THE GAP BETWEEN THE SCHUR GROUP AND THE SUBGROUP GENERATED BY CYCLIC CYCLOTOMIC ALGEBRAS

ALLEN HERMAN, GABRIELA OLTEANU, AND ÁNGEL DEL RÍO

Abstract. Let K be an abelian extension of the rationals. Let $S(K)$ be the Schur group of K and let $CC(K)$ be the subgroup of $S(K)$ generated by classes containing cyclic cyclotomic algebras. We characterize when $CC(K)$ has finite index in $S(K)$ in terms of the relative position of K in the lattice of cyclotomic extensions of the rationals.

1. Introduction

Throughout this article, K is an abelian extension of the rationals, $Br(K)$ denotes the Brauer group of K and $S(K)$ the Schur subgroup of K. Recall that a *cyclotomic algebra* over K is a crossed product $(E/K, \alpha)$, where E/K is a finite cyclotomic extension and α is a factor set taking values in the group of roots of unity of E. If $(E/K, \alpha)$ is a cyclotomic algebra and the extension E/K is cyclic then we say that $(E/K, \alpha)$ is a *cyclic cyclotomic algebra*. Some properties of cyclic cyclotomic algebras with respect to ring isomorphism were studied in [HOR1].

It is well known that every element of $Br(K)$ is represented by a cyclic algebra over K and every element of $S(K)$ is represented by a cyclotomic algebra over K [Yam]. However, in general, not every element of $S(K)$ is represented by a cyclic cyclotomic algebra. In fact, as we will see in this paper, in general, $S(K)$ is not generated by classes represented by cyclic cyclotomic algebras.

Let $CC(K)$ denote the subgroup of $S(K)$ generated by classes containing cyclic cyclotomic algebras. In other words $CC(K)$ is formed by elements of $S(K)$ represented by tensor products of cyclic cyclotomic algebras. The aim of this article is to study the gap between $S(K)$ and $CC(K)$. More precisely, we give a characterization of when $CC(K)$ has finite index in $S(K)$ in terms of the relative position of K in the lattice of cyclotomic extensions of the rationals.

For every positive integer n, let ζ_n denote a complex primitive n-th root of unity. By the Benard-Schacher Theorem [BS], $S(K) = \bigoplus_p S(K)_p$, where p runs over the primes such that $\zeta_p \in K$ and $S(K)_p$ denotes the p-primary part of $S(K)$. Thus $CC(K)$ has finite index in $S(K)$ if and only if $CC(K)_p = CC(K) \cap S(K)_p$ has finite index in $S(K)_p$ for every prime p with $\zeta_p \in K$. Therefore, we are going to fix a prime p such that $\zeta_p \in K$ and our main result gives necessary and sufficient conditions for $[S(K)_p : CC(K)_p] < \infty$, in terms of the Galois group of a certain cyclotomic field F that we are going to introduce next.

Research supported by the National Science and Engineering Research Council of Canada, PN-II-ID-PCE-2007-1 project ID_532, contract no. 29/28.09.2007, D.G.I. of Spain and Fundación Séneca of Murcia.

Let $L = \mathbb{Q}(\zeta_m)$ be a minimal cyclotomic field containing K, a the maximum positive integer such that $\zeta_{p^a} \in K$, s the maximum positive integer such that $\zeta_{p^s} \in L$ and

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

where $v_p : \mathbb{Q} \to \mathbb{Z}$ denotes the p-adic valuation. Then we let $\zeta = \zeta_{p^{a+b}}$ and define $F = L(\zeta)$.

The Galois groups of F mentioned above are

$$\Gamma = \mathrm{Gal}(F/\mathbb{Q}), \quad G = \mathrm{Gal}(F/K), \quad C = \mathrm{Gal}(F/K(\zeta)) \quad \text{and} \quad D = \mathrm{Gal}(F/K(\zeta+\zeta^{-1})).$$

Notice that if $C \neq D$ then $p^a = 2$ and $\rho(\zeta) = \zeta^{-1}$ for every $\rho \in D \setminus C$. On the other hand $D \neq G$. Indeed, otherwise $\zeta_{p^{a+b}} + \zeta_{p^{a+b}}^{-1} = \zeta + \zeta^{-1} \in \mathbb{Q}(\zeta) \cap L = \mathbb{Q}(\zeta_{p^s})$. Since $a \geq 1$ and $b \geq s$, this implies that $p = 2$, $a = 1$ and $b = s$, in contradiction with the definition of b.

We need to fix elements ρ, σ of G, with $G = \langle \rho, \sigma, C\rangle$, such that $D = B \times \langle \rho \rangle$ and $C = B \times \langle \rho^2 \rangle$ for some subgroup B of C and $G/C = \langle \rho C \rangle \times \langle \sigma C \rangle$. Furthermore, if G/C is cyclic (equivalently $C = D$) then we select $\rho = 1$ and otherwise σ is selected so that $\sigma(\zeta_4) = \zeta_4$. The existence of such ρ and σ in G follows by standard arguments (see [Pen1, Lemma 1.4] or [HOR2, Lemma 3]).

The order of a group element g is denoted by $|g|$. Finally, to every $\psi \in \Gamma$ we associate two non-negative integers,

$$d(\psi) = \min\{a, \max\{h \geq 0 : \psi(\zeta_{p^h}) = \zeta_{p^h}\}\} \quad \text{and} \quad \nu(\psi) = \max\{0, a - v_p(|\psi G|)\},$$

and a subgroup of C:

$$T(\psi) = \{\eta \in B : \eta^{p^{\nu(\psi)}} \in B^{p^{d(\psi)}}\}.$$

Now we are ready to state our main result.

Theorem 1. *Let K be an abelian extension of the rationals, p a prime integer and use the above notation.*

If G/C is cyclic then the following are equivalent.

1. *$CC(K)_p$ has finite index in $S(K)_p$.*
2. *For every $\psi \in \Gamma_p$ one has* $\psi^{|\psi G|} \in \bigcup_{i=0}^{|\sigma C|-1} \sigma^i T(\psi)$.
3. *For every $\psi \in \Gamma_p$ satisfying $\nu(\psi) < \min\{v_p(\exp B), d(\psi)\}$, one has* $\psi^{|\psi G|} \in \bigcup_{i=0}^{|\sigma C|-1} \sigma^i T(\psi)$.

