilon_k(\beta_{ij}) \Upsilon_i(\beta_{jk}) \Upsilon_j(\beta_{ki})$.

(C3) $N_i(\beta_{ij}) \gamma_i = \Upsilon_j(\gamma_i) N_1^{t_1^{(i)}}(\beta_{ij}) \Upsilon_1^{t_1^{(i)}}(N_2^{t_2^{(i)}}(\beta_{2j})) \cdots \Upsilon_1^{t_1^{(i)}} \Upsilon_2^{t_2^{(i)}} \cdots \Upsilon_{i-2}^{t_{i-2}^{(i)}}(N_{i-1}^{t_{i-1}^{(i)}}(\beta_{(i-1)j}))$.

Proof. (1) implies (2). Assume that there is a factor set $\alpha \in Z^2(G, W)$ inducing the data (β_{ij}, γ_i) . Then there is a surjective homomorphism $\pi : \bar{G} \rightarrow G$ and a crossed section $g \mapsto u_g$ of π such that the β_{ij} and γ_i satisfy (1). Condition (C1) is clear. Conjugating by u_{g_k} in $u_{g_j} u_{g_i} = \beta_{ij} u_{g_i} u_{g_j}$ yields

$$\begin{aligned} \beta_{jk} \Upsilon_j(\beta_{ik}) \beta_{ij} u_{g_i} u_{g_j} &= \beta_{jk} \Upsilon_j(\beta_{ik}) u_{g_j} u_{g_i} = \beta_{jk} u_{g_j} \beta_{ik} u_{g_i} = u_{g_k} u_{g_j} u_{g_i} u_{g_k}^{-1} \\ &= u_{g_k} \beta_{ij} u_{g_i} u_{g_j} u_{g_k}^{-1} = \Upsilon_k(\beta_{ij}) \beta_{ik} u_{g_i} \beta_{jk} u_{g_j} = \Upsilon_k(\beta_{ij}) \beta_{ik} \Upsilon_i(\beta_{jk}) u_{g_i} u_{g_j}. \end{aligned}$$

Therefore, we have $\beta_{jk} \Upsilon_j(\beta_{ik}) \beta_{ij} = \Upsilon_k(\beta_{ij}) \beta_{ik} \Upsilon_i(\beta_{jk})$ and so (C2) follows from (C1).

To prove (C3), we use the obvious relation $(wu_{g_i})^t = N_i^t(w)u_{g_i}^t$. Conjugating by u_{g_j} in $u_{g_i}^{q_i} = \gamma_1 u_{g_1}^{t_1^{(i)}} \cdots u_{g_{i-1}}^{t_{i-1}^{(i)}}$ results in

$$\begin{aligned} N_i(\beta_{ij})\gamma_1 u_{g_1}^{t_1^{(i)}} \cdots u_{g_{i-1}}^{t_{i-1}^{(i)}} &= N_i^{q_i}(\beta_{ij})u_{g_i}^{q_i} = (\beta_{ij}u_{g_i})^{q_i} = u_{g_j}u_{g_i}^{q_i}u_{g_j}^{-1} = u_{g_j}\gamma_1 u_{g_1}^{t_1^{(i)}} \cdots u_{g_{i-1}}^{t_{i-1}^{(i)}}u_{g_j}^{-1} \\ &= \Upsilon_j(\gamma_1)(\beta_{1j}u_{g_1})^{t_1^{(i)}} \cdots (\beta_{(i-1)j}u_{g_{i-1}})^{t_{i-1}^{(i)}} = \Upsilon_j(\gamma_1)N_1^{t_1^{(i)}}(\beta_{1j})u_{g_1}^{t_1^{(i)}} \cdots N_{i-1}^{t_{i-1}^{(i)}}(\beta_{(i-1)j})u_{g_{i-1}}^{t_{i-1}^{(i)}} \\ &= \Upsilon_j(\gamma_1)N_1^{t_1^{(i)}}(\beta_{1j})\Upsilon_1^{t_1^{(i)}}(N_2^{t_2^{(i)}}(\beta_{2j})) \cdots \Upsilon_1^{t_1^{(i)}}\Upsilon_2^{t_2^{(i)}} \cdots \Upsilon_{i-2}^{t_{i-2}^{(i)}}(N_{i-1}^{t_{i-1}^{(i)}}(\beta_{(i-1)j}))u_{g_1}^{t_1^{(i)}} \cdots u_{g_{i-1}}^{t_{i-1}^{(i)}}. \end{aligned}$$

Cancelling on both sides produces (C3). This finishes the proof of (1) implies (2).

Before proving (2) implies (1), we show that if $\pi : \bar{G} \rightarrow G$ is a group homomorphism with kernel W inducing $\Upsilon, g \mapsto u_g$ is a crossed section of π and β_{ij} and γ_i are given by (1), then \bar{G} is isomorphic to the group \widehat{G} given by the following presentation: the set of generators of \widehat{G} is $\{\widehat{w}, \widehat{g}_i : w \in W, i = 1, \dots, n\}$, and the relations are

$$\widehat{w_1 w_2} = \widehat{w_1} \widehat{w_2}, \quad \Upsilon_i(w) = \widehat{g}_i \widehat{w} \widehat{g}_i^{-1}, \quad \widehat{g}_j \widehat{g}_i = \widehat{\beta}_{ij} \widehat{g}_i \widehat{g}_j \quad \text{and} \quad \widehat{g}_i^{q_i} = \widehat{\gamma}_1 \widehat{g}_1^{t_1^{(i)}} \cdots \widehat{g}_{i-1}^{t_{i-1}^{(i)}}, \tag{3}$$

for each $1 \leq i, j \leq n$ and $w, w_1, w_2 \in W$. Since the relations obtained by replacing \widehat{w} by w and \widehat{g}_i by u_{g_i} in Eq. (3) for each $x \in W$ and each $1 \leq i \leq n$, hold in \bar{G} , there is a surjective group homomorphism $\phi : \widehat{G} \rightarrow \bar{G}$, which associates \widehat{w} with w , for every $w \in W$, and \widehat{g}_i with u_{g_i} , for every $i = 1, \dots, n$. Moreover, ϕ restricts to an isomorphism $\widehat{W} \rightarrow W$ and $|\widehat{g}_i(\widehat{W}, \widehat{g}_1, \dots, \widehat{g}_{i-1})| = q_i$. Hence $|\widehat{G} : \widehat{W}| = q_1 \cdots q_n = |\bar{G} : W|$ and so $|\widehat{G}| = |\bar{G}|$. We conclude that ϕ is an isomorphism.

(2) implies (1). Assume that the β_{ij} 's and γ_i 's satisfy conditions (C1), (C2) and (C3). We will recursively construct groups $\bar{G}_0, \bar{G}_1, \dots, \bar{G}_n$. Start with $\bar{G}_0 = W$. Assume that $\bar{G}_{k-1} = \langle W, u_{g_1}, \dots, u_{g_{k-1}} \rangle$ has been constructed with $u_{g_1}, \dots, u_{g_{k-1}}$ satisfying the last three relations of (3), for $1 \leq i, j < k$, and that these relations, together with the relations in W , form a complete list of relations for \bar{G}_{k-1} . To define \bar{G}_k we first construct a semidirect product $H_k = \bar{G}_{k-1} \rtimes_{c_k} \langle x_k \rangle$, where c_k acts on \bar{G}_{k-1} by

$$c_k(w) = \Upsilon_k(w), \quad (w \in W), \quad c_k(u_{g_i}) = \beta_{ik}u_{g_i}.$$

In order to check that this defines an automorphism of \bar{G}_{k-1} we need to check that c_k respects the defining relations of \bar{G}_{k-1} . This follows from the commutativity of G and conditions (C1), (C2) and (C3) by straightforward calculations which we leave to the reader.

Notice that the defining relations of H_k are the defining relations of \bar{G}_{k-1} and the relations $x_k w = \Upsilon_k(w)x_k$ and $x_k u_{g_i} = \beta_{ik}u_{g_i}x_k$. Using (C3) one deduces $u_{g_i}x_k^{q_k}u_{g_i}^{-1} = u_{g_i}\gamma_k u_{g_1}^{t_1^{(k)}} \cdots u_{g_{k-1}}^{t_{k-1}^{(k)}}u_{g_i}^{-1}$, for each $i \leq k-1$. This shows that $y_k = x_k^{-q_k}\gamma_k u_{g_1}^{t_1^{(k)}} \cdots u_{g_{k-1}}^{t_{k-1}^{(k)}}$ belongs to the center of H_k . Let $\bar{G}_k = H_k / \langle y_k \rangle$ and $u_{g_k} = x_k \langle y_k \rangle$. Now it is easy to see that the defining relations of \bar{G}_k are the relations of W and the last three relations in (3), for $0 \leq i, j \leq k$.

It is clear now that the assignment $w \mapsto 1$ and $u_{g_i} \mapsto g_i$ for each $i = 1, \dots, n$ defines a group homomorphism $\pi : \bar{G} = \bar{G}_n \rightarrow G$ with kernel W and inducing Υ . If α is the factor set associated to π and the crossed section $g \mapsto u_g$, then (β_{ij}, γ_i) is the list of data induced by α . \square

Note that the group generated by the values of the factor set α coincides with the group generated by the data (β_{ij}, γ_i) . This observation will be used in the next section.

In the case $G = \langle g_1 \rangle \times \cdots \times \langle g_n \rangle$ we obtain the following corollary that one should compare with Theorem 1.3 of [1].

