

Algebras with Uniformly Distributed Invariants

RICHARD A. MOLLIN

Department of Mathematics, Queen's University, Kingston, Ontario, Canada K7L 3N6

Communicated by I. N. Herstein

Received April 1, 1975

INTRODUCTION

Let K be a finite abelian extension of the rational field Q . If A is a central simple algebra over K then we let $[A]$ denote the class of A in the Brauer group $B(K)$ of K . The *Schur subgroup* $S(K)$ of $B(K)$ consists of those algebra classes which contain a simple component of the group algebra $K[G]$ for some finite group G .

M. Benard and M. Schacher [2, Theorem 1, p. 380] have shown that if $[A]$ is in $S(K)$ then:

(1) If the index of A is m then ϵ_m is in K , where ϵ_m is a primitive m th root of unity.

(2) If \mathcal{P} is a K -prime lying over the rational prime p , and $\sigma \in \text{Gal}(K/Q)$ with $\epsilon_m^\sigma = \epsilon_m^b$ then the \mathcal{P} -invariant of A satisfies:

$$\text{inv}_{\mathcal{P}}(A) \equiv b \text{inv}_{\mathcal{P}^\sigma}(A) \pmod{1}$$

If a central simple algebra A over K satisfies (1) and (2) above then A is said to have *uniformly distributed invariants*.

Based on this result, we define the group, $U(K)$, as the subgroup of $B(K)$ consisting of those algebra classes which contain an algebra with uniformly distributed invariants. It follows from the Benard–Schacher result that $S(K)$ is a subgroup of $U(K)$.

In this paper we investigate general properties of $U(K)$, and the relationship between $S(K)$ and $U(K)$.

E. Witt, [12, Satz 10, 11, p. 243], proved that the index of an element of $S(K)$ at a prime $p \neq 2$ divides $p - 1$ and at $p = 2$ divides 2. In the first section we generalize Witt's results to $U(K)$ (and obtain a simpler proof of his results for $S(K)$).

Using the above result we obtain a bound on the local indicies of elements of $U(K)$, and show that the bound is attained. From this we get that the exponent of $U(K)$ equals the order of the group of roots of unity in K .

This result does not hold in general for $S(K)$. In fact, some of the latest research by G.J. Janusz [6], into $S(K)$ involves maximizing the index of elements of $S(K)$ at a given prime.

In Section 2 we obtain necessary and sufficient conditions for $U(K)$ to equal $U(L) \otimes_L K$ where L is a subfield of K . For $S(K)$, such conditions are unknown. However, certain authors such as Yamada [13, Theorem 7.3, p. 97, Theorem 7.14, p. 112], Benard and Schacher [2, Theorem 2, p. 383], and G. J. Janusz [8, Corollary 3.1] have found fields K for which $S(K)$ equals $S(L) \otimes_L K$ for some subfield L of K . From the above result for $U(K)$ we obtain a new result for $S(K)$; viz a sufficient condition for $S(K)$ to equal $S(L) \otimes_L K$. Using the above results we obtain a sufficient condition for $U(K)$ to equal $S(K)$.

The material presented in this paper is part of the author's doctoral thesis written at Queen's University, Kingston, Canada, under the direction of Professor I. P. Hughes. Thanks must go to the National Research Council, and the Canada Council, both of which helped to finance the research.

1

We assume throughout that K/Q is finite abelian, and let $K_{\mathcal{P}}$ denote the completion of K at \mathcal{P} . If $[A]$ is in $U(K)$, and \mathcal{P}' and \mathcal{P} are K -primes lying above the rational prime p then $A \otimes_K K_{\mathcal{P}'}$ and $A \otimes_K K_{\mathcal{P}}$, have the same index. This follows from the definition of $U(K)$ because $(b, m) = 1$, and the denominator of $\text{inv}_{\mathcal{P}}(A)$ divides the index of A . We call the common value of the indices of $A \otimes_K K_{\mathcal{P}}$ for all K -primes lying above p the p -local index of A , and denote it by, $\text{ind}_p(A)$. For a K -prime \mathcal{P} lying over p we call the invariant of $A \otimes_K K_{\mathcal{P}}$, $\text{inv}_{\mathcal{P}}(A)$, a p -local invariant of A . The result was obtained by Benard and Schacher [1, Theorem 1, p. 376] for elements of $S(K)$.

We continue with a discussion of some fundamental results concerning the decomposition of primes in an algebraic number field. These results will be used at various stages throughout the paper.

We let L/F be a finite Galois extension of number fields. Now we let $\not\!{f}$ denote any prime of F , finite or infinite, and let its decomposition in L be: $\not\!{f} = (\mathcal{P}_1 \cdots \mathcal{P}_\ell)^e$. We set $\mathcal{P} = \mathcal{P}_1$ and $D_{\mathcal{P}} = \{\sigma \in \text{Gal}(L/F) : \mathcal{P}^\sigma = \mathcal{P}\}$. We call $D_{\mathcal{P}}$ the *decomposition group* of \mathcal{P} . It is easy to see that $D_{\mathcal{P}\sigma} = \sigma^{-1}(D_{\mathcal{P}})\sigma$. Thus, when L/F is abelian $D_{\mathcal{P}}$ depends only on $\not\!{f}$ and not on the choice of \mathcal{P} . In this case we write $D_{\not\!{f}}$ instead of $D_{\mathcal{P}}$.