If G/C is non-cyclic then the following are equivalent:

1. *$CC(K)_2$ has finite index in $S(K)_2$.*
2. *For every $\psi \in \Gamma_2 \setminus G$, if $d = v_2([K \cap \mathbb{Q}(\zeta) : \mathbb{Q}]) + 2$ then*

$$\psi^{|\psi G|} \in \mathrm{Gal}(F/\mathbb{Q}(\zeta_{2^{d+1}})) \cap \left(\bigcup_{i=0}^{|\sigma C|-1} \sigma^i \langle \rho, T(\psi) \rangle \right).$$

Notice that conditions (2) and (3) in Theorem 1 can be verified by elementary computations in the Galois group Γ.

2. The subgroup of $S(K)$ generated by cyclic cyclotomic algebras

In this section we provide some information on the structure of $CC(K)_p$. We start by introducing some notation and recalling some known facts about local information concerning $S(K)$.

The group of roots of unity of a field E is denoted by $W(E)$. If A is a central simple K-algebra then $[A]$ denotes the class in the Brauer group of K containing A. By a crossed product algebra we mean an associative algebra $A = (E/K, \alpha) = \bigoplus_{\pi\in \mathrm{Gal}(E/K)} Eu_\pi$, where E/K is a finite Galois extension, $\alpha : \mathrm{Gal}(E/K) \times \mathrm{Gal}(E/K) \to E^*$ is a map, $\{u_\pi : \pi \in \mathrm{Gal}(E/K)\}$ is an E-basis of units of A and the product in A is determined by the rules: $u_\pi u_\tau = \alpha_{\pi,\tau} u_{\pi\tau}$ and $u_\pi a = \pi(a)u_\pi$. The map α is called the *factor set* of the crossed product and the basis $\{u_\pi : \pi \in \mathrm{Gal}(E/K)\}$ is called a *crossed section* of the crossed product. Replacing each element u_π of a crossed section by $v_\pi = \lambda_\pi u_\pi$, for λ_π a non-zero element of E gives rise to another crossed section of the crossed product which yields a different factor set. This change of crossed section is called a *diagonal change of basis*. A *cyclotomic algebra* over K is a crossed product algebra $(E/K, \alpha)$ for which E/K is a finite cyclotomic extension and the factor set α takes values in $W(E)$. When $\mathrm{Gal}(E/K) = \langle\tau\rangle$ is a cyclic group, there exists a diagonal change of basis for which $u_{\tau^i} = u_\tau^i$, for every $0 \le i \le |\tau|$, and hence the corresponding factor set is determined by $u_\tau^{|\tau|} = \zeta \in K^*$. The corresponding crossed product algebra is called a *cyclic algebra*, which we will denote by $(E/K, \zeta)$.

Let $\mathbb{P} = \{r \in \mathbb{N} : r \text{ is prime}\} \cup \{\infty\}$. Given $r \in \mathbb{P}$, 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:

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

Since E/K is a finite Galois extension and A has uniformly distributed invariants, $e(E/K, r)$, $f(E/K, r)$ and $m_r(A)$ do not depend on the selection of the prime of K dividing r (see [Ser] and [Ben]).

We also use the following notation, for $\pi \subseteq \mathbb{P}$ and $r \in \mathbb{P}$:

$$\begin{aligned} S(K,\pi) &= \{[A]\in S(K) : m_r(A)=1, \text{ for each } r\in\mathbb{P}\setminus\pi\},\\ S(K,r) &= S(K,\{r\}),\\ CC(K,\pi) &= CC(K)\cap S(K,\pi),\\ CC(K,r) &= CC(K)\cap S(K,r),\\ \mathbb{P}_p &= \left\{r\in\mathbb{P}\setminus\{\infty\} : CC(K,\{r,\infty\})_p = CC(K,r)_p \bigoplus CC(K,\infty)_p\right\}.\end{aligned}$$

If p is odd or $\zeta_4 \in K$ then $m_\infty(A) = 1$ for each Schur algebra A and so $\mathbb{P}_p = \mathbb{P} \setminus \{\infty\}$.

Finally, if r is odd then we set

$$\nu(r) = \max\{0, a + v_p(e(K(\zeta_r)/K, r)) - v_p(|W(K_r)|)\}.$$

The following theorem provides information on the structure of $CC(K)_p$.

Theorem 2.1. *For every prime p we have*

$$CC(K)_p = \left(\bigoplus_{r\in\mathbb{P}_p} CC(K,r)_p\right) \bigoplus \left(\bigoplus_{r\in\mathbb{P}\setminus\mathbb{P}_p} CC(K,\{r,\infty\})_p\right).$$

Let X_r denote the direct summand labelled by r in the previous decomposition, that is

$$X_r = \begin{cases} CC(K,r)_p, & \text{if } r\in\mathbb{P}_p; \\ CC(K,\{r,\infty\})_p, & \text{if } r\in\mathbb{P}\setminus\mathbb{P}_p \end{cases}$$

Then we have

1. *If r is odd then X_r is cyclic of order $p^{\nu(r)}$ and it is generated by the class of $(K(\zeta_r)/K,\zeta_{p^a})$.*
2. *X_2 has order 1 or 2 and if it has order 2 then $p^a = 2$ and X_2 is generated by the class of $(K(\zeta_4)/K,-1)$.*
3. *If $X_\infty \neq 1$, then $p=2$, $K\subseteq\mathbb{R}$, and X_∞ has exponent 2.*

Proof. Let $A = (E/K,\xi)$ be a cyclic cyclotomic algebra with $[A]\in S(K)_p$. One may assume without loss of generality that $\xi\in W(K)_p$. For every subextension M of E/K let M' denote the maximal subextension of M/K of degree a power of p. Since E/K is cyclic, the subextensions of E/K of degree a power of p are linearly ordered. This implies that $E' = K(\zeta_{r^k})'$ for some prime r and integer k. Furthermore, if $\ell = [E:K(\zeta_{r^k})]$, then $[A^{\otimes \ell}] = [(E/K,\xi^\ell)] = [(K(\zeta_{r^k})/K,\xi)]$. Since ℓ is coprime to p, $m_q(A) = m_q(A^{\otimes\ell}) = m_q(K(\zeta_{r^k})/K,\xi)$, for every $q\in\mathbb{P}$. If $q\notin\{r,\infty\}$ then $K(\zeta_{r^k})/K$ is unramified at q and therefore $m_q(A)=1$ [Rei, pg. 67, Exercise 16]. Thus $[A]\in CC(K,\{r,\infty\})$. This shows that $CC(K)_p = \sum_{r\in\mathbb{P}\setminus\{\infty\}} CC(K,\{r,\infty\})_p$.