Corollary 2. *If $G = \langle g_1 \rangle \times \cdots \times \langle g_n \rangle$ then a list $D = (\beta_{ij}, \gamma_i)_{1 \leq i, j \leq n}$ of elements of W is the list of data associated to a factor set in $Z^2(G, W)$ if and only if the elements of D satisfy (C1), (C2) and $N_i(\beta_{ij})\gamma_i = \Upsilon_j(\gamma_j)$, for every $1 \leq i, j \leq n$.*

In the remainder of this section we assume that $W = \langle \zeta \rangle$ is a cyclic p -group, for p a prime integer. Let p^a and p^{a+b} denote the orders of $W^G = \{x \in W : \Upsilon(g)(x) = x \text{ for each } g \in G\}$ and W , respectively. We assume that $0 < a, b$. We also set

$$C = \text{Ker}(\Upsilon) \quad \text{and} \quad D = \{g \in G : \Upsilon(g)(\zeta) = \zeta \text{ or } \Upsilon(g)(\zeta) = \zeta^{-1}\}.$$

Note that D is subgroup of G containing C , G/D is cyclic, and $[D : C] \leq 2$. Furthermore, the assumption $a > 0$ implies that if $C \neq D$ then $p^a = 2$.

Lemma 3. *There exists a $\rho \in D$ and a subgroup B of C such that $D = \langle \rho \rangle \times B$ and $C = \langle \rho^2 \rangle \times B$.*

Proof. The lemma is obvious if $C = D$ (just take $\rho = 1$). So assume that $C \neq D$ and temporarily take ρ to be any element of $D \setminus C$. Since $[D : C] = 2$, one may assume without loss of generality that $|\rho|$ is a power of 2. Write $C = C_2 \times C_{2'}$, where C_2 and $C_{2'}$ denote the 2-primary and 2'-primary parts of C , and choose a decomposition $C_2 = \langle c_1 \rangle \times \cdots \times \langle c_n \rangle$ of C_2 . By reordering the c_i 's if needed, one may assume that $\rho^2 = c_1^{a_1} \cdots c_k^{a_k} c_{k+1}^{2c_{k+1}} \cdots c_n^{2a_n}$ with a_1, \dots, a_k odd. Then replacing ρ by $\rho c_{k+1}^{-a_{k+1}} \cdots c_n^{-a_n}$ one may assume that $\rho^2 = c_1^{a_1} \cdots c_k^{a_k}$, with a_1, \dots, a_k odd. Let $H = \langle \rho, c_1, \dots, c_k \rangle$. Then $|\rho|/2 = |\rho^2| = \exp(H \cap C)$,

the exponent of $H \cap C$, and so ρ is an element of maximal order in H . This implies that $H = \langle \rho \rangle \times H_1$ for some $H_1 \leq H$. Moreover, if $h \in H_1 \setminus C$ then $1 \neq \rho^{|\rho|/2} = h^{|\rho|/2} \in \langle \rho \rangle \cap H_1$, a contradiction. This shows that $H_1 \subseteq C$. Thus $C_2 = (H \cap C_2) \times \langle c_{k+1} \rangle \times \cdots \times \langle c_n \rangle = \langle \rho^2 \rangle \times H_1 \times \langle c_{k+1} \rangle \times \cdots \times \langle c_n \rangle$. Then ρ and $B = H_1 \times \langle c_{k+1} \rangle \times \cdots \times \langle c_n \rangle \times C_2$ satisfy the required conditions. \square

By Lemma 3, there is a decomposition $D = B \times \langle \rho \rangle$ with $C = B \times \langle \rho^2 \rangle$, which will be fixed for the remainder of this section. Moreover, if $C = D$ then we assume $\rho = 1$. Since G/D is cyclic, $G/C = \langle \rho C \rangle \times \langle \sigma C \rangle$ for some $\sigma \in G$. It is easy to see that σ can be selected so that if $D = G$ then $\sigma = 1$, and $\sigma(\zeta) = \zeta^c$ for some integer c satisfying

$$v_p(c^{q_\sigma} - 1) = a + b, \quad \text{and} \quad v_p(c - 1) = \begin{cases} a & \text{if } G/C \text{ is cyclic and } G \neq D, \\ a + b & \text{if } G/C \text{ is cyclic and } G = D, \text{ and} \\ d \geq 2 & \text{for some integer } d, \text{ if } G/C \text{ is not cyclic,} \end{cases} \tag{4}$$

where $q_\sigma = |\sigma C|$ and the map $v_p : \mathbb{Q} \rightarrow \mathbb{Z}$ is the classical p -adic valuation. In particular, if G/C is non-cyclic (equivalently $C \neq D \neq G$) then $p^a = 2, b \geq 2, \rho(\zeta) = \zeta^{-1}$ and $\sigma(\zeta^{2^{b-1}}) = \zeta^{2^{b-1}}$.

For every positive integer t we set

$$V(t) = 1 + c + c^2 + \cdots + c^{t-1} = \frac{c^t - 1}{c - 1}.$$

Now we choose a decomposition $B = \langle c_1 \rangle \times \cdots \times \langle c_n \rangle$ and adapt the notation of Proposition 1 for a group epimorphism $f : \bar{G} \rightarrow G$ with kernel W inducing γ and elements $u_{c_1}, \dots, u_{c_n}, u_\sigma, u_\rho \in \bar{G}$ with $f(u_{c_i}) = c_i, f(u_\rho) = \rho$ and $f(u_\sigma) = \sigma$, by setting

$$\beta_{ij} = [u_{c_j}, u_{c_i}], \quad \beta_{i\rho} = \beta_{\rho i}^{-1} = [u_\rho, u_{c_i}], \quad \beta_{i\sigma} = \beta_{\sigma i}^{-1} = [u_\sigma, u_{c_i}], \quad \text{and} \quad \beta_{\sigma\rho} = \beta_{\rho\sigma}^{-1} = [\beta_\rho, \beta_\sigma].$$

We also set

$$q_i = |c_i|, \quad q_\rho = |\rho|, \quad \text{and} \quad \sigma^{q_\sigma} = c_1^{t_1} \cdots c_n^{t_n} \rho^{2t_\rho}, \quad \text{where } 0 \leq t_i < q_i \text{ and } 0 \leq t_\rho < |\rho^2|. \tag{5}$$

With a slightly different notation than in Proposition 1, we have, for each $1 \leq i \leq n, t_j^{(i)} = 0$ for each $0 \leq j < i, t_i^{(\rho)} = 0, t_i^{(\sigma)} = t_i$, and $t_\rho^{(\sigma)} = 2t_\rho$. Furthermore, $q_\rho = 1$ if $C = D$ and q_ρ is even if $C \neq D$. Continuing with the adaptation of the notation of Proposition 1 we set

$$\gamma_i = u_{c_i}^{q_i}, \quad \gamma_\rho = u_\rho^{q_\rho}, \quad \text{and} \quad \gamma_\sigma = u_\sigma^{q_\sigma} u_{c_1}^{-t_1} \cdots u_{c_n}^{-t_n} u_\rho^{2t_\rho}.$$

We refer to the list $\{\beta_{ij}, \beta_{i\sigma}, \beta_{i\rho}, \beta_{\sigma\rho}, \gamma_i, \gamma_\rho, \gamma_\sigma : 0 \leq i < j \leq n\}$, which we abbreviate as (β, γ) , as the data associated to the group epimorphism $f : \bar{G} \rightarrow G$ and choice of crossed section $u_{c_1}, \dots, u_{c_n}, u_\sigma, u_\rho$, or as the data induced by the corresponding factor set in $Z^2(G, W)$.

Furthermore, for every $w \in W, 1 \leq i \leq n$ and $t \geq 0$ one has

$$N_i^t(w) = w^t, \quad N_\sigma^t(w) = w^{V(t)} \quad \text{and} \quad N_\rho^t(w) = \begin{cases} w^t, & \text{if } \rho = 1; \\ 1, & \text{if } \rho \neq 1 \text{ and } t \text{ is even;} \\ w, & \text{if } \rho \neq 1 \text{ and } t \text{ is odd.} \end{cases}$$

In particular, for every $w \in W$ one has

$$N_i(w) = w^{q_i}, \quad N_\sigma(w) = w^{V(q_\sigma)}, \quad \text{and} \quad N_\rho(w) = 1.$$

Rewriting Proposition 1 for this case we obtain the following.

Corollary 4. *Let W be a finite cyclic p -group and let G be an abelian group acting on W with $G = \langle c_1, \dots, c_n, \sigma, \rho \rangle, B = \langle c_1 \rangle \times \cdots \times \langle c_n \rangle, D = B \times \langle \rho \rangle$ and $C = B \times \langle \rho^2 \rangle$ as above. Let q_i, q_ρ, q_σ and the t_i 's be given by (5). Let $\beta_{\sigma\rho}, \gamma_\rho, \gamma_\sigma \in W$ and for every $1 \leq i, j \leq n$ let $\beta_{ij}, \beta_{i\sigma}, \beta_{i\rho}$ and γ_i be elements of W . Then the following conditions are equivalent:*

(1) *The given collection $(\beta, \gamma) = \{\beta_{ij}, \gamma_i, \beta_{i\sigma}, \gamma_\sigma, \gamma_\rho, \beta_{\sigma\rho}\}$ is the list of data induced by some factor set in $Z^2(G, W)$.*

(2) *The following equalities hold for every $1 \leq i, j \leq n$:*

(C1) $\beta_{ii} = \beta_{ij}\beta_{ji} = 1.$

(C2) (a) $\beta_{ij} \in W^G.$

(b) *If $\rho \neq 1$ then $\beta_{i\sigma}^2 = \beta_{i\rho}^{1-c}.$*

(C3) (a) $\beta_{ij}^{q_i} = 1.$

(b) $\beta_{i\sigma}^{q_i} = \gamma_i^{c-1}.$

(c) $\beta_{i\sigma}^{-V(q_\sigma)} = \beta_{1i}^{t_1} \cdots \beta_{ni}^{t_n}.$

(d) $\gamma_\sigma^{c-1} \beta_{1\sigma}^{t_1} \cdots \beta_{n\sigma}^{t_n} = 1.$

(e) *If $\rho = 1$ then $\beta_{i\rho} = \beta_{\sigma\rho} = \gamma_\rho = 1.$*

(f) *If $\rho \neq 1$ then $\beta_{i\rho}^{q_i} \gamma_i^2 = 1, \beta_{\sigma\rho}^{V(q_\sigma)} \gamma_\sigma^2 = \beta_{1\rho}^{t_1} \cdots \beta_{n\rho}^{t_n}$ and $\gamma_\rho \in W^G.$*

Proof. By completing the data with $\beta_{\sigma i} = \beta_{i\sigma}^{-1}$, $\beta_{\rho i} = \beta_{i\rho}^{-1}$ and $\beta_{\sigma\sigma} = \beta_{\rho\rho} = 1$ we have that (C1) is a rewriting of condition (C1) from Proposition 1.

