Can. J. Math., Vol. XXXIII, No. 5, 1981, pp. 1074–1084

CYCLOTOMIC DIVISION ALGEBRAS

R. A. MOLLIN

1. Introduction. Let K be a field of characteristic zero. The Schur subgroup $S(K)$ of Brauer group $B(K)$ consists of those equivalence classes $[A]$ which contain an algebra which is isomorphic to a simple summand of the group algebra KG for some finite group G. It is well known that the classes in $S(K)$ are represented by cyclotomic algebras, (see [**16**]). However it is not necessarily the case that the division algebra representatives of these classes are themselves cyclotomic. The main result of this paper is to provide necessary and sufficient conditions for the latter to occur when K is any algebraic number field.

Next we provide necessary and sufficient conditions for the Schur group of a local field to be induced from the Schur group of an arbitrary subfield. We obtain a corollary from this result which links it to the main result. Finally we link the concept of the stufe of a number field to the existence of certain quaternion division algebras in $S(K)$.

The above results continue work begun in [**11**]-[**13**]. We note furthermore that in [**4**], [**5**] and [**7**] we have given explicit constructions of cyclotomic quaternion division algebras.

2. Notation and preliminaries. Let K be an algebraic number field containing ϵ_n, a primitive nth root of unity for a fixed positive integer n. Let S denote the set of all K-primes containing the infinite primes and all primes dividing n. For α in K^*, the multiplicative group of non-zero elements of K, we let S together with the K-primes dividing α be denoted by $S(\alpha)$. Furthermore we let $I_K{}^{S(\alpha)}$ denote the subgroup of the ideal group I_K, of K generated by the K-primes outside $S(\alpha)$. Now, for $\mathscr{B}$ in $I_K{}^{S(\alpha)}$ the power residue symbol is defined by:

$$\sqrt[n]{\alpha}^{\phi(\mathscr{B})} = (\alpha/\mathscr{B})^{n\sqrt{\alpha}}$$

where ϕ denotes the Artin map in $K(\sqrt[n]{\alpha})$ over K. We refer to our development in [**11**], for other details and properties involved.

A *crossed product algebra* is denoted by $(L/K, \beta)$. This is the central simple K-algebra having L-basis u_τ where $\tau \in G(L/K)$, the Galois group of L over K subject to:

$$u_\sigma u_\tau = \beta(\sigma, \tau)u_{\sigma\tau} \quad \text{for } \sigma, \tau \in G(L/K),$$

Received February 8, 1980 and in revised form February 10, 1981. This research was supported by an NSERC university research fellowship.

and

$$u_\sigma x = x^\sigma u_\sigma \quad \text{for } x \in L^*.$$

When $G = \langle x \rangle$ then $(L/K, \beta)$ denotes the crossed product in which:

$$u_\tau{}^i = \begin{cases} u_{\tau^i} & \text{if } 1 \leqq i < |L : K|; \\ \beta & \text{if } i = |L : K| \end{cases}$$

where $|L : K|$ denotes the degree of L over K. For further information on crossed products, the reader is referred to [**15**].

By [**16**, Corollary 3.11, p. 33], $S(K)$ consists of those classes which contain a *cyclotomic algebra*; i.e., a crossed product of the form $(K(\epsilon)/K, \beta)$ where ϵ is a root of unity and the values of the factor set β are roots of unity in $K(\epsilon)$. If $\mathfrak{P}$ and $\mathfrak{Q}$ are K-primes above q then $A \otimes_K K_{\mathfrak{P}}$ and $A \otimes_K K_{\mathfrak{Q}}$ have the same index, (see [**16**] or [**6**]) where $K_{\mathfrak{P}}$ denotes the completion of K at $\mathfrak{P}$. We denote the common value of the indices $A \otimes_K K_{\mathfrak{Q}}$ for all K-primes $\mathfrak{Q}$ above q by $\operatorname{ind}_q A$, called the *q-local index* of A.

Note that most fundamental results concerning the Schur group may be found in [**16**]. Furthermore, henceforth when we write a tensor product it shall be assumed to be taken over the center of the algebra in the left factor.

Now we give some comments on notation. L/K shall mean "the field extension L over K". If m is an integer and $m = p^a t$ where p and t are relatively prime then we shall use the symbol $|m|_p = p^a$ to denote the highest power of p dividing m. If $\alpha \in K^*$ and $\mathfrak{P}$ is a K-prime then $\nu_{\mathfrak{P}}(\alpha)$ refers to the $\mathfrak{P}$-adic valuation of α. When referring to a prime below $\mathfrak{P}$ in K/F we shall abuse notation by denoting it by $\mathfrak{P} \cap F$ rather than referring to the intersection of $\mathfrak{P}$ and the ring of integers of F. Finally $\sim$ will denote equivalence in the Brauer group.