If $\mathbb{P}\setminus\{\infty\} = \mathbb{P}_p$ then this implies that

$$CC(K)_p = \bigoplus_{r\in\mathbb{P}} CC(K,r) = \left(\bigoplus_{r\in\mathbb{P}_p} CC(K,r)\right)\bigoplus CC(K,\infty)$$

as wanted. Assume otherwise that $\mathbb{P}\setminus\{\infty\}\neq\mathbb{P}_p$. If $1\neq[A]\in CC(K,\infty)$ then for every $r\in\mathbb{P}$ and $[B]\in CC(K,\{r,\infty\})\setminus CC(K,r)$ one has $[B] = [A\otimes B]\cdot[A]$ and $[A\otimes B]\in CC(K,r)$, because $Br(K_\infty)$ has order 2. This implies that $CC(K,\{r,\infty\}) = CC(K,r)\bigoplus CC(K,\infty)$, contradicting the hypothesis. Hence $CC(K,\infty)=1$ and then

$$CC(K)_p = \left(\bigoplus_{r\in\mathbb{P}_p} CC(K,r)_p\right) \bigoplus \left(\bigoplus_{r\in\mathbb{P}\setminus\mathbb{P}_p} CC(K,\{r,\infty\})_p\right)$$

as desired.

(1). Let $r\in\mathbb{P}$. The map $K_r\otimes_K - : X_r\to S(K_r)$ is an injective group homomorphism. If r is odd then $S(K_r)$ is cyclic of order $e(K(\zeta_r)/K,r)$ and it is generated by the cyclic algebra $(K_r(\zeta_r)/K_r,\zeta_n)$, where $n = |W(K_r)|$ (see e.g. [Yam]). Therefore X_r is cyclic and hence it is generated by a class containing a cyclic cyclotomic algebra A. As above we may assume that $A = (K(\zeta_{r^k})/K,\zeta_{p^a}^\ell)$ for some $k,\ell\geq 1$. Since $[A] = [(K(\zeta_{r^k})/K,\zeta_{p^a})]^\ell$, one may assume that $\ell = 1$. Then $|X_r| = m_r(A) = m_r((K(\zeta_{r^k})'/K,\zeta_{p^a})) = m_r((K(\zeta_r)/K,\zeta_{p^a})) = m((K_r(\zeta_r)/K_r,\zeta_{p^a})) = m((K_r(\zeta_r)/K_r,\zeta_{p^{a+a(r)}})^{\otimes a(r)}) = p^{\nu(r)}$, where $a+a(r) = v_p(n)$. This proves (1).

(2) and (3) follow by similar or standard arguments. □

Remark 2.2. Notice that the proof of Theorem 2.1 shows that if A is a cyclic cyclotomic algebra of index a power of p then $[A] \in S(K, \{r, \infty\})$ for some prime $r \in \mathbb{P} \setminus \{\infty\}$ and if p is odd or $\zeta_4 \in K$ then $[A] \in S(K, r)$.

By Theorem 2.1, if r is odd then $\nu(r) = \max\{v_p(m_r(A)) : [A] \in CC(K)_p\}$. We can extend the definition of $\nu(r)$ by setting $\nu(2) = \max\{v_p(m_2(A)) : [A] \in CC(K)_p\}$. Notice that $\nu(2) \leq 1$ and $\nu(2) = 1$ if and only if $p^a = 2$ and $(K(\zeta_4)/K, -1)$ is non-split. We will need to compare $\nu(r)$ to

$$\beta(r) = \max\{v_p(m_r(A)) : [A] \in S(K)_p\}.$$

Recall that $S(K_r)$ is finite (see e.g. [Yam]) and so $\beta(r) < \infty$.

A consequence of Theorem 2.1 is the following.

Corollary 2.3. *Let $r \in \mathbb{P}$. Then*

1. *$CC(K)_p = S(K)_p$ if and only if $\nu(r) = \beta(r)$ for each $r \in \mathbb{P} \setminus \{\infty\}$.*
2. *$CC(K)_p$ has finite index in $S(K)_p$ if and only if $\nu(r) = \beta(r)$ for all but finitely many primes r.*

Proof. We prove (2) and let the reader to adapt the proof to show (1).

Assume that $CC(K)_p$ has finite index in $S(K)$ and let $[A_1], \dots, [A_n]$ be a complete set of representatives of cosets modulo $CC(K)_p$. Then $\pi = \{r \in \mathbb{P} : m_r(A_i) \neq 1 \text{ for some } i\}$ is finite and $\nu(r) = \beta(r)$ for every $r \in \mathbb{P} \setminus \pi$. Conversely, assume that $\nu(r) = \beta(r)$ for every $r \in \mathbb{P} \setminus \pi$, with π a finite subset of $\mathbb{P}$ containing ∞. Then $S(K, \pi)_p$ is finite and we claim that $S(K)_p = S(K, \pi)_p + CC(K)_p$. Let $[B] \in S(K)_p$. We prove that $[B] \in S(K, \pi)_p + CC(K)_p$ by induction on $h(B) = \prod_{r \in \mathbb{P} \setminus \pi} m_r(B)$. If $h(B) = 1$ then $[B] \in S(K, \pi)_p$ and the claim follows. Assume that $h(B) > 1$ and the induction hypothesis. Then there is a cyclic cyclotomic algebra A and $r \in \mathbb{P} \setminus \pi$ such that $m_r(B) = m_r(A) > 1$. Since $S(K_r)$ is cyclic, there is a positive integer ℓ coprime to $m_r(B)$ such that $(A^{\otimes \ell}) \otimes_K K_r \cong B \otimes_K K_r$ as K_r-algebras. Let $C = (A^{\text{op}})^{\otimes \ell} \otimes B$. Since $A^{\otimes \ell} \in CC(K, \{r, \infty\})_p$, it follows that $h(C) = \frac{h(B)}{m_r(A)} < h(B)$, and hence $[C] \in S(K, \pi)_p + CC(K)_p$, by the induction hypothesis. Therefore, $[B] = [A]^\ell [C] \in S(K, \pi)_p + CC(K)_p$, as required. $\square$

Notice that for p odd Corollary 2.3 is a straightforward consequence of the decomposition of $CC(K)_p$ given in Theorem 2.1 and the Janusz Decomposition Theorem [Jan2].