(C2) is the rewriting of condition (C2) from Proposition 1 because this condition vanishes when $1 \leq i, j, k \leq n$ and when two of the elements i, j, k are equal. Furthermore, permuting i, j, k in (C2) yields equivalent conditions. So we only have to consider three cases: substituting $i = i, j = j$, and $k = \sigma$; $i = i, j = j$, and $k = \rho$; and $i = i, j = \rho$, and $k = \sigma$. In the first two cases one obtains $\sigma(\beta_{ij}) = \rho(\beta_{ij}) = \beta_{ij}$, or equivalently $\beta_{ij} \in W^G$. For $\rho = 1$ the last case vanishes, and for $\rho \neq 1$ (C2) yields $\beta_{i\sigma}^2 = \beta_{i\rho}^{1-c}$.

Rewriting (C3) from Proposition 1 we obtain: (a) for $i = i, j = j$; (b) for $i = i$ and $j = \sigma$; (c) for $i = \sigma$ and $j = i$; and (d) for $i = \sigma$ and $j = \sigma$.

We consider separately the cases $\rho = 1$ and $\rho \neq 1$ for the remaining cases for rewriting (C3). Assume first that $\rho = 1$. When i is replaced by ρ and j replaced by i (respectively, by σ) we obtain $\beta_{i\rho} = 1$ (respectively $\beta_{\sigma\rho} = 1$). On the other hand the requirement of only using normalized crossed sections implies $\gamma_\rho = 1$ in this case. When $j = \rho$ the conditions obtained are trivial.

Now assume that $\rho \neq 1$. For $i = i$ and $j = \rho$ one obtains $\beta_{i\rho}^{q_i} \gamma_i^2 = 1$. For $i = \rho$ and $j = i$ one obtains a trivial condition because $N_\rho(x) = 1$. For $i = \sigma$ and $j = \rho$, we obtain $\beta_{\sigma\rho}^{V(q_\sigma)} \gamma_\sigma^2 = \beta_{1\rho}^{t_1} \cdots \beta_{n\rho}^{t_n}$. For $i = \rho$ and $j = \sigma$ one has $\sigma(\gamma_\rho) = \gamma_\rho$, and for $i = \rho$ and $j = \rho$ one obtains $\rho(\gamma_\rho) = \gamma_\rho$. The last two equalities are equivalent to $\gamma_\rho \in W^G$. \square

Corollary 5. *With the notation of Corollary 4, assume that G/C is non-cyclic and q_k and t_k are even for some $k \leq n$. Let (β, γ) be the list of data induced by a factor set in $Z^2(G, W)$. Then the list obtained by replacing $\beta_{k\sigma}$ by $-\beta_{k\sigma}$ and keeping the remaining data fixed is also induced by a factor set in $Z^2(G, W)$.*

Proof. It is enough to show that $\beta_{k\sigma}$ appears in all the conditions of Corollary 4 with an even exponent. Indeed, it only appears in (C2.b) with exponent 2; in (C3.b) with exponent q_k ; in (C3.c) with exponent $-V(q_\sigma)$; and in (C3.d) and (C3.f) with exponent t_k . By the assumption it only remains to show that $V(q_\sigma)$ is even. Indeed, $v_2(V(q_\sigma)) = v_2(c^{q_\sigma} - 1) - v_2(c - 1) = 1 + b - v_2(c - 1) \geq 1$ because $c \not\equiv 1 \pmod{2^{1+b}}$. \square

The data (β, γ) induced by a factor set are not cohomologically invariant because they depend on the selection of π and of the u_{c_i} 's, u_σ and u_ρ . However, at least the β_{ij} are cohomologically invariant. For every $\alpha \in H^2(G, W)$ we associate a matrix $\beta_\alpha = (\beta_{ij})_{1 \leq i, j \leq n}$ of elements of W^G as follows: First select a group epimorphism $\pi : \bar{G} \rightarrow G$ realizing α and $u_{c_1}, \dots, u_{c_n} \in \bar{G}$ such that $\pi(u_{c_i}) = c_i$, and then set $\beta_{ij} = [u_{c_j}, u_{c_i}]$. The definition of β_α does not depend on the choice of π and the u_{c_i} 's because if $w_1, w_2 \in W$ and $u_1, u_2 \in \bar{G}$ then $[w_1 u_1, w_2 u_2] = [u_1, u_2]$.

Proposition 6. *Let $\beta = (\beta_{ij})_{1 \leq i, j \leq n}$ be a matrix of elements of W^G and for every $1 \leq i, j \leq n$ let $a_{ii} = 0$ and $a_{ij} = \min(a, v_p(q_i), v_p(q_j))$, if $i \neq j$.*

Then there is an $\alpha \in H^2(G, W)$ such that $\beta = \beta_\alpha$ if and only if the following conditions hold for every $1 \leq i, j \leq n$:

$$\beta_{ij} \beta_{ji} = \beta_{ij}^{p^{a_{ij}}} = 1. \tag{6}$$

Proof. Assume first that $\beta = \beta_\alpha$ for some $\alpha \in Z^2(G, W)$. Then (6) is a consequence of conditions (C1), (C2.a) and (C3.a) of Corollary 4.

Conversely, assume that β satisfies (6). The idea of the proof is that one can enlarge β to a list of data (β, γ) that satisfies conditions (C1)–(C3) of Corollary 4. Hence the desired conclusion follows from the corollary.

Condition (C1) follows automatically from (6). If $i, j \leq n$ then $\beta_{ij} \in W^G$ follows from the fact that $a \geq a_{ij}$ and so (6) implies that $\beta_{ij}^a = 1$. Hence (C2.a) holds. Also (C3.a) holds automatically from (6) because $p^{a_{ij}}$ divides q_i . Hence, we have to select the $\beta_{i\sigma}$'s, $\beta_{i\rho}$'s, γ_i 's, $\beta_{\sigma\rho}$, γ_σ , and γ_ρ for (C2.b) and (C3.b)–(C3.f) to hold.

Assume first that $D = G$. In this case we just take $\beta_{i\sigma} = \beta_{i\rho} = \beta_{\sigma\rho} = \gamma_i = \gamma_\sigma = \gamma_\rho = 1$ for every i . Then (C2.b), (C3.b), (C3.d) and (C3.f) hold trivially by our selection. Moreover, in this case $\sigma = 1$ and so $t_i = 0$ for each $i = 1, \dots, n$, hence (C3.c) also holds.

In the remainder of the proof we assume that $D \neq G$. First we show how one can assign values to $\beta_{\sigma i}$ and γ_i , for $i \leq n$ for (C3.b)–(C3.d) to hold. Let $d = v_p(c - 1)$ and $e = v_p(V(q_\sigma)) = a + b - d$. (see (4)). Note that $d = a$ if $C = D$ and $a = 1 \leq 2 \leq d \leq b$ if $C \neq D$ (because we are assuming that $D \neq G$). Let X_1, X_2, Y_1 and Y_2 be integers such that $c - 1 = p^d X_1$, $V(q_\sigma) = p^e X_2$, and $X_1 Y_1 \equiv X_2 Y_2 \equiv 1 \pmod{p^{a+b}}$. By (6), $\beta_{ij}^{p^{a_{ij}}} = 1$ and so $\beta_{ij} \in W^{p^{a+b-a_{ij}}}$. Therefore there are integers b_{ij} , for $1 \leq i, j \leq n$ such that $b_{ii} = b_{ij} + b_{ji} = 0$ and $\beta_{ij} = \zeta^{b_{ij} p^{a+b-a_{ij}}}$. For every $i \leq n$ set

$$x_i = Y_2 \sum_{j=1}^n t_j b_{ji} p^{a-a_{ji}}, \quad \beta_{\sigma i} = \zeta^{x_i p^{d-a}} \quad y_i = Y_1 Y_2 \sum_{j=1}^n t_j b_{ji} \frac{q_i}{p^{a_{ij}}}, \quad \text{and} \quad \gamma_i = \zeta^{y_i}.$$

Then $V(q_\sigma)p^{d-a}x_i = p^e X_2 Y_2 \sum_{j=1}^n t_j b_{ji} p^{d-a_{ji}} \equiv \sum_{j=1}^n t_j b_{ji} p^{a+b-a_{ji}} \pmod{p^{a+b}}$ and therefore

$$\beta_{\sigma i}^{V(q_\sigma)} = \zeta^{\sum_{j=1}^n t_j b_{ji} p^{a+b-a_{ji}}} = \prod_{i=1}^n \beta_{ji}^{t_j},$$

that is (C3.c) holds. Moreover $q_i p^{d-a} x_i = p^d Y_2 \sum_{j=1}^n t_j b_{ji} \frac{q_i}{p^{a_{ij}}} \equiv p^d X_1 Y_i = (c - 1)y_i$ and therefore $\beta_{i\sigma}^{q_i} = \gamma_i^{c-1}$, that is (C3.b) holds.