The fixed field Z of $D_{\mathcal{P}}$ is called the *decomposition field* at \mathcal{P} . When $D_{\mathcal{P}}$ is normal in $\text{Gal}(L/F)$ then $\not\!{f}$ does all its splitting in Z/F ; i.e. $\not\!{f}$ has the factorization: $\not\!{f} = (q_1 \cdots q_\ell)$ in Z where $\ell = |Z:F|$, [7, Proposition 1.4, p. 97]. Thus, for example, if $F = Q$, $\not\!{f} = p$ is a rational prime, and ϵ_m is in Z then it follows

that p splits completely in $Q(\epsilon_m)$. We note that p splits completely in $Q(\epsilon_m)$ if and only if the Frobenius automorphism σ at p is trivial, [5, Sect. 5.5, pp. 84–88]. If $p \nmid m$ then the Frobenius automorphism σ at p in $Q(\epsilon_m)/Q$ is characterized by $\epsilon_m^\sigma = \epsilon_m^p$, [5, Theorem 6–2–14, p. 102]. Hence, p splits completely in $Q(\epsilon_m)$ if and only if $p \equiv 1 \pmod{m}$, [5, Theorem 6–2–15, p. 103].

Now we generalize Witt’s results [12, Theorems 10; 11, p. 243].

THEOREM 1.1. *If K/Q is finite abelian, p is an odd prime and $[A]$ is in $U(K)$ has $\text{ind}_p(A) = n$ then $p \equiv 1 \pmod{n}$. If $p = 2$ then $\text{ind}_p(A) = 1$ or 2 .*

Proof. We let $[A]$ in $U(K)$ have $\text{ind}_p(A) = n$. If $n \leq 2$ then the result is clear. Thus we may assume $n > 2$.

We let $D = D_p$ be the decomposition group of $G = \text{Gal}(K/Q)$ at p . By the definition of $U(K)$ we have that ϵ_n is in K . For σ in D , $\epsilon_n^\sigma = \epsilon_n^b$ for some integer b relatively prime to n . If \mathcal{P} is a K -prime lying over the rational prime p we have that, since $\mathcal{P} = \mathcal{P}^\sigma$:

$$\text{inv}_{\mathcal{P}}(A) \equiv b \text{inv}_{\mathcal{P}^\sigma}(A) \equiv b \text{inv}_{\mathcal{P}}(A) \pmod{1}$$

by the definition of $U(K)$. Therefore, $b \equiv 1 \pmod{n}$, and so σ fixes ϵ_n . But σ in D was arbitrary. Thus, $Q(\epsilon_n)$ is contained in the fixed field of D , i.e. the decomposition field at p . From the discussion preceding the theorem we see that p splits completely in $Q(\epsilon_n)$, and so $p \equiv 1 \pmod{n}$ since $n > 2$. We note that p cannot be 2, and the theorem is proved. Q.E.D.

COROLLARY 1.2. *We maintain the above notation. If $n = q^a$ where q is prime and ϵ_{q^r} is the highest q -power root of unity in K such that $p = 1 + q^d$ with q relatively prime to d , then $a \leq \min\{r, c\}$.*

Proof. This is clear from the theorem.

COROLLARY 1.3. *Let $[A] \in U(K)$ and let \mathcal{P} and \mathcal{P}_1 be K -primes dividing p . Suppose $\text{ind}_p(A) = n$. Then $\text{inv}_{\mathcal{P}}(A) = \text{inv}_{\mathcal{P}_1}(A)$ if and only if $\mathcal{P} \cap Q(\epsilon_n) = \mathcal{P}_1 \cap Q(\epsilon_n)$.*

Proof. Let $\sigma \in G = \text{Gal}(K/Q)$ with $\epsilon_m^\sigma = \epsilon_m^b$. If $p = 2$ then $n = 1$ or 2 by the theorem. In this case our result is immediate from the definition of $U(K)$. If $p > 2$ we let H be the subgroup of G fixing $Q(\epsilon_n)$. Thus $b \equiv 1 \pmod{n}$ if and only if $\sigma \in H$. By the theorem $p \equiv 1 \pmod{n}$ and from the discussion preceding the theorem we see that this means p splits completely in $Q(\epsilon_n)$. Thus $\sigma \in H$ if and only if $\mathcal{P} \cap Q(\epsilon_n) = \mathcal{P}^\sigma \cap Q(\epsilon_n)$. Q.E.D.