3. Examples

In this section we present several examples comparing $S(K)$ and $CC(K)$ for various fields. We use the standard notation for the generalized quaternion algebra:

$$\left(\frac{a, b}{K}\right) = K[i, j | i^2 = a, j^2 = b, ji = -ij, a, b \in K^*] \quad \text{and} \quad \mathbb{H}(K) = \left(\frac{-1, -1}{K}\right).$$

Example 3.1. $K = \mathbb{Q}$.

It follows from the Hasse–Brauer–Noether–Albert Theorem that $CC(\mathbb{Q}, r)$ is trivial for all primes r. The cyclic cyclotomic algebra $\mathbb{H}_{2,\infty} = \mathbb{H}(\mathbb{Q}) = (\mathbb{Q}(\zeta_4)/\mathbb{Q}, -1)$ is a rational quaternion algebra which lies in $CC(\mathbb{Q},\{2,\infty\})$. When r is odd, the cyclic algebra $\mathbb{H}_{r,\infty} = (\mathbb{Q}(\zeta_r)/\mathbb{Q}, -1)$ has real completion $\mathbb{R}\otimes_{\mathbb{Q}}\mathbb{H}_{r,\infty} \simeq M_n(\mathbb{H}(\mathbb{R}))$, for $n=\frac{r-1}{2}$, so $m_\infty(\mathbb{H}_{r,\infty})=2$. The extension $\mathbb{Q}_r(\zeta_r)/\mathbb{Q}_r$ is unramified at primes other than r, so $[\mathbb{H}_{r,\infty}]\in CC(\mathbb{Q},\{r,\infty\})$ (and $m_r(\mathbb{H}_{r,\infty})$ must be 2). If r and q are distinct finite primes, then $[\mathbb{H}_{r,\infty}][\mathbb{H}_{q,\infty}]$ is an element of $CC(\mathbb{Q},\{r,q\})$, and it follows from Remark 2.2 that this element cannot be represented by a cyclic cyclotomic algebra. Nevertheless, it is easy to see at this point that $S(\mathbb{Q}) = CC(\mathbb{Q})$.

The smallest example of an algebra representing an element in $CC(\mathbb{Q},\{2,3\})$ is the generalized quaternion algebra $\left(\frac{-3,2}{\mathbb{Q}}\right)$. The algebra of 2×2 matrices over $\left(\frac{-3,2}{\mathbb{Q}}\right)$ is isomorphic to a simple component of the rational group algebra of the group of order 48 that has the following presentation $\langle x,y,z : x^{12}=y^2=z^2=1, x^y=x^5, x^z=x^7, [y,z]=x^9\rangle$.

Example 3.2. *$CC(K,\infty)\neq 1$.*

It is also possible that $CC(K,\infty)$ is non-trivial. For example, $\mathbb{H}(\mathbb{Q}(\sqrt{2})) = (\mathbb{Q}(\zeta_8)/\mathbb{Q}(\sqrt{2}),-1)$ is homomorphic to a simple component of the rational group algebra of the generalized quaternion group of order 16. It has real completion isomorphic to $\mathbb{H}(\mathbb{R})$ at both infinite primes of $\mathbb{Q}(\sqrt{2})$, so $m_\infty(\mathbb{H}(\mathbb{Q}(\sqrt{2})))=2$. If r is an odd prime then $m_r(\mathbb{H}(\mathbb{Q}(\sqrt{2})))=1$. Since $\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2$ is ramified and the sum of the local invariants at infinite primes is an integer, we deduce that $m_2(\mathbb{H}(\mathbb{Q}(\sqrt{2})))=1$, so it follows that $[\mathbb{H}(\mathbb{Q}(\sqrt{2}))]\in CC(\mathbb{Q}(\sqrt{2}),\infty)$.

Example 3.3. *Cyclotomic fields.*

Suppose $K=\mathbb{Q}(\zeta_m)$ for some positive integer $m>2$. Assume that either m is odd or $4|m$. The main theorem of [Jan3] shows that if p is a prime dividing m and $m=p^n m_0$ with m_0 coprime to p, then

$$S(\mathbb{Q}(\zeta_m))_p = \{[A\otimes_{\mathbb{Q}(\zeta_{p^n})}\mathbb{Q}(\zeta_m)] : [A]\in S(\mathbb{Q}(\zeta_{p^n}))_p\}.$$

When $p^n>2$, we know by [BS, Theorem 3] that $S(\mathbb{Q}(\zeta_{p^n}))_p$ is generated by the Brauer classes of characters of certain metacyclic groups, which, in their most natural crossed product presentation, take the form of cyclic cyclotomic algebras. Therefore, $S(\mathbb{Q}(\zeta_{p^n}))_p = CC(\mathbb{Q}(\zeta_{p^n}))_p$. Since it is easy to see that when K is an extension of a field E, $\{[A\otimes_E K] : [A]\in CC(E)\}\subseteq CC(K)$, we can conclude that $S(\mathbb{Q}(\zeta_m)) = CC(\mathbb{Q}(\zeta_m))$ for all positive integers m.

Combining Corollary 2.3 with the results of [Jan2] one can obtain examples with $S(K)_p\neq CC(K)_p$.

Example 3.4. *$CC(K)_p\neq S(K)_p$, p odd.*

By Theorem 2.1, if $CC(K)_p = S(K)_p$ then $S(K)_p=\bigoplus_{r\in\mathbb{P}} S(K,r)_p$. However Proposition 6.2 of [Jan2] shows that for every odd prime p there are infinitely many abelian extensions K of $\mathbb{Q}$ such that $S(K)_p\neq\bigoplus_{r\in\mathbb{P}} S(K,r)_p$. Thus for such fields K one has $S(K)_p\neq CC(K)_p$.

Example 3.5. *$CC(K)_2\neq S(K)_2$ with $\zeta_4\in K$.*

Let q be a prime of the form $1+5\cdot 2^9 t$ with $(t,10)=1$. In the last section of [Jan3] one constructs a subfield K of $\mathbb{Q}(\zeta_{2^9\cdot 5\cdot q})$ such that $\max\{m_q(A) : [A]\in S(K)_2\}=4$ (in particular $\zeta_4\in K$), and for every $[A]\in S(K)_2$ with $m_q(A)=4$, one has $m_r(A)\neq 1$, for some prime r not dividing $10q$. In the notation of Corollary 2.3 this means that $v_2(|S(K,q)|) < \beta(q) = 4$ (for $p = 2$). Then $S(K)_2 \neq \bigoplus_{r\in\mathbb{P}} S(K,r)_2$ and, as in Example 3.4, this implies that $CC(K)_2 \neq S(K)_2$.