We now compute

$$\sum_{i=1}^n t_i x_i = Y_2 \sum_{1 \leq i < j \leq n} t_i t_j b_{ij} p^{a-a_{ij}} = Y_2 \sum_{i=1}^{n+1} t_i^2 b_{ii} p^{a-a_{ii}} + Y_2 \sum_{1 \leq i < j \leq n} t_i t_j (b_{ij} + b_{ji}) p^{a-a_{ij}} = 0. \tag{7}$$

Then setting $\gamma_\sigma = 1$, one has

$$\gamma_\sigma^{c-1} \prod_{i=1}^n \beta_{i\sigma}^{t_i} = \prod_{i=1}^n \zeta^{-t_i x_i p^{d-a}} = \zeta^{-p^{d-a} \sum_{i=1}^n t_i x_i} = 1$$

and (C3.d) holds. This finishes the assignments of $\beta_{i\sigma}$ and γ_i for $i \leq n$ and of γ_σ .

If $C = D$ then a quick end is obtained assigning $\beta_{i\rho} = \beta_{\sigma\rho} = \gamma_\rho = 1$.

So it only remains to assign values to $\beta_{i\rho}$, $\beta_{\sigma\rho}$ and γ_ρ under the assumption that $C \neq D$. Set $\beta_{i\rho} = \zeta^{-Y_1 x_i}$. In this case $p^a = 2$ and therefore $2p^{d-a} x_i = p^d x_i \equiv (c - 1)Y_1 x_i$ and $q_i Y_1 x_i = 2y_i$. Thus $\beta_{i\sigma}^2 \beta_{i\rho}^{c-1} = \zeta^{2p^{d-a} x_i \zeta^{(1-c)Y_1 x_i}} = 1$, hence (C2.b) holds, and $\beta_{i\rho}^{q_i} \gamma_i^2 = \zeta^{-q_i Y_1 x_i + 2y_i} = 1$, hence the first relation of (C3.f) follows.

Finally, using (7) one has

$$\beta_{1\rho}^{t_1} \cdots \beta_{n\rho}^{t_n} = (\beta_{1\sigma}^{t_1} \cdots \beta_{n\sigma}^{t_n})^{-Y_1} = 1 = \gamma_\sigma^2$$

and the last two relations of (C3.f) hold when $\beta_{\sigma\rho} = \gamma_\rho = 1$. \square

Let $\beta = (\beta_{ij})$ be an $n \times n$ matrix of elements of W^G satisfying (6). Then the map $\Psi : B \times B \rightarrow W^G$ given by

$$\Psi((c_1^{x_1} \cdots c_n^{x_n}, c_1^{y_1} \cdots c_n^{y_n})) = \prod_{1 \leq i, j \leq n} \beta_{ij}^{x_i y_j}$$

is a skew pairing of B over W^G in the sense of [3]; that is, it satisfies the following conditions for every $x, y, z \in B$:

$$(\Psi 1) \quad \Psi(x, x) = \Psi(x, y)\Psi(y, x) = 1, \quad (\Psi 2) \quad \Psi(x, yz) = \Psi(x, y)\Psi(x, z).$$

Conversely, every skew pairing of B over W^G is given by a matrix $\beta = (\beta_{ij} = \Psi(c_i, c_j))_{1 \leq i, j \leq n}$ satisfying (6). In particular, every class in $H^2(G, W)$ induces a skew pairing $\Psi = \Psi_\alpha$ of B over W^G given by $\Psi(x, y) = \alpha_{x,y} \alpha_{y,x}^{-1}$, for all $x, y \in B$, for any cocycle α representing the given cohomology class.

In terms of skew pairings, Proposition 6 takes the following form.

Corollary 7. *If Ψ is a skew pairing of B over W^G then there is an $\alpha \in H^2(G, W)$ such that $\Psi = \Psi_\alpha$.*

Corollary 7 was obtained in [3, Proposition 2.5] for $p^a \neq 2$. The remaining cases were considered in [5, Corollary 1.3], where it is stated that for every skew pairing Ψ of C over W^G there is a factor set $\alpha \in Z^2(G, W)$ such that $\Psi(x, y) = \alpha_{x,y} \alpha_{y,x}^{-1}$, for all $x, y \in C$. However, this is false if $\rho^2 \neq 1$ and B has nontrivial elements of order 2. Indeed, if Ψ is the skew pairing of B over W^G given by the factor set α then $\Psi(x, \rho^2) = 1$ for each $x \in C$. To see this we introduce a new set of generators of G , namely $G = \langle c_1, \dots, c_n, c_{n+1}, \rho, \sigma \rangle$ with $c_{n+1} = \rho^2$. Then condition (C3) of Proposition 1, for $i = \rho$ and $j = i$ reads $\beta_{(n+1)i} = 1$ which is equivalent to $\Psi(c_i, \rho^2) = 1$ for all $1 \leq i \leq n$. Using this it is easy to give a counterexample to [5, Corollary 1.3].

Before finishing this section we mention two lemmas that will be needed in next section. The first is elementary and so the proof has been omitted.

Lemma 8. *Let S be the set of skew pairings of B with values in W^G . If $B = B' \times B''$ and $b_1, b_2 \in B'$ and $b_3 \in B''$ then*

$$\max\{\Psi(b_1 \cdot b_3, b_2) : \Psi \in S\} = \max\{\Psi(b_1, b_2) : \Psi \in S\} \cdot \max\{\Psi(b_3, b_2) : \Psi \in S\}.$$

Lemma 9. *Let $\widehat{B} = B \times \langle g \rangle$ be an abelian group and let $h \in B$. If $k = \gcd\{p^a, |g|\}$ and $t = |hB^k|$ then t is the maximum possible value of $\Psi(h, g)$ as Ψ runs over all skew pairings of \widehat{B} over $\langle \zeta_{p^a} \rangle$.*

Proof. Since k divides p^a , the hypothesis $t = |hB^k|$ implies that there is a group homomorphism $\chi : B \rightarrow \langle \zeta_{p^a} \rangle$ such that $\chi(B^k) = 1$ and $\chi(h)$ has order t . Let $\Psi : \widehat{B} \times \widehat{B} \rightarrow \langle \zeta_{p^a} \rangle$ be given by $\Psi(xg^i, yg^j) = \chi(x^i y^{-j}) = \chi(x)^i \chi(y)^{-j}$, for $x, y \in B$.

If $g^i = g^{i'}$, then $i \equiv i' \pmod{|g|}$ and hence $i \equiv i' \pmod{k}$. Therefore, $x^i B^k = x^{i'} B^k$, which implies that $\chi(x)^i = \chi(x)^{i'}$. This shows that Ψ is well defined. Now it is easy to see that Ψ is a skew pairing and $\Psi(h, g) = \chi(h)$ has order t .

Conversely, if Ψ is any skew pairing of \widehat{B} over $\langle \zeta_{p^a} \rangle$, then $\Psi(x, g)^{p^a} = 1$ and $\Psi(x, g)^{|x|} = \Psi(1, g) = 1$ for all $x \in B$. This implies that $\Psi(x^k, g) = \Psi(x, g)^k = 1$ for all $x \in B$, and so $\Psi(B^k, g) = 1$. Therefore $\Psi(h, g)^t = \Psi(h^t, g) \in \Psi(B^k, g) = 1$, so the order of $\Psi(h, g)$ divides t . \square

3. Local index computations

In this section K denotes an abelian number field, p a prime, and r an odd prime. Our goal is to find a global formula for $\beta(r) = \beta_p(r)$, the maximum nonnegative integer for which $p^{\beta(r)}$ is the r -local index of a Schur algebra over K .

We are going to abuse the notation and denote by K_r the completion of K at a (any) prime of K dividing r . If E/K is a finite Galois extension, one may assume that the prime of E dividing r , used to compute E_r , divides the prime of K over r , used to compute K_r . We use the classical notation:

$$\begin{aligned} e(E/K, r) &= e(E_r/K_r) = \text{ramification index of } E_r/K_r. \\ f(E/K, r) &= f(E_r/K_r) = \text{residue degree of } E_r/K_r. \\ m_r(A) &= \text{Index of } K_r \otimes_K A, \text{ for a Schur algebra } A \text{ over } K. \end{aligned}$$

By Benard–Schacher Theory and because E/K is a finite Galois extension, $e(E/K, r)$, $f(E/K, r)$ and $m_r(A)$ do not depend on the selection of the prime of K dividing r (see [7,2]). By the Benard–Schacher Theorem and because $|S(K_r)|$ divides $r - 1$ [8], if either $\zeta_p \notin K$ or $r \not\equiv 1 \pmod{p}$ then $\beta(r) = 0$. So to avoid trivialities we assume that $\zeta_p \in K$ and $r \equiv 1 \pmod{p}$.

Suppose $K \subseteq F = \mathbb{Q}(\zeta_n)$ for some positive integer n and let $n = r^{v_r(n)} n'$. Then $\text{Gal}(F/\mathbb{Q})$ contains a canonical Frobenius automorphism at r which is defined by $\psi_r(\zeta_{r^{v_r(n)}}) = \zeta_{r^{v_r(n)}}$ and $\psi_r(\zeta_{n'}) = \zeta_{n'}^r$. We can then define the canonical Frobenius automorphism at r in $\text{Gal}(F/K)$ as $\phi_r = \psi_r^{f(K/\mathbb{Q}, r)}$. On the other hand, the inertia subgroup at r in $\text{Gal}(F/K)$ is by definition the subgroup of $\text{Gal}(F/K)$ that acts as $\text{Gal}(F_r/K_r(\zeta_{n'}))$ in the completion at r .