COROLLARY 1.4. *Let $[A] \in U(K)$ and suppose $\text{ind}_n(A) = n$. Then each of the values t/n , where $0 < t < n$, and $(t, n) = 1$ occurs equally often as each p -local invariant of A , viz $|H: D|$ times, where H and D are as above.*

Proof. Corollary 1.3 yields that we have the same invariant of A at two K -primes above p if and only if those two K -primes lie above a single $Q(\epsilon_n)$ -prime. We now determine the number of primes into which each $Q(\epsilon_n)$ -prime splits in K .

From the discussion preceding the theorem we see that p does all its splitting in Z , the decomposition field at p . By the theorem, if $p > 2$ then $p \equiv 1 \pmod n$ and by the discussion preceding the theorem we have that p splits completely in $Q(\epsilon_n)$; whereas if $p = 2$ then $n = 1$ or 2 . In either case $Q(\epsilon_n) \subseteq Z$, i.e. $D \subseteq H$. Thus each $Q(\epsilon_n)$ -prime splits into $|Z: Q(\epsilon_n)| = |H: D|$ primes in K , and so each p -local invariant of A occurs $|H: D|$ times.

Now n divides m . Hence, if $\sigma \in G$ and $\epsilon_n^\sigma = \epsilon_n^b$, then as σ ranges over all elements of $G(K/Q)$, $b \pmod n$ takes each element of $(Z/nZ)^*$ an equal number of times. Since the denominator of $\text{inv}_\sigma(A)$ is n then from the definition of $U(K)$ we get that each value t/n occurs equally often as $\text{inv}_{\sigma\sigma}(A)$. Thus each p -local invariant occurs equally often as the values t/n , where $0 < t < n$ and $(t, n) = 1$. Q.E.D.

We note that Yamada [13, Theorem (4.4), p. 43] generalized Witt's results; viz that for an odd prime p , $\text{ind}_p(A)$ must divide $(p - 1)/c$ for $[A]$ in $S(K)$, where c is the tame ramification index of $K_\mathcal{P}/Q_p$, \mathcal{P} being a K -prime dividing p . Furthermore, he refined the result for $p = 2$, [13, Theorem 5.14, p. 88].

From the next theorem it follows that this generalization fails for $U(K)$. Moreover, Corollary 1.2 gave a bound on the local indicies of elements of $U(K)$, and the next theorem yields that those bounds are always attained by some element of $U(K)$. From this we see that the exponent of $U(K)$ equals the order of the group of roots of unity in K .

THEOREM 1.5. *Let K/Q be finite abelian. If ϵ_m is in K and $p \equiv 1 \pmod m$ where p is a prime, then there exists $[A]$ in $U(K)$ with $\text{ind}_p(A) = m$.*

Proof. We assume ϵ_m is in K , and p is a prime such that $p \equiv 1 \pmod m$. If $m = 2$ then the result is clear. Therefore we may assume $m > 2$; i.e. $Q(\epsilon_m) \neq Q$.

We let H be the subgroup of $G = \text{Gal}(K/Q)$ fixing $Q(\epsilon_m)$ and let $D = D_p$ be the decomposition group of G at p .

Now we choose coset representatives $\{\sigma_i\}$ of D in G through H , and let $\epsilon_m^{\sigma_i} = \epsilon_m^{b_i}$.

We define an algebra A such that

$$\text{inv}_\sigma(A) = 1/m \quad \text{and} \quad \text{inv}_{\sigma\sigma}(A) = b_i^{-1}/m.$$

where \mathcal{P} is a K -prime lying above p and b_i^{-i} is the multiplicative inverse of b_i mod m ; and:

$$\text{inv}_\varphi(A) = 0 \quad \text{for } K\text{-primes } \varphi \text{ not above } p.$$

We now show that:

$$\sum_{\mathcal{P}} \text{inv}_{\mathcal{P}}(A) \equiv 0 \pmod{1}$$

where \mathcal{P} ranges over all K -primes above p . We have:

$$\sum_{\mathcal{P}} \text{inv}_{\mathcal{P}}(A) = (1/m) \sum b_i^{-1} = (|H: D|/m) \sum_{j=1}^{\phi(m)} (t_j)$$

where $0 < t_j < m$, $(t_j, m) = 1$, and $\phi(m)$ is the Euler function. Now, we note that since the t_j may be arranged in pairs $t_j, m - t_j$ then m divides $\sum_{j=1}^{\phi(m)} (t_j)$. Thus, $\text{inv}_{\mathcal{P}}(A) \equiv 0 \pmod{1}$ which implies, by Hasse's sum theorem that $[A]$ is in $B(K)$, and by construction is in $U(K)$. But, $\text{ind}_p(A) = m$, thereby completing the proof. Q.E.D.

2

We let L be a subfield of K where K/Q is finite abelian. We proceed to find necessary and sufficient conditions for $U(K)$ to equal $U(L) \otimes_L K$. Now we use the results of Section 1 to prove the following lemma:

LEMMA 2.1. *Let K/Q be finite abelian. If $[A]$ is in $U(K)$ and $\text{ind}_p(A) = m > 2$ then the invariants of A at the primes above p sum to zero modulo 1.*

Proof. We let $[A]$ in $U(K)$ have $\text{ind}_p(A) = m > 2$. We let $D = D_p$ be the decomposition group of $G = \text{Gal}(K/Q)$ at p , and let H be the subgroup of G fixing $Q(\epsilon_m)$.