3. Cyclotomic division algebras. Let K be an algebraic number field and let n be the order of the largest root of unity in K. Let D be a *K-division algebra*, i.e., a finite dimensional division algebra over K, with center K. We say that D is a *cyclotomic division algebra* if D is a cyclic crossed product $(L/K, \epsilon)$ where ϵ is a root of unity in K, and L is a cyclotomic extension of K in the sense that $K \subseteq L \subseteq K(\zeta)$ for some root of unity ζ. Furthermore we shall let S_p denote the set of all rational primes q such that $|\operatorname{ind}_q D|_p > 1$ for a given prime p. Now the stage is set for the main result.

THEOREM 1. *Let $[D] \in S(K)$ with index m. D is a cyclotomic division algebra if and only if: for all finite primes p and q where q is in S_p the following hold;*

(a) $c \leqq a + d - b$ *and,*

(b) *For each K-prime* $\mathfrak{Q}$ *above* q *we have;*

$$|K_{\mathfrak{Q}} : Q_q(\epsilon_{p^d})|_p = \min\{p^{a+d-c-b}, p^{d-b}\},$$

where $|n|_p = p^a$, $|\mathrm{ind}_q D|_p = p^b$, $|q-1|_p = p^c$, *and* $|m|_p = p^d$.

Proof. First we assume that $D \sim (L/K, \epsilon)$ is a cyclotomic division algebra. We note that we may assume without loss of generality that $[D] \in S(K)_p$. Assume $\mathrm{ind}_q D = p^b$ for finite $q \in S_p$. We initially deal with the case where either $q \neq 2$ or $p \neq 2$.

Since the index of D is p^d then $|L : K| = p^d$, (see [**15**]). Therefore, by Kummer theory $L = K(\sqrt[p^d]{\alpha})$ for some $\alpha \in K^*$. Moreover since a unit is a norm in an unramified extension (see [**3**]), then q must be ramified in L/K, (see [**15**, (30.7), p. 26]). Suppose $\epsilon = \epsilon_{p^c}$. Now we show that $c = a$ is forced. Inflate D to $K(\sqrt[p^a]{\alpha})$ to get:

$$\mathrm{inf}\,[D] = [(K(\sqrt[p^a]{\alpha})/K, \epsilon_{p^c}{}^{p^{a-d}})]$$

from [**15**, Theorem (30.10), p. 262]. Therefore:

$$\mathrm{inf}\,[D] = [(K(\sqrt[p^a]{\alpha})/K, \epsilon_{p^{c-d+a}})].$$

But $c - a + d \geqq d$ from [**15**, Corollary (30.7), p. 262]. Therefore $c \geqq a$ and since we clearly have $c \leqq a$ then $c = a$ as required. Thus:

$$\mathrm{inf}\,[D] = [(K(\sqrt[p^a]{\alpha})/K, \epsilon_{p^d})]$$

which is equivalent to $[D]$ in $S(K)$.

Now, since $q \neq 2$ or $p \neq 2$ then $q \neq p$ (see [**16**] or [**6**]). Moreover; $N(\mathfrak{Q}) \equiv 1 \pmod{p^a}$ where $\mathfrak{Q}$ is a K-prime above q, and N denotes the norm in K/Q. Thus we may invoke the relationship between the norm and power residue symbols to get:

$$(\alpha, \epsilon_{p^d})_{\mathfrak{Q}} = (\epsilon_{p^d}/\mathfrak{Q})^{\nu_{\mathfrak{Q}}(\alpha)} = \epsilon_{p^d}{}^{[(N(\mathfrak{Q})-1)/p^a]\nu_{\mathfrak{Q}}(\alpha)}.$$

Since $\mathrm{ind}_q D = p^b$ and the inflation map does not change the class of D in $B(K)$ then $(\alpha, \epsilon_{p^d})_q$ is forced to be a p^b-th root in unity [**15**, Corollary 30.7, p. 261]. Hence: $|N(\mathfrak{Q}) - 1|_p \leqq p^{a+d-b}$ is forced. Since $N(\mathfrak{Q}) = q^f$ where f is the residue class degree of q in K/Q then $|q-1|_p \leqq p^{a+d-b}$ which is (1).

Now, let N' denote the norm in $K_{\mathfrak{Q}}$ over $Q_q(\epsilon_{p^a})$, and let $\mathfrak{Q}'$ be a $Q(\epsilon_{p^a})$-prime below $\mathfrak{Q}$. Since L/K is cyclotomic we may assume that $Q(\sqrt[p^d]{\alpha})/Q$ is abelian without loss of generality. Thus, by [**2**, Proposition 12-2-5, p. 221] we have:

$$(\alpha, \epsilon_{p^d})_{\mathfrak{Q}} = (\alpha, N'(\epsilon_{p^d}))\mathfrak{Q}' = (\alpha, \epsilon_{p^d})_{\mathfrak{Q}'}{}^{|K_q : Q_{\mathfrak{Q}}(\epsilon_{p^a})|}$$

where the latter equality holds since $d \leqq a$. On the other hand if N''

denotes the norm in $Q(\epsilon_{p^a})/Q$ then we have:

$$(\alpha, \epsilon_{p^d})_{\mathfrak{Q}'} = (\epsilon_{p^d}/\mathfrak{Q}')^{\nu_{\mathfrak{Q}'}(\alpha)} = \epsilon_{p^d}^{[(N''(\mathfrak{Q}')-1)/p^a]\nu_{\mathfrak{Q}'}(\alpha)}.$$