We use the following notations.

Notation 10. First we define some positive integers:

$$\begin{aligned} m &= \text{minimum even positive integer with } K \subseteq \mathbb{Q}(\zeta_m), \\ a &= \text{minimum positive integer with } \zeta_{p^a} \in K, \\ s &= v_p(m) \text{ and} \end{aligned}$$

$$b = \begin{cases} s, & \text{if } p \text{ is odd or } \zeta_4 \in K, \\ s + v_p([\mathbb{K} \cap \mathbb{Q}(\zeta_{p^s}) : \mathbb{Q}]) + 2, & \text{if } \text{Gal}(K(\zeta_{p^{2a+s}})/K) \text{ is not cyclic, and} \\ s + 1, & \text{otherwise.} \end{cases}$$

We also define

$$\begin{aligned} L &= \mathbb{Q}(\zeta_m), \quad \zeta = \zeta_{p^{a+b}}, \quad W = \langle \zeta \rangle, \quad F = L(\zeta), \\ G &= \text{Gal}(F/K), \quad C = \text{Gal}(F/K(\zeta)), \quad \text{and} \quad D = \text{Gal}(F/K(\zeta + \zeta^{-1})). \end{aligned}$$

Since $\zeta_p \in K$, the automorphism $\gamma : G \rightarrow \text{Aut}(W)$ induced by the Galois action satisfies the conditions of Section 2 and the notation is consistent. As in that section we fix elements ρ and σ in G and a subgroup $B = \langle c_1 \rangle \times \dots \times \langle c_n \rangle$ of C such that $D = B \times \langle \rho \rangle$, $C = B \times \langle \rho^2 \rangle$ and $G/C = \langle \rho C \rangle \times \langle \sigma C \rangle$. Furthermore, $\sigma(\zeta) = \zeta^c$ for some integer c chosen according to (4). Notice that by the choice of b , $G \neq B$.

We also fix an odd prime r and set

$$e = e(K(\zeta_r)/K, r), \quad f = f(K/\mathbb{Q}, r) \quad \text{and} \quad v(r) = \max\{0, a + v_p(e) - v_p(r^f - 1)\}.$$

Let $\phi \in G$ be the canonical Frobenius automorphism at r in G , and write

$$\phi = \rho^{j'} \sigma^{j'} \eta, \quad \text{with } \eta \in B, \quad 0 \leq j' < |\rho| \quad \text{and} \quad 0 \leq j < |\sigma C|.$$

Let q be an odd prime not dividing m . Let $G_q = \text{Gal}(F(\zeta_q)/K)$, $C_q = \text{Gal}(F(\zeta_q)/K(\zeta))$ and let c_0 denote a generator of $\text{Gal}(F(\zeta_q)/F)$. Finally we fix

$$\begin{aligned} \theta &= \theta_q, \text{ a generator of the inertia group of } r \text{ in } G_q \text{ and} \\ \phi_q &= c_0^{s_0} \phi = c_0^{s_0} \eta \rho^{j'} \sigma^{j'} = \eta_q \rho^{j'} \sigma^{j'}, \text{ the canonical Frobenius automorphism at } r \text{ in } G_q. \end{aligned}$$

Observe that we are considering G as a subgroup of G_q by identifying G with $\text{Gal}(F(\zeta_q)/K(\zeta))$. Again the Galois action induces a homomorphism $\gamma_q : G_q \rightarrow \text{Aut}(W)$ and $W^{G_q} = \langle \zeta_{p^a} \rangle$. So this action satisfies the conditions of Section 2 and we adapt the notation by setting

$$B_q = \langle c_0 \rangle \times B, \quad C_q = \text{Gal}(F(\zeta_q)/K(\zeta)) = \text{Ker}(\gamma_q) \quad \text{and} \quad D_q = \text{Gal}(F(\zeta_q)/K(\zeta + \zeta^{-1})).$$

Notice that $C_q = \langle c_0 \rangle \times C = B_q \times \langle \rho^2 \rangle$ and $D_q = D \times \langle c_0 \rangle$. Hence $G/C \simeq G_q/C_q$.

If Ψ is a skew pairing of B over W^G then Ψ has a unique extension to a skew pairing Ψ of C over W^G which satisfies $\Psi(B, \rho^2) = \Psi(\rho^2, B) = 1$. So we are going to apply skew pairings of B to pairs of elements in C under the assumption that we are using this extension.

Since $p \neq r, \theta \in C_q$. Moreover, if $r = q$ then θ is a generator of $\text{Gal}(F(\zeta_r)/F)$ and otherwise $\theta \in C$. Notice also that if G/C is non-cyclic then $p^a = 2$ and $K \cap \mathbb{Q}(\zeta_{2^s}) = \mathbb{Q}(\zeta_{2^d} + \zeta_{2^d}^{-1})$, where $d = v_p(c - 1)$, and so $b = s + d$.

It follows from results of Janusz [3, Proposition 3.2] and Pendergrass [6, Theorem 1] that $p^{\beta(r)}$ always occurs as the r -local index of a cyclotomic algebra of the form $(L(\zeta_q)/L, \alpha)$ where q is either 4 or a prime not dividing m and α takes values in $W(L(\zeta_q))_p$, with the possibility of $q = 4$ occurring only in the case when $p^s = 2$. By inflating the factor set α to $F(\zeta_q)$ (which will be equal to F when $p^s = 2$), we have that $p^{\beta(r)} = m_r(A)$, where

$$\begin{aligned} A &= (F(\zeta_q)/K, \alpha) \text{ (we also write } \alpha \text{ for the inflation),} \\ q &\text{ is an odd prime not dividing } m, \text{ and} \\ \alpha &\text{ takes values in } \langle \zeta_{p^4} \rangle \text{ if } p^s = 2 \text{ and in } \langle \zeta_{p^s} \rangle \text{ otherwise.} \end{aligned} \tag{8}$$

So it suffices to find a formula for the maximum r -local index of a Schur algebra over K of this form.

Write $A = \bigoplus_{g \in G_q} F(\zeta_q)u_g$, with $u_g^{-1}xu_g = g(x)$ and $u_gu_h = \alpha_{g,h}u_{gh}$, for each $x \in F(\zeta_q)$ and $g, h \in G_q$. After a diagonal change of basis one may assume that if $g = c_0^{s_0}c_1^{s_1} \dots c_n^{s_n}\rho^{s_\rho}\sigma^{s_\sigma}$ with $0 \leq s_i < q_i = |c_i|, 0 \leq s_\rho < |\rho|$ and $0 \leq s_\sigma < q_\sigma = |\sigma C|$ then $u_g = u_{c_0}^{s_0}u_{c_1}^{s_1} \dots u_{c_n}^{s_n}u_\rho^{s_\rho}u_\sigma^{s_\sigma}$.

It is well known (see [8] and [3, Theorem 1]) that

$$m_r(A) = |\xi|, \quad \text{where } \xi = \xi_\alpha = \left(\frac{\alpha_{\theta, \phi_q}}{\alpha_{\phi_q, \theta}} \right)^{r^{v_r(e)}} u_\theta^{r^{v_r(e)}(r^f - 1)}. \tag{9}$$

This can be slightly simplified as follows. If $r|e$ then $\langle \theta \rangle$ has an element θ^k of order r . Since θ fixes every root of unity of order coprime with r , necessarily r^2 divides m and the fixed field of θ^k in L is $\mathbb{Q}(\zeta_{m/r})$. Then $K \subseteq \mathbb{Q}(\zeta_{m/r})$, contradicting the minimality of m . Thus $r \nmid e$ and so

$$\xi = \frac{\alpha_{\theta, \phi_q}}{\alpha_{\phi_q, \theta}} u_\theta^{r^f - 1} = \frac{\alpha_{\theta, \phi_q}}{\alpha_{\phi_q, \theta}} \gamma_\theta^{\frac{r^f - 1}{e}} = [u_\theta, u_{\phi_q}] \gamma_\theta^{\frac{r^f - 1}{e}}, \quad \text{where } \gamma_\theta = u_\theta^e. \tag{10}$$

With our choice of the $\{u_g : g \in G_q\}$, we have

$$[u_\theta, u_{\phi_q}] = [u_\theta, u_{\eta_q} u_\rho^j u_\sigma^i] = \Psi(\theta, \eta_q)[u_\theta, u_\rho^j u_\sigma^i],$$

where $\Psi = \Psi_\alpha$ is the skew pairing associated to α . Therefore,

$$\xi = \xi_0 \Psi(\theta, \eta_q) \quad \text{with} \quad \xi_0 = \xi_{0,\alpha} = [u_\theta, u_\rho^j u_\sigma^i] \gamma_\theta^{\frac{r^f - 1}{e}}.$$

Let (β, γ) be the data associated to the factor set α (relative to the set of generators $c_1, \dots, c_n, \rho, \sigma$).

Lemma 11. Let $A = (F(\zeta_q)/K, \alpha)$ be a cyclotomic algebra satisfying the conditions of (8) and use the above notation. Let $\theta = c_0^{s_0}c_1^{s_1} \dots c_n^{s_n}\rho^{2s_{n+1}}$, with $0 \leq s_i < q_i$ for $0 \leq i \leq n$, and $0 \leq s_{n+1} \leq |\rho^2|$.