By Corollary 1.4, each of the values t/m , where $0 < t < m$, and $(t, m) = 1$ occurs equally often as each p -local invariant of A , viz $|H: D|$ times. Thus, we have:

$$\sum_{\mathcal{P}} \text{inv}_{\mathcal{P}}(A) = |H: D| \sum_{i=1}^{\phi(m)} (t_i/m)$$

where $(t_i, m) = 1$, and $\phi(m)$ is the Euler function.

Now, since the t_i may be arranged in pairs, t_i and $m - t_i$, then m divides $\sum_{i=1}^{\phi(m)} (t_i)$. Thus we have:

$$\sum_{\mathcal{P}} \text{inv}_{\mathcal{P}}(A) \equiv 0 \pmod{1}$$

which completes the proof.

Q.E.D.

Before proceeding with the next result we note the following formulae [3, Chap. 7]:

$$(2.2) \quad \text{If } [A], [B] \in B(K) \text{ and } \mathfrak{p} \text{ is a prime of } K, \text{ then: } \text{inv}_{\mathfrak{p}}(A \otimes_K B) \equiv \text{inv}_{\mathfrak{p}}(A) + \text{inv}_{\mathfrak{p}}(B) \pmod{1}.$$

$$(2.3) \quad \text{If } [A] \in B(K), L/K \text{ is finite and } \mathcal{P} \text{ is an } L\text{-prime above } \mathfrak{p} \text{ then } \text{inv}_{\mathcal{P}}(A \otimes_K L) \equiv |\mathcal{O}_{\mathcal{P}}L : \mathcal{O}_{\mathcal{P}}K| \text{inv}_{\mathcal{P} \cap K}(A) \pmod{1}.$$

LEMMA 2.4. *If $[A], [B] \in U(K)$ and \mathcal{P} is a K -prime above the rational prime \mathfrak{p} with $\text{inv}_{\mathcal{P}}(A) = \text{inv}_{\mathcal{P}}(B)$ then $\text{inv}_{\mathcal{P}_i}(A) = \text{inv}_{\mathcal{P}_i}(B)$ for all K -primes \mathcal{P}_i above \mathfrak{p} .*

Proof. We have:

$$0 = \text{inv}_{\mathcal{P}}(A) - \text{inv}_{\mathcal{P}}(B) \equiv \text{inv}_{\mathcal{P}}(A) + \text{inv}_{\mathcal{P}}(B^{\text{op}}) \pmod{1}$$

where B^{op} is the opposite algebra of B , i.e. $[B]^{-1} = [B^{\text{op}}]$. Thus, by (2.2) we get:

$$\text{inv}_{\mathcal{P}}(A \otimes_K B^{\text{op}}) \equiv 0 \pmod{1}.$$

It now suffices to show that $\text{inv}_{\mathcal{P}_i}(A \otimes_K B^{\text{op}}) \equiv 0 \pmod{1}$ for all K -primes \mathcal{P}_i above \mathfrak{p} . Since $G = \text{Gal}(K/Q)$ transitively permutes the K -primes above \mathfrak{p} , [5, Proposition 5-4, p. 68], then there exists $\sigma \in G$ such that $\mathcal{P}_i^{\sigma} = \mathcal{P}$. Now if $\epsilon_m^{\sigma} = \epsilon_m^b$ where $\text{ind}_{\mathfrak{p}}(A \otimes_K B^{\text{op}}) = m$ then:

$$\text{inv}_{\mathcal{P}_i}(A \otimes_K B^{\text{op}}) \equiv b \text{inv}_{\mathcal{P}_i^{\sigma}}(A \otimes_K B^{\text{op}}) \equiv b \text{inv}_{\mathcal{P}}(A \otimes_K B^{\text{op}}) \equiv 0 \pmod{1}.$$

Q.E.D.

Before proceeding with the next theorem we state the following useful result known as the *Dirichlet density theorem*:

THEOREM 2.5. [5, Corollary 9-2-7, p. 168]. *Let K/L be finite abelian with Galois group G . If $\sigma \in G$ then there are infinitely many primes \mathcal{P} with σ as Frobenius automorphism.*

We note that if \mathcal{P} is unramified in K/L then the order of the Frobenius automorphism of \mathcal{P} in K/L is the inertial degree of \mathcal{P} in K/L , [5, Sect. 5.5]. Although we use Theorem (2.5) in the proof of the next result we will not need the full force of the theorem until the proof of Theorem (2.9).

We let L be a subfield of K where K/Q is finite abelian, and let n be the order of the largest root of unity in K . We note that n must be even. For a prime q we let $U(K)_q$ denote the q -primary part of $U(K)$.

THEOREM 2.6. $U(K) = U(L) \otimes_L K$ if and only if

- (1) $(n, |K:L|) = 1$; and
- (2) $Q(\epsilon_n) \subseteq L$.