Example 3.6. *$CC(K)_2 \neq S(K)_2$ with $\zeta_4 \notin K$.*

An example with $S(K)_2 \neq CC(K)_2$ and $\zeta_4 \notin K$ can be obtained using Theorem 5 of [Jan1]. This result gives necessary and sufficient conditions for $S(k)$ to have order 2 when k is a cyclotomic extension of $\mathbb{Q}_2$. This is the maximal 2-local index for a Schur algebra. If $|S(k)| = 2$ then $\zeta_4 \notin k$. If, moreover, $\mathbb{H} = (k(\zeta_4)/k, -1)$ is not split then $CC(k)_2 = S(k)_2$, because $\mathbb{H}$ is a cyclic cyclotomic algebra. However, there are some fields k for which $|S(k)| = 2$ and $\mathbb{H}$ is split. In that case $S(k)$ is generated by the class of a cyclotomic algebra A and we are going to show that $CC(k) \neq S(k)$. Then for any algebraic number field with $K_2 = k$ we will also have $CC(K)_2 \neq S(K)_2$.

Indeed, if $CC(k) = S(k)$ then A is equivalent to a cyclic cyclotomic algebra $(k(\zeta_m)/k, \zeta)$. One may assume that $\zeta \in W(k)_2 \setminus \{1\}$ and hence $\zeta = -1$, because $\zeta_4 \notin k$. Write $m = 2^{v_2(m)}m'$, with m' odd. Since $k(\zeta_m)/k$ must be ramified, $v_2(m) \geq 2$. If $k(\zeta_{m'})/k$ has even degree then this would contradict the fact that $k(\zeta_m)/k$ is cyclic. So $k(\zeta_{m'})/k$ has odd degree and therefore $(k(\zeta_m)/k, -1)$ is equivalent to $(k(\zeta_{2^{v_p(m)}})/k, -1)$ by [Rei, (30.10)]. Then A is equivalent to $(k(\zeta_4)/k, -1)$ by [Jan1, Theorem 1], yielding a contradiction.

4. Finiteness of $S(K)_p/CC(K)_p$

In this section we prove Theorem 1. The main idea is to compare $\nu(r)$ and $\beta(r)$ for odd primes r not dividing m. We will use the notation introduced in sections 1 and 2 including the Galois groups Γ, G, C, D, and B, the elements $\rho, \sigma \in G$, and the decompositions $D = \langle\rho\rangle \times B$ and $C = \langle\rho^2\rangle \times B$.

We also use the following numerical notation for every odd prime r not dividing m:

$$\begin{aligned} a + a(r) &= v_p(|W(K_r)|), \\ d(r) &= \min\{a, v_p(r-1)\}, \\ f_r &= f(K/\mathbb{Q}, r), \\ f(r) &= v_p(f_r), \end{aligned}$$

and introduce $\psi_r \in \Gamma$ and $\phi_r \in G$ as follows:

$$\psi_r(\varepsilon) = \varepsilon^r \text{ for every root of unity } \varepsilon \in F, \quad \text{and} \quad \phi_r = \psi_r^{f_r}.$$

The order of ψ_r modulo G is f_r, and ψ_r and ϕ_r are Frobenius automorphisms at r in Γ and G respectively. By the uniqueness of an unramified extension of a local field of given degree, one has $v_p(|W(K_r)|) = v_p(|W(\mathbb{Q}_r)|) + f(r) = v_p(e(K(\zeta_r)/K, r)) + f(r)$. Thus

$$\nu(r) = \max\{0, a - f(r)\}. \tag{1}$$

This gives $\nu(r)$ in terms of the numerical information associated to r. Next we quote a result from [HOR2] which gives the value of $\beta(r)$. This result was obtained by Janusz [Jan2, Theorem 3] in the case when p is odd or $\zeta_4 \in K$. The remaining case was considered by Pendergrass in [Pen1], but the results there were based on incorrect calculations involving factor sets (see [HOR2]).

Theorem 4.1. *Let r be an odd prime not dividing m and use the above notation. Let $\phi_r = \psi_r^{f_r} = \rho^{j'}\sigma^j\eta$, with $\eta \in B$, $0 \le j' < |\rho|$ and $0 \le j < |\sigma C|$.*

(1) *If G/C is non-cyclic (and hence $p^a = 2$) and $j \not\equiv j' \mod 2$, then $\beta(r) = 1$.*
(2) *Otherwise $\beta(r) = \max\{\nu(r), v_p(|\eta B^{p^{d(r)}}|)\}$.*

We will need the following lemma.

Lemma 4.2. *$\nu(r)$ and $\beta(r)$ depend only on $d(r)$ and the element $\psi_r \in \Gamma$.*

Proof. $\nu(r)$ is determined by $f(r)$ (see (1)), and $f(r)$ by $f_r = |\psi_r G|$. So $\nu(r)$ is determined by ψ_r. On the other hand, $\psi_r = \rho^{j'}\sigma^j\eta$ for uniquely determined integers $0 \le j' < |\rho|$, $0 \le j < |\sigma C|$ and $\eta \in B$. Therefore, ψ_r determines whether or not $j \equiv j' \mod 2$, and also the element η required in Theorem 4.1. So knowing ψ_r and $d(r)$ will allow one to compute $\beta(r)$. □

We can now give a necessary and sufficient condition, in local terms, for $CC(K)_p$ to have finite index in $S(K)_p$.

Theorem 4.3. *$CC(K)_p$ has finite index in $S(K)_p$ if and only if $\nu(r) = \beta(r)$ for all odd primes r not dividing m.*

Proof. The sufficiency is a consequence of Corollary 2.3.

Suppose that there is an odd prime r not dividing m for which $\nu(r) < \beta(r)$. By Dirichlet's Theorem on primes in arithmetic progression there are infinitely many primes r' such that $r' \equiv r \mod \operatorname{lcm}(m, p^{a+b}, p^{v_p(r-1)+1})$. For such an r' one has $\psi_{r'} = \psi_r$ and $v_p(r'-1) = v_p(r-1)$. Then $\beta(r') = \beta(r) > \nu(r) = \nu(r')$ for infinitely many primes r', by Lemma 4.2, and hence $[S(K)_p : CC(K)_p] = \infty$, by Corollary 2.3. □

When p is odd, this result can be interpreted in terms of the local subgroups of $S(K)_p$ and $CC(K)_p$.