- (1) If G/C is cyclic then $\xi_0^{p^{v(r)}} = 1$.
- (2) Assume that G/C is non cyclic and let $\mu_i = \beta_{i\rho}^{\frac{1-c}{2}} \beta_{i\sigma}^{-1}$. Then $\mu_i = \pm 1$ and $\xi_0^{p^{v(r)}} = \prod_{i=0}^n \mu_i^{2^{v(r)}(j+j')s_i}$.

Proof. For the sake of regularity we write $c_{n+1} = \rho^2$. Since $e = |\theta|$, we have that q_i divides es_i for each i . Furthermore, $v_p(e)$ is the maximum of the $v_p\left(\frac{q_i}{\text{gcd}(q_i, s_i)}\right)$ for $i = 1, \dots, n$. Then

$$v_p(e) - v_p(r^f - 1) = \max \left\{ v_p\left(\frac{q_i}{\text{gcd}(q_i, s_i)}\right), i = 1, \dots, n \right\}.$$

Hence

$$\begin{aligned} v(r) &= \max\{0, v_p(e) + a - v_p(r^f - 1)\} \\ &= \min \left\{ x \geq 0 : p^a \text{ divides } p^x \cdot \frac{s_i(r^f - 1)}{q_i}, \text{ for each } i = 1, \dots, n \right\}. \end{aligned} \tag{11}$$

Now we compute γ_θ in terms of the previous expression of θ . Set $v = u_{c_{n+1}}^{s_{n+1}}$ and $y = u_{c_0}^{s_0}u_{c_1}^{s_1} \dots u_{c_n}^{s_n}$. Then

$$u_\theta = yv = \gamma yv, \quad \text{with } \gamma = \Psi(c_{n+1}^{s_{n+1}}, c_0^{s_0}c_1^{s_1} \dots c_n^{s_n}).$$

Thus $\gamma^e = \Psi(c_{n+1}^{es_{n+1}}, c_0^{s_0} c_1^{s_1} \dots, c_n^{s_n}) = 1$. Using that $[y, \gamma] = 1$, one easily proves by induction on m that

$$(\gamma v)^m = \gamma^{\binom{m}{2}} y^m v^m.$$

Hence

$$(\gamma v)^e = \gamma^{\binom{e}{2}} y^e v^e = \gamma^{\binom{e}{2}} y^e u_{c_{n+1}}^{es_{n+1}} = \gamma^{\binom{e}{2}} y^e \gamma_\rho^{\frac{es_{n+1}}{q_{n+1}}},$$

and $\gamma^{\binom{e}{2}} = \pm 1$. (If p or e is odd then necessarily $\gamma^{\binom{e}{2}} = 1$.) Now an easy induction argument shows

$$\gamma_\theta = \mu \gamma_0^{\frac{es_0}{q_0}} \gamma_1^{\frac{es_1}{q_1}} \dots \gamma_n^{\frac{es_n}{q_n}} \gamma_\rho^{\frac{es_{n+1}}{q_{n+1}}}, \quad \text{for some } \mu = \pm 1.$$

Note that $v(r) + v_p(r^f - 1) - v_p(e) \geq a \geq 1$, by (11). Then $\mu^{p^{v(r)} \frac{r^f - 1}{e}} = \gamma_\rho^{p^{v(r)} \frac{r^f - 1}{e}} = 1$, because both μ and γ_ρ are ± 1 , and they are 1 if p is odd (see (C3.e) and (C3.f)). Thus

$$\gamma_\theta^{p^{v(r)} \frac{r^f - 1}{e}} = \prod_{i=0}^n \gamma_i^{p^{v(r)} \frac{(r^f - 1) s_i}{q_i}}. \tag{12}$$

(1) Assume that G/C is cyclic. We have that $\rho = 1$ and $v_p(c - 1) = a$. Note that the β 's and γ 's are p^b -th roots of unity by (8).

Let Y be an integer satisfying $Y \frac{c-1}{p^a} \equiv 1 \pmod{p^b}$. Since $\phi_q = \sigma^j \eta_q$ with $\eta_q \in C_q$, we have $r^f \equiv c^j \pmod{p^{a+b}}$ and so $Y \frac{r^f - 1}{p^a} = Y \frac{c-1}{p^a} \frac{c^j - 1}{c-1} \equiv V(j) \pmod{p^b}$. Then $\beta_{i\sigma}^{Y \frac{r^f - 1}{p^a}} = \beta_{i\sigma}^{V(j)}$.

Using that p^a divides $p^{v(r)} \frac{s_i(r^f - 1)}{q_i}$ (see (11)) and $Y \frac{c-1}{p^a} \equiv 1 \pmod{p^b}$ we obtain

$$\gamma_i^{p^{v(r)} \frac{s_i(r^f - 1)}{q_i}} = (\gamma_i^{c-1})^{Y \frac{p^{v(r)} s_i(r^f - 1)}{p^a q_i}}.$$

Combining this with (C3.b) we have

$$\begin{aligned} [u_{c_i}^{s_i}, u_\sigma^j]^{p^{v(r)}} \gamma_i^{p^{v(r)} \frac{s_i(r^f - 1)}{q_i}} &= [u_{c_i}, u_\sigma]^{s_i V(j) p^{v(r)}} (\gamma_i^{c-1})^{Y \frac{p^{v(r)} s_i(r^f - 1)}{p^a q_i}} \\ &= [u_{c_i}, u_\sigma]^{s_i V(j) p^{v(r)}} \beta_{i\sigma}^{Y \frac{p^{v(r)} s_i(r^f - 1)}{p^a}} \\ &= ([u_{c_i}, u_\sigma] \beta_{i\sigma})^{p^{v(r)} s_i V(j)} = 1, \end{aligned} \tag{13}$$

because $\beta_{i\sigma} = [u_\sigma, u_{c_i}] = [u_{c_i}, u_\sigma]^{-1}$. Using (12) and (13) we have

$$\xi_0^{p^{v(r)}} = [u_\theta, u_\sigma^j]^{p^{v(r)}} \gamma_\theta^{p^{v(r)} \frac{r^f - 1}{e}} = \prod_{i=0}^n [u_{c_i}^{s_i}, u_\sigma^j]^{p^{v(r)}} \gamma_i^{p^{v(r)} \frac{s_i(r^f - 1)}{q_i}} = 1$$

and the lemma is proved in this case.

(2). Assume now that G/C is non-cyclic. Then $p^a = 2$ and if $d = v_2(c - 1)$ then $d \geq 2$ and $b = s + d$. The data for α lie in $\langle \zeta_{2^{s+1}} \rangle \subseteq \langle \zeta_{2^b} \rangle \subseteq \langle \zeta_{2^{1+s+d}} \rangle = W(F)_2$. (C2.b) implies $\mu_i = \pm 1$ and using (C3.b) and (C3.f) one has $\gamma_i^{c+1} = \beta_{i\sigma}^{q_i} \beta_{i\rho}^{-q_i}$. Let X and Y be integers satisfying $X \frac{c-1}{2^d} \equiv Y \frac{c+1}{2} \equiv 1 \pmod{2^{1+s+d}}$ and set $Z = Y \frac{r^f - 1}{2}$.

Recall that $2^a = 2$ divides $2^{v(r)} \frac{s_i(r^f - 1)}{q_i}$, by (11). Therefore,

$$\gamma_i^{2^{v(r)} \frac{s_i(r^f - 1)}{q_i}} = (\gamma_i^{c+1})^{2^{v(r)} \frac{s_i(r^f - 1)}{2q_i}} = (\beta_{i\sigma}^{s_i} \beta_{i\rho}^{-s_i})^{2^{v(r)} Z}. \tag{14}$$

Let $j'' \equiv j' \pmod{2}$ with $j'' \in \{0, 1\}$. Then $\mathcal{Y}(\rho^{j''}) = \mathcal{Y}(\rho^{j'})$ and $N_{i\rho}^{j''}(w) = w^{j''}$. Therefore,

$$\begin{aligned} [u_\theta, u_\rho^{j'} u_\sigma^j] &= [u_\theta, u_\rho^{j''} u_\sigma^j] [u_\rho^{j'} u_\rho^{-j''}] = \prod_{i=0}^n (\beta_{i\rho}^{-s_i})^{j''} (\beta_{i\sigma}^{-s_i})^{V(j) (-1)^{j''}} \\ &= \prod_{i=0}^n (\beta_{i\rho}^{-s_i})^{j''} (\beta_{i\sigma}^{-s_i})^{X \frac{c-1}{2^d} V(j) (-1)^{j''}} = \prod_{i=0}^n (\beta_{i\rho}^{-s_i})^{j''} (\beta_{i\sigma}^{-s_i})^{X \frac{c-1}{2^d} (-1)^{j''}}. \end{aligned} \tag{15}$$

Using (12), (14) and (15) we obtain

$$\xi_0^{2^{v(r)}} = [u_\theta, u'_\rho u'_\sigma]^{2^{v(r)}} \gamma_\theta^{2^{v(r)} \frac{r^f-1}{e}} = \left(\prod_{i=0}^n \beta_{i\rho}^{-s_i} \right)^{2^{v(r)}(Z+j'')} \left(\prod_{i=0}^n \beta_{i\sigma}^{s_i} \right)^{2^{v(r)} \left(Z - X \frac{c^j-1}{2^d} (-1)^{j''} \right)}. \tag{16}$$

We claim that $Z + j'' \equiv 0 \pmod{2^{d-1}}$. On the one hand $Y \equiv 1 \pmod{2^{d-1}}$. On the other hand, $\phi_q = \rho^j \sigma^j \eta_q$, with $\eta_q \in C_q$ and so $r^f \equiv (-1)^{j'} c^j \pmod{2^{1+s+d}}$. Hence $r^f \equiv (-1)^{j'} = (-1)^{j''} \pmod{2^d}$ and therefore $Z + j'' = Y \frac{r^f-1}{2} + j'' \equiv \frac{(-1)^{j''}-1}{2} + j'' \pmod{2^{d-1}}$. Considering the two possible values of $j'' \in \{0, 1\}$ we have $\frac{(-1)^{j''}-1}{2} + j'' = 0$ and the claim follows.