Proof. If q is any prime dividing n then it suffice to show that: $U(K) = U(L) \otimes_L K$ if and only if:

- (1) $(q, |K:L|) = 1$; and
- (2) There are no higher q -power roots of unity in K than in L .

We assume that: $U(L) \otimes_L K = U(K)_q$, and let ϵ_{q^a} be the highest q -power root of unity in L . We first show that $(q, |K:L|) = 1$. If we assume $q \mid |K:L|$ then by Theorem (2.5) we may choose an element σ of order q in $\text{Gal}(K/L)$ as the Frobenius automorphism corresponding to some prime p . From the discussion preceeding the theorem we see that p has inertial degree equal to q in K/L . Since σ fixes $Q(\epsilon_{q^a})$ then by the discussion preceeding Theorem (1.1) we see that ϵ_{q^a} is in the decomposition field at p , and so p splits completely in $Q(\epsilon_{q^a})$, which implies that $p \equiv 1 \pmod{q^a}$. Thus, by Theorem (1.5) there exists an $[A]$ in $U(K)$ with $\text{ind}_p(A) = q^a$. However by hypothesis, $[A] = [B \otimes_L K]$ where $[B]$ is in $U(L)$.

Since $\text{inv}_{\mathcal{P}}(A) = \text{inv}_{\mathcal{P}}(B \otimes_L K)$ where \mathcal{P} is a K -prime above p , then $\text{inv}_{\mathcal{P}}(A) \equiv |K_{\mathcal{P}} : L_{\mathcal{P}_i}| \cdot \text{inv}_{\mathcal{P}_i}(B) \pmod{1}$ where \mathcal{P} lies above the L -prime \mathcal{P}_i . Now, Corollary (1.2) yields that since ϵ_{q^a} is the highest q -power root of unity in L then $\text{ind}_{\mathcal{P}_i}(B) \leq q^a$. But by the choice of the prime p we have that $q \mid |K_{\mathcal{P}} : L_{\mathcal{P}_i}|$. Therefore, $\text{ind}_{\mathcal{P}}(A) \leq q^{a-1}$ a contradiction. Hence we have condition (1); $q \nmid |K:L|$.

Now we show $\epsilon_{q^{a+1}}$ is not in K to yield condition (2). If $\epsilon_{q^{a+1}}$ is in K , and p is a prime such that $p \equiv 1 \pmod{q^{a+1}}$ then by Theorem (1.5) there is an element $[C]$ in $U(K)_q$ with $\text{ind}_p(C) = q^{a+1}$. But, by hypothesis $[C] = [D \otimes_L K]$ where $[D]$ is in $U(L)_q$. From this it follows that $\text{ind}_p(D) = q^{a+1}$. But there does not exist an element with index q^{a+1} , in $U(L)_q$ at any prime because $\epsilon_{q^{a+1}}$ is not in L , a contradiction. Hence, we have condition (2): there are no higher q -power roots of unity in K than in L .

Conversely, we assume (1) and (2). We let $[A]$ be in $U(K)_q$ and prove $[A]$ is in $U(L) \otimes_L K$. We let S denote the set of rational primes at which A has nonzero invariants. Now, we proceed to find algebras $[B]$ in $U(L)_q$ with nonzero invariants exactly at primes in S , such that the product of the $[B \otimes_L K]$ equals $[A]$ in $U(K)_q$.

If $q = 2$, let S' be the subset of S consisting of primes p , finite or infinite, at which $\text{ind}_p(A) = 2$. Now, if $S - S'$ is nonempty then Lemma (2.1) yields that the invariants at K -primes above any given prime in $S - S'$ must sum to zero modulo 1. Therefore, by Hasse's sum theorem the total number of K -primes above primes in S' must be even. But, condition (1) of the

hypothesis ensures that $|K:L|$ is odd, so the total number of L -primes lying over primes in S' must be even. Therefore, by Hasse's sum theorem, there is an element $[B']$ in $B(L)$ with $\text{ind}(B') = 2$ at the primes p in S' , and with other local indicies equal to 1. Then clearly $[B']$ is in $U(L)$. Now, since $|K:L|$ is odd then $[B' \otimes_L K]$ in $U(K)$ has invariant $1/2$ at the K -primes in S' , and zero invariant elsewhere.

We now consider the primes in $S - S'$ provided $S - S'$ is nonempty. We note that the following argument holds for the case $q \neq 2$ as well, wherein S' is empty.

For primes p in $S - S'$, $\text{ind}_p(A) = q^v$, say, is greater than 2. Thus by Theorem (1.1), $p \equiv 1 \pmod{q^v}$. Now by condition (2) of the hypothesis, ϵ_{q^v} is in L . Thus, Theorem (1.5) ensures that there is an element $[B]$ in $U(L)$ with $\text{ind}_p(B) = q^v$, and other local indices equal to 1.