Theorem 4.4. *Let K be a subfield of $\mathbb{Q}(\zeta_n)$ and p an odd prime and n a positive integer. Then the following conditions are equivalent:*

(1) *$CC(K)_p$ has finite index in $S(K)_p$.*
(2) *$CC(K,r)_p = S(K,r)_p$, for almost all $r \in \mathbb{P}$.*
(3) *$CC(K,r)_p = S(K,r)_p$, for every prime r not dividing n.*

Proof. By the Janusz Decomposition Theorem [Jan2], we have

$$S(K)_p = S(K,\pi)_p \bigoplus \left(\bigoplus_{r \notin \pi} S(K,r)_p \right),$$

where π is the set of prime divisors of m, the smallest integer for which $K \subseteq \mathbb{Q}(\zeta_m)$. This shows that $\beta(r) = v_p(|S(K,r)|_p)$, whenever r is a prime that does not divide m and hence, for such primes $\nu(r) = \beta(r)$ if and only if $CC(K,r)_p = S(K,r)_p$. Now the results follows from Corollary 2.3 and Theorem 4.3. □

An obvious consequence of Theorem 4.4 is the following:

Corollary 4.5. *If K is a subfield of $\mathbb{Q}(\zeta_n)$ and p is an odd prime then the order of the group $\bigoplus_{r\in\mathbb{P},r\nmid n} S(K,r)_p/CC(K,r)_p$ is either 1 or infinity.*

We now proceed with the proof of the main theorem.

Proof of Theorem 1. For each $\psi \in \Gamma$ we put $h(\psi) = \max\{0 \le h \le a+b : \psi(\zeta_{p^h}) = \zeta_{p^h}\}$. Clearly $d(\psi) = \min\{a, h(\psi)\}$. By Dirichlet's Theorem on primes in arithmetic progression, for every $\psi \in \Gamma$ there exists an odd prime r not dividing m such that $\psi = \psi_r$. For such a prime one has $h(\psi) = \min\{a+b, v_p(r-1)\}$. This prime r can be selected so that $h(\psi) = v_p(r-1)$, because otherwise we would have $h(\psi) = a+b < v_p(r-1)$, and we could replace r by a prime r' satisfying $r' \equiv r \mod m$ and $r' \equiv 1 + p^{a+b} \mod p^{a+b+1}$. For such an r', one has $d(r) = d(r')$, and thus $\nu(r) = \nu(r')$ and $\beta(r) = \beta(r')$ by Lemma 4.2.

Let $q = |\sigma C|$.

We now consider the case when G/C is cyclic. Then $D = C = B$ and $\rho = 1$. We set $t = v_p(\exp(B))$. If $t = 0$, then $T(\psi) = B$ for every $\psi \in \Gamma_p$, so that (2) and (3) obviously hold. Furthermore $|\eta B^{p^{d(r)}}| = 1$ and so $\nu(r) = \beta(r)$ for all odd primes r not dividing m, by Theorem 4.1. So (1) holds by Theorem 4.3. So to avoid trivialities we assume that $t > 0$.

(1) implies (2). Suppose K does not satisfy condition (2) and let $\psi \in \Gamma_p$ with $\psi^{|\psi G|} \notin \bigcup_{j=0}^{q-1} \sigma^i T(\psi)$. Let r be an odd prime not dividing m for which $\psi = \psi_r$ and $h(\psi) = v_p(r-1)$. Then $d(r) = d(\psi)$ and $p^{f(r)} = f_r = |\psi G|$, so $\nu(r) = \nu(\psi)$. The assumption $\psi^{|\psi G|} \notin \bigcup_{j=0}^{q-1} \sigma^i T(\psi)$ means that when we express $\psi^{|\psi G|}$ as $\sigma^j \eta$ with $0 \le j < q$ and $\eta \in B$, the order of $\eta B^{p^{d(\psi)}}$ in $B/B^{p^{d(\psi)}}$ is strictly greater than $p^{\nu(\psi)} = p^{\nu(r)}$. By Theorem 4.1, we have $\beta(r) > \nu(r)$ for this odd prime r not dividing m, and so Theorem 4.3 implies that (1) fails.

(2) implies (3) is obvious.

(3) implies (1). Assume that (1) fails. Then, by Theorem 4.3, there exists a prime r not dividing m for which $\beta(r) > \nu(r)$. As above, we may select such an r so that $v_p(r-1) \le a+b$.

Let $\psi = \psi_r$. Our choice of r implies that $d(\psi) = d(r)$. We claim that one can assume $\psi \in \Gamma_p$. If $\psi \notin \Gamma_p$, then let ℓ be the least positive integer such that ψ^ℓ lies in Γ_p. Let r' be a prime integer such that $r' \equiv r^\ell \mod \operatorname{lcm}(m, p^{a+b})$. Since ℓ is coprime to p, we have $v_p(r'-1) = v_p(r^\ell - 1) = v_p(r-1)$ and therefore $d(\psi^\ell) = d(r') = d(r) = d(\psi)$. Since $\psi_{r'} = \psi_r^\ell$ and ℓ is coprime to p, we also have $f(r') = f(r) = f(\psi)$. It follows from Lemma 4.2 that $\beta(r) = \beta(r')$ and $\nu(r) = \nu(r')$. So by replacing r by r' if necessary, one may assume that $\psi \in \Gamma_p$ and $d(\psi) = d(r)$.

For this prime r and element $\psi = \psi_r \in \Gamma_p$, the assumption $\beta(r) > \nu(r)$ and Theorem 4.1 imply that, when we write $\phi_r = \psi^{f_r} = \sigma^j \eta$, with $0 \le j < q$ and $\eta \in B$, the order of $\eta B^{p^{d(r)}}$ in $B/B^{p^{d(r)}}$ is precisely $p^{\beta(r)}$. Then $\eta^{p^{\nu(r)}} \notin B^{p^{d(r)}}$, equivalently $\eta \notin T(\psi)$ and hence $\psi^{|\psi G|} \notin \bigcup_{j=0}^{q-1} \sigma^i T(\psi)$.

Since the exponent of $B/B^{p^{d(r)}}$ is precisely p^k, where $k = \min\{t, d(r)\}$, this can only be possible if $\nu(\psi) = \nu(r) < k = \min\{t, d(\psi)\}$. This shows that if condition (1) fails, then condition (3) also fails. This completes the proof in the case that G/C is cyclic.