From $d = v_2(c - 1)$ one has $c \equiv 1 + 2^{d-1} \pmod{2^d}$ and hence $Y \equiv 1 + 2^{d-1} \pmod{2^d}$ and $r^f \equiv (-1)^{j'} c^j \equiv (-1)^{j'} (1 + j2^d) \pmod{2^{1+s+d}}$. Then

$$\begin{aligned} \frac{Z + j''}{2^{d-1}} &= \frac{Y(r^f - 1) + 2j''}{2^d} \equiv \frac{Y((-1)^{j''} (1 + j2^d) - 1) + 2j''}{2^d} = \frac{Y \left(\frac{(-1)^{j''}-1}{2} + (-1)^{j''} j2^{d-1} \right) + j''}{2^{d-1}} \\ &\equiv \frac{(1 + 2^{d-1})(-j'' + (-1)^{j''} j2^{d-1}) + j''}{2^{d-1}} = \frac{-j'' - j''2^{d-1} + (-1)^{j''} j2^{d-1} + (-1)^{j''} j2^{2(d-1)} + j''}{2^{d-1}} \\ &\equiv -j'' + (-1)^{j''} j \equiv j + j'' \equiv j + j' \pmod{2}. \end{aligned}$$

Using this, the equality $\beta_{i\rho}^{\frac{1-c}{2}} = \mu_i \beta_{i\sigma}$ and the fact that $\mu_i = \pm 1$ we obtain

$$\beta_{i\rho}^{-(Z+j'')} = \beta_{i\rho}^{-X \frac{c-1}{2^d} (Z+j'')} = \beta_{i\rho}^{-X \frac{c-1}{2} \frac{Z+j''}{2^{d-1}}} = \mu_i^{Z+j''} \beta_{i\sigma}^{X \frac{Z+j''}{2^{d-1}}} = \mu_i^{j+j'} \beta_{i\sigma}^{X \frac{Z+j''}{2^{d-1}}}.$$

Combining this with (16) we have

$$\begin{aligned} \xi_0^{2^{v(r)}} &= \prod_{i=0}^n \mu_i^{2^{v(r)}(j+j'')s_i} \prod_{i=0}^n (\beta_{i\sigma}^{s_i})^{2^{v(r)} \left[Z - X \frac{c^j-1}{2^d} (-1)^{j''} + \frac{X(Z+j'')}{2^{d-1}} \right]} \\ &= \prod_{i=0}^n \mu_i^{2^{v(r)}(j+j'')s_i} \prod_{i=0}^n (\beta_{i\sigma}^{s_i})^{2^{v(r)} \left[\frac{2^d Z + X(c^j-1)(-1)^{j''} + 2X(Z+j'')}{2^d} \right]}. \end{aligned}$$

To finish the proof it is enough to show that the exponent of each $\beta_{i\sigma}$ in the previous expression is a multiple of 2^{1+s} . Indeed, $2^d \equiv X(c - 1) \pmod{2^{1+s+d}}$ and so

$$\begin{aligned} 2^d Z + X(c^j - 1)(-1)^{j''} + 2X(Z + j'') &\equiv ZX(c - 1) - X(c^j - 1)(-1)^{j''} + 2X(Z + j'') \\ &= X \left(Y \frac{r^f - 1}{2} (c + 1) + (c^j - 1)(-1)^{j''} + 2j'' \right) \\ &= X \left((r^f - 1)Y \frac{c + 1}{2} - c^j (-1)^{j''} + (-1)^{j''} + 2j'' \right) \\ &\equiv X(r^f - 1 - c^j (-1)^{j''} + 1) \equiv 0 \pmod{2^{1+s+d}} \end{aligned}$$

as required. This finishes the proof of the lemma in Case 2. \square

We need the following Proposition from [3].

Proposition 12. For every odd prime $q \neq r$ not dividing m let $d(q) = \min\{a, v_p(q - 1)\}$. Then

- (1) $|c_0^{kq} C / C^{p^{d(q)}}| \leq |\theta_q^f C / C^{p^a}|$, and
- (2) the equality holds if $q \equiv 1 \pmod{p^a}$ and r is not congruent with a p -th power modulo q . There are infinitely many primes q satisfying these conditions.

Proof. See Proposition 4.1 and Lemma 4.2 of [3]. \square

We are ready to prove the main result of the paper.

Theorem 13. Let K be an abelian number field, p a prime and r an odd prime. If either $\zeta_p \notin K$ or $r \not\equiv 1 \pmod{p}$ then $\beta_p(r) = 0$. Assume otherwise that $\zeta_p \in K$ and $r \equiv 1 \pmod{p}$, and use Notation 10 including the decomposition $\phi = \eta \rho^j \sigma^j$ with $\eta \in B$.

- (1) Assume that r does not divide m .
 - (a) If G/C is non-cyclic and $j \not\equiv j' \pmod{2}$ then $\beta_p(r) = 1$.
 - (b) Otherwise $\beta_p(r) = \max\{v(r), v_p(|\eta B^{p^{d(r)}}|)\}$, where $d(r) = \min\{a, v_p(r - 1)\}$.

- (2) Assume that r divides m and let q_0 be an odd prime not dividing m such that $q_0 \equiv 1 \pmod{p^a}$ and r is not a p -th power modulo q_0 . Let $\theta = \theta_{q_0}$ be a generator of the inertia group of G_{q_0} at r .
- (a) If G/C is non-cyclic, $j \not\equiv j' \pmod{2}$ and θ is not a square in D then $\beta_p(r) = 1$.
 - (b) Otherwise $\beta_p(r) = \max\{\nu(r), h, \nu_p(|\theta^f C^{p^a}|)\}$, where $h = \max_{\psi} \{\nu_p(|\Psi(\theta, \eta)|)\}$ as Ψ runs over all skew pairings of B over $\langle \zeta_{p^a} \rangle$.

Proof. For simplicity we write $\beta(r) = \beta_p(r)$. We already explained why if either $\zeta_p \notin K$ or $r \not\equiv 1 \pmod{p}$ then $\beta_p(r) = 0$. So in the remainder of the proof we assume that $\zeta_p \in K$ and $r \equiv 1 \pmod{p}$, and so K, p , and r satisfy the condition mentioned at the beginning of the section. It was also pointed out earlier in this section that $p^{\beta(r)}$ is the r -local index of a crossed product algebra A of the form $A = (F(\zeta_q)/K, \alpha)$ with q and α taking values in $\langle \zeta_{p^s} \rangle$ or in $\langle \zeta_4 \rangle$. Moreover, since $p^{\nu(r)}$ is the r -local index of the cyclic Schur algebra $(K(\zeta_r)/K, c_0, \zeta_{p^a})$ [3], we always have $\nu(r) \leq \beta(r)$.

In Case 1 one may assume that $q = r$, because $(F(\zeta_q)/K, \alpha)$ has r -local index 1 for every $q \neq r$. Since $\text{Gal}(F(\zeta_r)/F)$ is the inertia group at r in G_r , in this case one may assume that $\theta = \theta_r = c_0$. On the contrary, in Case 2, $q \neq r$, and $\theta = c_1^{s_1} \dots c_n^{s_n} \rho^{2s_{n+1}}$, for some s_1, \dots, s_{n+1} .

In cases (1.a) and (2.a), G/C is non-cyclic and hence $p^a = 2$. Then $\beta(r) \leq 1$, by the Benard–Schacher theorem, and hence if $\nu(r) = 1$ then $\beta(r) = 1$. So assume that $\nu(r) = 0$. Furthermore, in case (2.a), s_i is odd for some $i \leq n$, because $\theta \notin D^2$. Now we can use Corollary 5 to produce a cyclotomic algebra $A' = (F(\zeta_q)/K, \alpha')$ so that $\xi_\alpha = -\xi_{\alpha'}$. Indeed, there is such an algebra such that all the data associated to α are equal to the data for A , except for $\beta_{0\sigma}$, in case (1.a), and $\beta_{k\sigma}$, case (2.a). Using Lemma 11 and the assumptions $\nu(r) = 0$ and $j \not\equiv j' \pmod{2}$, one has $\xi_{0,\alpha} = -\xi_{0,\alpha'}$ and $\Psi_\alpha = \Psi_{\alpha'}$. Thus $\xi_\alpha = -\xi_{\alpha'}$, as claimed. This shows that $\beta(r) = 1$ in cases (1.a) and (2.a).

In case (1.b), $\xi = \xi_0 \Psi(c_0, \eta)$. By Lemma 11, ξ_0 has order dividing $p^{\nu(r)}$ in this case and, by Lemma 9, $\max\{|\Psi(\theta, \eta)| : \Psi \in S\} = |\eta B^{p^{d(r)}}|$, where S is the set of skew pairings of B_r with values in $\langle p^a \rangle$. Using this and $\nu(r) \leq \beta(r)$ one deduces that $\beta(r) = \max\{\nu(r), \nu_p(|\eta B^{p^{d(r)}}|)\}$.

The formula for case (2.b) is obtained in a similar way using the equality $\xi = \xi_0 \Psi(\theta, \eta) \Psi(\theta, c_0^{s_0})$ and Lemmas 8 and 9.