We let $\text{inv}_{\mathcal{P}_1}(B) = t/q^v$ where $(t, q) = 1$, and \mathcal{P}_1 is an L -prime above p , and let $\text{inv}_{\mathcal{P}}(A) = r/q^v$ where $(r, q) = 1$, and \mathcal{P} is a K -prime above \mathcal{P}_1 . If we let $|K_{\mathcal{P}} : L_{\mathcal{P}_1}| = u$ then $(u, q) = 1$ since, by condition (1) of the hypothesis, $q \nmid |K:L|$.

We consider $B^{t^{-1}ru^{-1}} = B_p$ and note that it is easy to check:

$$\text{inv}_{\mathcal{P}}(B_p \otimes_L K) \equiv \text{inv}_{\mathcal{P}}(A) \pmod{1}.$$

We note that by Lemma (2.4) we have:

$$\text{inv}_{\mathcal{P}_i}(B_p \otimes_L K) \equiv \text{inv}_{\mathcal{P}_i}(A) \pmod{1}$$

for all K -primes \mathcal{P}_i extending p .

Thus, $B_p \otimes_L K$ and A have the same p -local invariants. Hence we have:

if $q = 2$:

$$[A] = [B' \otimes_L K] \cdot \prod_p [B_p \otimes_L K]$$

where p ranges over all primes in $S - S'$ unless $S - S'$ is empty in which case:

$$[A] = [B' \otimes_L K].$$

if q is odd:

$$[A] = \prod_p [B_p \otimes_L K]$$

where p ranges over all primes in S .

In any case we have that $[A]$ is in $U(L)_q \otimes_L K$. Therefore;

$$U(K)_q \subseteq U(L)_q \otimes_L K.$$

Conversely we now show that:

$$U(L)_q \otimes_L K \subseteq U(K)_q.$$

If $[A] \in U(L)_q$ with $\text{ind}_{\mathcal{P}}(A) = q^a$ then given a K -prime \mathcal{P} we have, by (2.3), that;

$$\text{inv}_{\mathcal{P}}(A \otimes_L K) \equiv |K_{\mathcal{P}} : L_{\mathcal{P} \cap L} | \text{inv}_{\mathcal{P} \cap L}(A) \pmod{1}.$$

Now, if $\sigma \in G(K/Q)$ consider σ_L as the restriction of σ to L . If $\epsilon_{q^a}^{\sigma} = \epsilon_{q^a}^b$ then :

$$\text{inv}_{(\mathcal{P} \cap L)}(A) \equiv b \text{inv}_{(\mathcal{P} \cap L)} \sigma_L(A) \pmod{1}$$

by the definition of $U(L)_q$. Hence:

$$\begin{aligned} \text{inv}_{\mathcal{P}}(A \otimes_L K) &\equiv b |K_{\mathcal{P}} : L_{\mathcal{P} \cap L} | \text{inv}_{(\mathcal{P} \cap L)} \sigma_L(A) \pmod{1} \\ &\equiv b |K_{\mathcal{P}} : L_{\mathcal{P} \cap L} | \text{inv}_{(\mathcal{P} \cap L)}(\sigma(A)) \pmod{1} \\ &\equiv b \text{inv}_{\mathcal{P}} \sigma(A) \pmod{1} \end{aligned}$$

We have shown that: $U(L)_q \otimes_L K \subseteq U(K)_q$. Hence:

$$U(K)_q = U(L)_q \otimes_L K$$

and the theorem is proved.

Q.E.D.

We note that the following corollary was obtained independently by J. W. Pendegras [10], wherein he uses G. Janusz' results on the generators of $S(K)$ [9].

COROLLARY 2.7. *If $q \nmid |K:L|$ and there are no higher q -power roots of unity in K than in L then*

$$S(K)_q = S(L)_q \otimes_L K.$$

Proof. It suffices to show

$$S(K)_q \subseteq S(L)_q \otimes_L K.$$

From the theorem we get that:

$$S(K)_q \subseteq U(L)_q \otimes_L K.$$

Thus, if $[A]$ is in $S(K)_q$ then $[A] = [B \otimes_L K]$ where $[B]$ is in $U(L)_q$. So it suffices to show $[B]$ is in $S(L)_q$.

We denote by *Res* the restriction homomorphism of $B(L)$ to $B(K)$, and denote by *Cor* the corestriction homomorphism of $B(K)$ into $B(L)$. We have that:

$$\text{Res}([B]) = [B \otimes_L K] = [A].$$

We also have that:

$$\text{Cor} \cdot \text{Res}([B]) = ([B])^{|K:L|}.$$

But corestriction maps $S(K)_q$ into $S(L)_q$, and so $[B]^{|L:K|}$ is in $S(L)_q$. However, $q \nmid |K:L|$ so that $[B]$ is in $S(L)_q$, and the corollary is proved. Q.E.D.

The converse of Corollary 2.7 is false, as the following shows. G. J. Janusz [8], has shown that if ϵ_{q^a} is the highest q -power root of unity in $Q(\epsilon_m)$ then:

$$S(Q(\epsilon_m))_q = S(Q(\epsilon_{q^a}))_q \otimes_{Q(\epsilon_{q^a})} Q(\epsilon_m)$$

so we get a counterexample to the converse of the corollary by considering any field $Q(\epsilon_m)$ for which q divides $|Q(\epsilon_m):Q(\epsilon_{q^a})|$.