Now suppose G/C is non-cyclic. In particular, $p^a = 2$ and $\sigma(\zeta_4) = \zeta_4$. Let $d = v_2([K \cap \mathbb{Q}(\zeta) : \mathbb{Q}]) + 2$ and let c be an integer such that $\sigma(\zeta) = \zeta^c$. Then $v_p(c-1) = d$ and $d(\psi) = 1$ for all $\psi \in \Gamma_2$.

(1) implies (2). Suppose (2) fails. Then there exists a $\psi \in \Gamma_2 \setminus G$ such that either $\psi^{|\psi G|} \notin \mathrm{Gal}(F/\mathbb{Q}(\zeta_{2^{d+1}}))$ or $\psi^{|\psi G|} \notin \bigcup_{i=0}^{q-1} \sigma^i \langle \rho, T(\psi)\rangle$.

As above, there exists an odd prime r not dividing m such that $\psi = \psi_r$, $|\psi G| = f_r$, and $\nu(\psi) = \nu(r)$. Since $\psi \notin G$ we have $f(r) > 0$ and so $\nu(r) = 0$, by (1). Also from $f(r) > 0$ one deduces that $\phi_r = \psi^{f_r}$ fixes ζ_4 and so when we write $\phi_r = \rho^{j'}\sigma^j\eta$ with $0 \le j' < |\rho|$, $0 \le j \le q$, $\eta \in B$, we have that j' is even.

If $\phi_r \notin \mathrm{Gal}(F/\mathbb{Q}(\zeta_{2^{d+1}}))$, then j is odd, and we are in the case of Theorem 4.1, part (1), with $\nu(r) = 0$ and $\beta(r) = 1$. Otherwise j is even and $\psi^{|\psi G|} \notin \bigcup_{i=0}^{q-1} \sigma^i \langle \rho, T(\psi)\rangle$. Then $\eta \notin T(\psi)$, or equivalently, $\nu(r) < v_2(|\eta B^2|)$ (observe that $d(r) = 1$). By Theorem 4.1, we have $\beta(r) = v_2(|\eta B^2|) > \nu(r)$. Therefore, in all cases in which (2) fails, we have $\nu(r) < \beta(r)$. So (1) fails by Theorem 4.3.

(2) implies (1). Suppose (1) fails. By Theorem 4.3, there exists an odd prime r not dividing m such that $0 = \nu(r) < \beta(r) = 1$. Since $\nu(r) = 0$, we must have $f(r) > 0$, so $\psi = \psi_r \notin G$. As above, we may adjust ψ_r by an odd power and make a different choice of r without changing $\nu(r)$ or $\beta(r)$ in order to arrange that $\psi \in \Gamma_2$. Write $\phi_r = \psi^{f_r} = \psi^{|\psi G|} = \rho^{j'}\sigma^j\eta$, with $0 \le j' < |\rho|$, $0 \le j < q$ and $\eta \in B$. As above, j' is even because $f(r) > 0$. If j is odd, then $\psi^{|\psi G|} \notin \mathrm{Gal}(F/\mathbb{Q}(\zeta_{2^{d+1}}))$ and so (2) fails. Suppose now that j is even, so we have $\psi^{|\psi G|} \in \mathrm{Gal}(F/\mathbb{Q}(\zeta_{2^{d+1}}))$. Then the fact that $\beta(r) = 1$ implies by Theorem 4.1, part (2), that $|\eta B^{2^{d(r)}}| = 2$. Since $d(r) \le a = 1$, we have $d(\psi) = d(r) = 2$ and so $\eta \notin B^2$ and $\eta \notin T(\psi)$. Then $\psi^{|\psi G|} \notin \prod_{i=0}^{q-1} \sigma^i \langle \rho, T(\psi)\rangle$ and so (2) fails. □

Some obvious consequences of Theorem 1 are the following.

Corollary 4.6. *If $\psi^{|\psi G|} \notin \langle \sigma, \rho, T(\psi)\rangle$, for some $\psi \in \Gamma_p$, then $CC(K)_p$ does not have finite index in $S(K)_p$.*

Corollary 4.7. *If G/C is cyclic and $\nu(\psi) \ge \min\{v_p(\exp B), d(\psi)\}$ for all $\psi \in \Gamma_p$, then $CC(K)_p$ has finite index in $S(K)_p$.*

Corollary 4.8. *If G/C is cyclic and $v_p(\exp B) + v_p(\exp(\mathrm{Gal}(K/\mathbb{Q}))) \le a$ then $CC(K)_p$ has finite index in $S(K)_p$.*

Proof. If $\psi \in \Gamma_p$ then $v_p(|\psi G|) \le v_p(\exp(\mathrm{Gal}(K/\mathbb{Q}))) \le a - v_p(\exp B)$, by assumption. Therefore $\nu(\psi) = \max\{0, a - v_p(|\psi G|)\} \ge v_p(\exp B)$ and Corollary 4.7 applies. □

Example 4.9. *A simple example with $[S(K)_p : CC(K)_p] = \infty$.*

Let p and q be odd primes with $v_p(q-1) = 2$. Let K be the subextension of $L = \mathbb{Q}(\zeta_{pq})/\mathbb{Q}(\zeta_p)$ with index p in $\mathbb{Q}(\zeta_{pq})$. Then $F = \mathbb{Q}(\zeta_{p^2q})$, $G \cong \langle\theta\rangle \times C$ is elementary abelian of order p^2, and Γ_p has an element ψ such that ψ^p generates C. Then $a = v_p(|\psi G|) = 1$ and so $\nu(\psi) = 0$ and $d(\psi) = 1$. Therefore, $T(\psi) = 1$ and hence $\langle \sigma, T(\psi)\rangle = \langle\sigma\rangle$. However $\langle\sigma\rangle \cap C = 1$ and hence

$\psi^{|\psi G|} = \psi^p \notin \langle \sigma, T(\psi) \rangle$. So it follows from Corollary 4.6 that $CC(K)_p$ has infinite index in $S(K)_p$.

The reader may check using Theorem 1 that $[S(K)_p : CC(K)_p] = \infty$ for the fields K constructed by Janusz that were mentioned in Example 3.4. The same holds for the field of Example 3.5. This can be verified using the arguments in the proofs of Lemmas 4.2 and 6.4 and Proposition 6.5 in [Jan2] where it is proved that $0 = v_p(|S(K,q)|) < \beta(q)$ for all the primes q such that $q \equiv 1 \mod 16$ and r is not a square modulo q.