□

4. Examples

As we indicated in the introduction, the authors' main motivation for Theorem 13 is the study the gap between the Schur group of an abelian number field K and its subgroup generated by classes containing cyclic cyclotomic algebras over K , a problem which reduces to studying the gaps between the integers $\nu_p(r)$ and $\beta_p(r)$ for all finite primes p and odd primes r . (For details, see [4].) What Theorem 13 really allows one to do is to compute $\beta_p(r)$ in terms of the number of p -th power roots of unity in K and the embedding of $\text{Gal}(F/K)$ in $\text{Gal}(F/\mathbb{Q})$. In this section, we will provide some examples of abelian number fields K to illustrate the computations involved in the various cases of Theorem 13. We use the notation of the previous sections in all of these examples.

Example 14. Let $K = \mathbb{Q}(\zeta_m)$, with m minimal. Let p be a prime for which $\zeta_p \in K$, and let r be an odd prime which is $\equiv 1 \pmod{p}$. Let a be the maximal integer for which $\zeta_{p^a} \in K$, and let $s = \nu_p(m)$. If we are not in the case when $b = s$, then $p = 2, s = 0$, and $K(\zeta_{p^{2a+s}}) = K(\zeta_4)$, so we will be in the case where $b = s + 1 = 1$. Since $K = L$, we have that $F = K(\zeta_{p^{a+b}})$, so C is trivial. Also, $G = \text{Gal}(K(\zeta_{p^{a+b}})/K)$ will be cyclic for either case of b . Therefore, either case (1b) or (2b) of Theorem 13 applies, and it is immediate from $C = B = 1$ that $\beta_p(r) = \nu_p(r)$ for each choice of p and r .

Example 15. Let p and r be odd primes with $\nu_p(r - 1) = 2$. Let K be the extension of $\mathbb{Q}(\zeta_p)$ with index p in $L = \mathbb{Q}(\zeta_{pr})$, and consider $\beta_p(r)$. We have $a = s = b = 1$, and $F = \mathbb{Q}(\zeta_{p^2r})$. We have that $G = \langle \theta \rangle \times C$ is elementary abelian of order p^2 , so we are in case (2b) of Theorem 13. Since $\text{Gal}(F/\mathbb{Q})$ has an element ψ such that ψ^p generates C , letting q_0 and θ be as in Theorem 13(2), we find that $\nu_p(|\psi G|) = 1$. It follows that $p^f = p$, so $\nu_p(r) = 0$ and $\nu_p(|\theta^f C^{p^a}|) = 1$. Since ϕ generates C , we have that $\phi = \eta$ and so $h = 1$ by Lemma 9. So $\beta_p(r) = 1$ in this case.

Example 16. Let q be a prime greater than 5, and let $K = \mathbb{Q}(\zeta_q, \sqrt{2})$. Let $p = 2$, and let r be any prime for which $r^2 \equiv 1 \pmod{q}$ and $r \equiv 5 \pmod{2^6}$. In computing $\beta_2(r)$, one sees that $a = 1$ and $L = \mathbb{Q}(\zeta_{8q})$, so $s = 3$. Since $\text{Gal}(K(\zeta_{25})/K)$ is not cyclic, we set $b = 5 + \nu_2([\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]) = 6$, so $F = \mathbb{Q}(\zeta_{64q})$. Since $\mathbb{Q}(\zeta_q) \subset K$, we have $C = \text{Gal}(F/K(\zeta_{64})) = 1$. For our generators of $\text{Gal}(F/K)$, we may choose ρ, σ such that $\rho(\zeta_q) = \zeta_q, \rho(\zeta_{64}) = \zeta_{64}^{-1}, \sigma(\zeta_q) = \zeta_q$, and $\sigma(\zeta_{64}) = \zeta_{64}^9$. By our choice of r , we have that $\psi_r \notin G$, but $5^2 \equiv 9^3 \pmod{64}$ implies that $\psi_r^2 = \sigma^3$. This means that we are in case (1a) of Theorem 13 with $\nu_p(r) = 0$ and $j \not\equiv j' \pmod{2}$, so $\beta_2(r) = 1$.

Example 17. Let r be a prime for which $r \equiv 5 \pmod{64}$. Let K' be the unique subfield of index 2 in $\mathbb{Q}(\zeta_r)$, and let $K = K'(\sqrt{2})$. Consider $\beta_2(r)$ for the field K . As in the previous example, we have $L = \mathbb{Q}(\zeta_{8r}), F = \mathbb{Q}(\zeta_{64r})$ and we choose $\rho, \sigma \in G$ satisfying $\rho(\zeta_{64}) = \zeta_{64}^{-1}$ and $\sigma(\zeta_{64}) = \zeta_{64}^9$. Using Proposition 12, choose an odd prime q_0 for which r in not a square modulo q_0 . If ψ_r is the Frobenius automorphism in $\text{Gal}(F(\zeta_{q_0})/\mathbb{Q})$, then $\psi_r \notin G_{q_0}$, and $\phi_r = \psi_r^2$ sends ζ_{64} to $\zeta_{64}^{5^2} = \zeta_{64}^{9^3}$. Therefore, $\phi_r = \sigma^3 \eta_{q_0}$, where $\eta_{q_0} \in C_{q_0}$ fixes ζ_{64r} . Since $\zeta_r \notin K, \theta = \theta_{q_0}$ generates a direct factor of G_{q_0} and so it cannot be a square in D . It follows that the conditions of case (2a) of Theorem 13 hold, and so we can conclude $\beta_2(r) = 1$.

Example 18. Let p be an odd prime and let q and r be primes for which $v_p(q-1) = v_p(r-1) = 2$, $v_q(r^p-1) = 0$, and $v_q(r^{p^2}-1) = 1$. The existence of such primes q and r for each odd prime p is a consequence of Dirichlet's Theorem on primes in arithmetic progression. Indeed, given p and q primes with $v_p(q-1) = 2$, there is an integer k , coprime to q such that the order of k modulo q^2 is p^2 . Choose a prime r for which $r \equiv k+q \pmod{q^2}$ and $r \equiv 1+p^2 \pmod{p^3}$. Then p , q and r satisfy the given conditions.

Let K be the compositum of K' and K'' , the unique subextensions of index p in $\mathbb{Q}(\zeta_{p^2q})/\mathbb{Q}(\zeta_{p^2})$ and $\mathbb{Q}(\zeta_{p^2r})/\mathbb{Q}(\zeta_{p^2})$ respectively. Then $m = p^2rq$, $a = 2$ and $L = \mathbb{Q}(\zeta_m) = K(\zeta_q) \otimes_K K(\zeta_r)$. Therefore, $F = \mathbb{Q}(\zeta_{p^4qr})$, and $G = \text{Gal}(F/K(\zeta_{qr})) \times \text{Gal}(F/K(\zeta_{p^4q})) \times \text{Gal}(F/K(\zeta_{p^4r}))$. We may choose σ so that $\langle \sigma \rangle = \text{Gal}(F/K(\zeta_{qr})) \cong G/C$ has order p^2 . The inertia subgroup of r in G is $\text{Gal}(F/K(\zeta_{p^4q}))$, which is generated by an element θ of order p .

Since $K = K' \otimes_{\mathbb{Q}(\zeta_{p^2})} K''$ and $K''/\mathbb{Q}(\zeta_{p^2})$ is totally ramified at r , we have that K'_r is the maximal unramified extension of K_r/\mathbb{Q}_r . It follows from $v_q(r^{p^2}-1) = 1$ and $v_q(r^p-1) = 0$ that $[\mathbb{Q}_r(\zeta_q) : \mathbb{Q}_r] = p^2$, and so $[K'_r : \mathbb{Q}_r] = p = f(K/\mathbb{Q}, r)$. Therefore $v_p(|W(K_r)|) = v_p(|W(\mathbb{Q}_r)|) + f(r) = v_p(r-1) + 1 = 3$, and so we have $v(r) = \max\{0, a + v_p(|\theta|) - v_p(|W(K_r)|)\} = 0$. Since $|C| = p$ and θ has order p , we also see that $\theta^{f(r)}C^{p^2}$ is trivial, so $v_p(|\theta^{f(r)}C^{p^2}|) = 0$.

Let ψ_r be the Frobenius automorphism of r in $\text{Gal}(F/\mathbb{Q})$. Then $\psi_r^p = \sigma^p \eta$, where $\eta \in B$ generates $\text{Gal}(F/K(\zeta_{p^4r}))$. Since $\langle \theta \rangle \cap \langle \eta \rangle = 1$, it follows from Lemma 9 that $h = v_p(|\theta|) = 1$. So case (2b) of Theorem 13 applies to show that $\beta_p(r) = h = 1$.

Acknowledgements

Research supported by the National Science and Engineering Research Council of Canada, UEFISCSU project ID 532, contract no. 29/28.09.2007, D.G.I. of Spain and Fundación Séneca of Murcia.

References

- [1] S.A. Amitsur, D. Saltman, Generic abelian crossed products and p -algebras, *J. Algebra* 51 (1978) 76–87.
- [2] M. Benard, M. Schacher, The Schur subgroup II, *J. Algebra* 22 (1972) 378–385.
- [3] G.J. Janusz, The Schur group of an algebraic number field, *Ann. of Math. (2)* 103 (1976) 253–281.
- [4] A. Herman, G. Olteanu, Á. del Río, The gap between the Schur group and the subgroup generated by cyclic cyclotomic algebras, preprint.
- [5] J.W. Pendergrass, The 2-part of the Schur group, *J. Algebra* 41 (1976) 422–438.
- [6] J.W. Pendergrass, The Schur subgroup of the Brauer group, *Pacific J. Math.* 69 (1977) 477–499.
- [7] J.-P. Serre, *Local Fields*, Springer, 1979.
- [8] T. Yamada, The Schur Subgroup of the Brauer Group, in: *Lecture Notes in Mathematics*, vol. 397, Springer-Verlag, 1974.