From Theorem 2.6 we get a result by Yamada [13, Theorem 7.3, p. 97], namely that: if K/Q is abelian and $|K:Q|$ is odd then K is real and $U(K) = S(K)$. It is clear that $|K:Q|$ being odd implies that K is real. Now by Theorem 2.6, $|K:Q|$ being odd implies that $U(K) = U(Q) \otimes_Q K$. But $U(Q) = S(Q)$ by K . Fields [4, p. 223]. Therefore $U(K) = S(Q) \otimes_Q K \subseteq S(K)$. But, $S(K) \subseteq U(K)$. Hence; $U(K) = S(K) = S(Q) \otimes_Q K$, and the assertion is proved.

The following corollary gives a sufficient condition for $U(K)_q = S(K)_q$ when q is odd.

COROLLARY 2.8. *If q is an odd prime and ϵ_{q^a} is the highest q -power root of unity in K with $q \nmid |K:Q(\epsilon_{q^a})|$ then:*

$$U(K)_q = S(K)_q = S(Q(\epsilon_{q^a}))_q \otimes_{Q(\epsilon_{q^a})} K$$

Proof. We may assume $a > 0$ since otherwise $S(K)_q = U(K)_q = 1$. It follows from Corollary 2.7 that $S(K)_q = S(Q(\epsilon_{q^a}))_q \otimes_{Q(\epsilon_{q^a})} K$. From Theorem 2.6 we get $U(K)_q = U(Q(\epsilon_{q^a}))_q \otimes_{Q(\epsilon_{q^a})} K$. Thus, it suffices to show that

$$U(Q(\epsilon_{q^a}))_q = S(Q(\epsilon_{q^a}))_q.$$

Since we know, $S(Q(\epsilon_{q^a}))_q \subseteq U(Q(\epsilon_{q^a}))_q$ it remains to show $U(Q(\epsilon_{q^a}))_q \subseteq S(Q(\epsilon_{q^a}))_q$.

Benard and Schacher [2, Theorem 3, p. 384], have shown that $S(Q(\epsilon_{q^a}))_q$ is generated by classes $[C_p]$ where:

- (1) p ranges over all primes such that $p \equiv 1 \pmod{q}$, and
- (2) $\text{ind}_p(C_p) = q^s$ where $s = \min\{a, c\}$ with $p = 1 + q^e d$, $(q, d) = 1$, and all other local indicies equal 1.

We let $[A]$ be in $U(Q(\epsilon_{q^a}))_q$. If p' is a prime such that $\text{ind}_{p'}(A) = q^t$ then by Theorem 1.1, $p' \equiv 1 \pmod{q^t}$, and by Corollary 1.2 we have $t \leq \min\{a, c\}$ where $p' \equiv 1 + q^e d$, $(q, d) = 1$.

We let \mathcal{P} be a K -prime lying over p' such that $\text{inv}_{\mathcal{P}}(C_{p'}) = 1/q^s$. If $\text{inv}_{\mathcal{P}}(A) = u/q^t$ then we set $e = uq^s/q^t$ then it follows that $[C_{p'}]^e$ and $[A]$ have equal p' -local invariants.

For each such prime p' we select such a $[C_{p'}]^e$. Then the product of the $[C_{p'}]^e$ equals $[A]$ in $S(Q(\epsilon_{q^a}))_q$, which completes the proof. Q.E.D.

Corollary 2.8 fails for the case $q = 2$. $S(Q(\epsilon_{2^a}))_2$, for $a > 1$ is generated by the $[C_p]$ as stated in the above proof with the restriction that p range over all odd primes such that $p \not\equiv -1 \pmod{2^a}$. This last statement was missed by Benard and Schacher in [2, Section 4, pp. 383–384] but noted and corrected in [13, p. 138] by Yamada, and independently by the author. It can be verified in a similar manner to the proof of Corollary 2.8 that: any element in $U(Q(\epsilon_{2^a}))$, with zero invariant at all primes p such that $p \equiv -1 \pmod{2^a}$, is in $S(Q(\epsilon_{2^a}))$.

We now investigate the relationship between $S(K)_q$ and $U(K)_q$ when $q \nmid |K:Q(\epsilon_{q^a})|$ where q is an odd prime. We begin by letting $L = Q(\epsilon_n)$ be the smallest cyclotomic field in which K is contained.

THEOREM 2.9. *Let K/Q be finite abelian and let ϵ_{q^a} be the highest q -power root of unity in K where $a > 0$ and q is an odd prime. Then if $q \nmid |K:Q(\epsilon_{q^a})|$ and $q \nmid |L:K|$ then $S(K)_q$ is of infinite index in $U(K)_q$.*

Proof. We proceed to obtain coset representatives of $S(K)_q$ in $U(K)_q$.