In all the examples shown so far, the index of $CC(K)_p$ in $S(K)_p$ is either 1 or infinity. This, together with Corollary 4.5, may lead one to believe that the quotient group $S(K)_p/CC(K)_p$ is either trivial or infinite for every field K and every prime p. By Corollary 2.3 and Theorem 4.3, $S(K)_p/CC(K)_p$ is both finite and non-trivial if and only if $\nu(r) = \beta(r)$ for every odd prime not dividing m and $\nu(r) \neq \beta(r)$ for r either 2 or an odd prime dividing m. In the following example we show that for every odd prime p there exists a field K satisfying these conditions.

Example 4.10. *An example with $CC(K)_p \neq S(K)_p$ and $[S(K)_p : CC(K)_p] < \infty$.*

Let p be an arbitrary 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 $r \equiv k + q \mod q^2$ and $r \equiv 1 + p^2 \mod p^3$. 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 $G = \mathrm{Gal}(F/K(\zeta_{qr})) \times \mathrm{Gal}(F/K(\zeta_{p^4q})) \times \mathrm{Gal}(F/K(\zeta_{p^4r}))$. We may choose σ so that $\langle \sigma \rangle = \mathrm{Gal}(F/K(\zeta_{qr})) \cong G/C$ has order p^2. The inertia subgroup of r in G is $\mathrm{Gal}(F/K(\zeta_{p^4q}))$, which is generated by an element θ of order p. Note that $B = C$ and $v_p(\exp(\mathrm{Gal}(K/\mathbb{Q}))) = v_p(\exp B) = 1 < a = 2$. Hence K satisfies the conditions of Corollary 4.8 and so $CC(K)_p$ has finite index in $S(K)_p$.

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 $\nu(r) = \max\{0, a + v_p(|\theta|) - v_p(|W(K_r)|)\} = 0$.

Let ψ_r be the Frobenius automorphism of r in $\mathrm{Gal}(F/\mathbb{Q})$. Then $\psi_r^p = \sigma^p \eta$, where $\eta \in B$ generates $\mathrm{Gal}(F/K(\zeta_{p^4r}))$. Since $\langle \theta \rangle \cap \langle \eta \rangle = 1$, there exists a skew pairing $\Psi : B \times B \to W(K)_p$ such that $\Psi(\theta, \eta)$ has order p. By [HOR2, Theorem 13], it follows that $\beta(r) \geq 1$, and so $S(K)_p \neq CC(K)_p$.

The last example shows that when G/C is noncyclic, it is possible for $CC(K)_2$ to have infinite index in $S(K)_2$ even when $t = v_2(\exp B) = 0$. It also is a counterexample to [Pen1, Theorem 2.2].

Example 4.11. An example with $[S(K)_2 : CC(K)_2] = \infty$ and $C = 1$.

Let q be an odd prime greater than 5. Let $K = \mathbb{Q}(\zeta_q, \sqrt{2})$, and consider $[S(K)_2 : CC(K)_2]$. It is easy to see that $p^a = 2$ and $b = 2$. Since $\mathrm{Gal}(K(\zeta_{2^4})/K)$ is noncyclic, we compute $s = a + b + v_2([\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] + 2 = 6$, and so $F = \mathbb{Q}(\zeta_{64q})$. Since $\mathbb{Q}(\zeta_q) \subset K$, we have $C = \mathrm{Gal}(F/K(\zeta_{64})) = 1$. For our generators of $\mathrm{Gal}(F/K)$, we may choose ρ, σ such that $\rho(\zeta_q) = \zeta_q$, $\rho(\zeta_{64}) = \zeta_{64}^{-1}$, $\sigma(\zeta_q) = \zeta_q$, and $\sigma(\zeta_{64}) = \zeta_{64}^9$. Let r be any prime for which $r^2 \equiv 1 \mod q$ and $r \equiv 5 \mod 2^6$. Then $\psi_r \notin G$, but $5^2 \equiv 9^3 \mod 64$ implies that $\psi_r^2 = \sigma^3$. This means that we are in the case of Theorem 4.1 where $\nu(r) = 0$ and j is odd, so $\beta(r) = 1$. So $[S(K)_2 : CC(K)_2]$ is infinite.

References

[Ben] M. Benard, *The Schur subgroup I*, J. Algebra **22**(1972), 374–377.

[BS] M. Benard and M. Schacher, *The Schur subgroup II*, J. Algebra **22**(1972), 378–385.

[HOR1] A. Herman, G. Olteanu and Á. del Río, *Ring isomorphism of cyclic cyclotomic algebras*, to appear in Algebr. Represent. Theory.

[HOR2] A. Herman, G. Olteanu and Á. del Río, *The Schur Group of an Abelian Number Field*, J. Pure Appl. Algebra (2008), `doi:10.1016/j.jpaa.2008.05.002`.

[Jan1] G.J. Janusz, *Generators for the Schur group of local and global number fields*, Pacific J. Math. **56** (1975), 525–546.

[Jan2] G.J. Janusz, *The Schur group of an algebraic number field*, Ann. of Math. (2) **103** (1976), 253–281.

[Jan3] G.J. Janusz, *The Schur group of cyclotomic fields*, J. Number Theory **7** (1975), 345–352.

[Pen1] J.W. Pendergrass, *The 2-part of the Schur group*, J. Algebra **41** (1976), 422–438.

[Pen2] J.W. Pendergrass, *The Schur subgroup of the Brauer group*, Pacific J. Math. **69** (1977), 477–499.

[Rei] I. Reiner, *Maximal orders*, Academic Press 1975, reprinted by LMS 2003.

[Ser] J.-P. Serre, *Local fields*, Springer 1979.

[Yam] T. Yamada, *The Schur subgroup of the Brauer group*, Lecture Notes in Mathematics **397**, Springer–Verlag, 1974.

Department of Mathematics, University of Regina, Regina, Canada

E-mail address: `aherman@math.uregina.ca`

Department of Mathematics and Computer Science, North University of Baia Mare, Victoriei 76, 430122 Baia Mare, Romania and Faculty of Mathematics and Computer Science, Babeş-Bolyai University, M. Kogalniceanu 1, 400084 Cluj-Napoca, Romania.

E-mail address: `golteanu@ubm.ro, olteanu@math.ubbcluj.ro`

Departamento de Matemáticas, Universidad de Murcia, 30100 Murcia, España

E-mail address: `adelrio@um.es`