Choose an element σ of order q in $\text{Gal}(L/Q(\epsilon_{q^a}))$ as the Frobenius automorphism corresponding to some prime p . Since $q \nmid |L:K|$ then σ restricts nontrivially to K . Thus, p splits completely in $Q(\epsilon_{q^a})/Q$, has inertial degree equal to q in $K/Q(\epsilon_{q^a})$ and splits completely again in L/K . By Dirichlet's density theorem there are infinitely many such primes p and we note that $p \equiv 1 \pmod{q^a}$. Thus, for each such p we obtain an element $[A_p]$ in $U(K)_q$ with $\text{ind}_p(A_p) = q^a$, by Theorem 1.5.

Now we show $[A_p]$ is not in $S(K)_q$. First we note that it is easy to check that $q \nmid |L:K|$ implies ϵ_{q^a} is the highest q -power root of unity in L . In this case G. Janusz [8] has shown that

$$S(K)_q = S(Q(\epsilon_{q^a}))_q \otimes_{Q(\epsilon_{q^a})} K.$$

If $[A_p]$ is in $S(K)_q$ then $[A_p] = [B_p \otimes K]$ where $[B_p]$ is in $S(Q(\epsilon_{q^a}))_q$. We have: $\text{inv}_{\mathcal{P}}(A_p) = \text{inv}_{\mathcal{P}}(B_p \otimes K)$ where \mathcal{P} is a K -prime lying above p . So if \mathcal{P} lies over \mathcal{P}' in $K/Q(\epsilon_{q^a})$ then: $\text{inv}_{\mathcal{P}}(A_p) \equiv |K_{\mathcal{P}}:Q_{\mathcal{P}}(\epsilon_{q^a})| \text{inv}_{\mathcal{P}}(B_p) \pmod{1}$.

But $q \nmid |K_{\mathcal{P}}:Q_{\mathcal{P}}(\epsilon_{q^a})|$ and elements of $S(Q(\epsilon_{q^a}))_q$ have indicies less than or equal to q^a . Therefore, $\text{ind}_p(A_p) \leq q^{a-1}$, a contradiction, hence, $[A_p]$ is not in $S(K)_q$ for any such p . Similarly, we get $[A_p] \cdot [A_{p'}]^{-1}$ is not in $S(K)_q$ for any $[A_p] \neq [A_{p'}]$. Thus, the $[A_p]$ provide an infinite number of coset representatives of $S(K)_q$ in $U(K)_q$, and the proof is completed. Q.E.D.

Theorem 2.9 generalizes results by M. Schacher [11, Theorem 1, p. 15].

Using a result by G. Janusz [6], the author has made progress in the case not covered by the above theorem. Maintaining the notation of the Theorem, it has been shown that $|U(K)_q : S(K)_q|$ is infinite when q divides both $|K : Q(\epsilon_{qa})|$ and $|L : K|$ provided $q^{a+b} \nmid |L : K|$ where q^{a+b} is the highest q -power root of unity in $L = Q(\epsilon_n)$. When $q^{a+b} \mid |L : K|$ the difficulty occurs when n is divisible by exactly one prime congruent to 1 modulo q . The author conjectures that $q \mid |K : Q(\epsilon_{qa})|$ is not a sufficient condition for $|U(K)_q : S(K)_q|$ to be infinite. The details of the progress made in the aforementioned case will be published at a later date.

REFERENCES

1. M. BERNARD AND M. M. SCHACHER, The Schur Subgroup I, *J. Algebra* **22** (1972), 374–377.
2. M. BERNARD AND M. M. SCHACHER, The Schur Subgroup II, *J. Algebra* **22** (1972), 378–385.
3. M. DEURING, "Algebren," 2nd edit., Springer-Verlag, Berlin, 1968.
4. K. L. FIELDS, On the Brauer Speiser Theorem, *Bull. Amer. Math. Soc.* **77** (1971), 223.
5. L. J. GOLDSTEIN, Analytic Number Theory, Prentice-Hall, New Jersey, 1971.
6. G. J. JANUSZ, The Schur Group of an Algebraic Number Field, *Annals of Math.* **103** (1976), 345–352.
7. G. J. JANUSZ, "Algebraic Number Field," Academic Press, New York, 1973.
8. G. J. JANUSZ, The Schur Group of Cyclotomic Fields, *J. Number Theory* **7** (1975), 345–352.
9. G. J. JANUSZ, Generators for the Schur Group of Local and Global Number Fields, *Pacific J. Math.* **56** (1975), 525–546.
10. J. W. PENDERGRASS, The Schur Subgroup of the Brauer Group, Doctoral thesis written at the University of Illinois, 1974.
11. M. M. SCHACHER, More on the Schur Subgroup, *Proc. Amer. Math. Soc.* **31** (1972), 15–17.
12. E. WITT, Die Algebraische Struktur des Gruppenringes einer Endlichen Gruppe über einem Zahlkörper, *J. Reine Angew. Math.* **190** (1952), 231–245.
13. T. YAMADA, The Schur Subgroup of the Brauer Group, Lecture Notes in Mathematics, No. 397, Springer-Verlag (1974).