Hence:

$$(\alpha, \epsilon_{p^d})_{\mathfrak{Q}} = \epsilon_{p^d}^{[(N''(\mathfrak{Q}')-1)/p^a][\nu_{\mathfrak{Q}'}(\alpha)]\,|K_{\mathfrak{Q}}:Q_q(\epsilon_{p^a})|}.$$

Since (α, ϵ_{p^d}) must be a p^b-th root of unity and we have shown that

$$|q - 1|_p = p^c \leqq p^{a+d-b}$$

then it must follow that:

$$|K_{\mathfrak{Q}} : Q_q(\epsilon_{p^a})|_p = \min\{p^{d-b}, p^{a-c+d-b}\}.$$

This completes the case: $q \neq 2$ or $p \neq 2$.

Now if $p = q = 2$ then $a = b = c = d = 1$ and $c = 0$. Therefore (1) trivially holds. We now demonstrate that (2) holds; i.e. that $|K_{\mathfrak{Q}} : Q_2|_2 = 1$. We have $(\alpha, -1)_2 = -1$. Now, since L/K is cyclotomic we may assume $Q(\sqrt{\alpha})/Q$ is abelian. Thus we may use [**2**, Proposition 12-2-5, p. 221] to get

$$(\alpha, -1)_{\mathfrak{Q}} = (\alpha, N(-1))_2$$

where N denotes the norm in $K_{\mathfrak{Q}}/Q_2$. Hence $N(-1) = -1$ which ensures that $|K_{\mathfrak{Q}} : Q_2|_2 = 1$. This completes the proof of the necessity.

Conversely, we assume $[D] \in S(K)$ with non-trivial local indicies at the primes of $T = \{q_1, q_2, \ldots, q_s\}$. Also for each q in T we assume (1) and (2) hold. Now, we assume without loss of generality that $[D] \in S(K)_p$. To see this we suppose that for each prime p_i dividing m we find a cyclotomic division algebra $D_i = (L_i/K, \epsilon_i)$ with index $|m|_{p_i}$. Then we let L be the compositum of the L_i. Thus,

$$D \sim D_1 \otimes \ldots \otimes D_s \sim (L/K, \pi_i \inf^{(i)} \epsilon_i)$$

where $\inf^{(i)}$ is the inflation map from L_i to L. We note that L/K is cyclic since it is the compositum of cyclic extensions of relatively prime degrees and clearly $\pi \inf^{(i)} \epsilon_i$ is a root of unity in K. Thus D is the required division algebra.

Now we assume $[D] \in S(K)_p$ with $\mathrm{ind}_{q_i} D = p^{b_i}$ for each $q_i \in T$. First we prove that for each odd prime $q_i \in T$ we have the existence of a field L_i in $K(\epsilon_{q_i})$ with degree p^{b_i} over K. Assume that the claim is false; i.e.,

$$|K(\epsilon_{q_i}) : K| < p^{b_i}.$$

Let c_K be the tame ramification index of $\mathfrak{Q}_i$ in K/Q where $\mathfrak{Q}_i \cap Q = (q_i)$. Thus we have:

$$|q_i - 1|_p \leqq |K(\epsilon_{q_i}) : K|_p |c_K|_p < p^{b_i} |c_K|_p.$$

https://doi.org/10.4153/CJM-1981-082-5 Published online by Cambridge University Press

However, by [**16**, Theorem 4.4] we have that p^{b_i} divides $|q_i - 1|_p / |c_K|_p$. Therefore:

$$|q_i - 1|_p \geqq p^{b_i}|c_K|_p.$$

We conclude that $|q_i - 1|_p > |q_i - 1|_p$, a contradiction which establishes the claim.

Hence for each odd $q_i \in T$ we have the existence of a subfield L_i of $K(\epsilon_{q_i})$ with degree p^{b_i} over K. From [**16**, Theorem 6.1, p. 89] we have $\epsilon_{p^{b_i}}$ is in K and so by Kummer theory $L_i = K(\beta_i)$ where $\beta_i^{p^{b_i}} \in K$.

Now set $\beta = \delta \prod \beta_i$ where the product, $\prod$, ranges over all i such that $q_i \in T$ is odd and where; if $p^a = 2$ then:

$$\delta = \begin{cases} \sqrt{-2} \text{ if } 2 \in T \text{ and } |T|_2 > 1 \\ \sqrt{-r} \text{ if } 2 \notin T \text{ and } |T|_2 = 1 \\ \sqrt{r} \quad \text{if } 2 \in T \text{ and } |T|_2 = 1 \end{cases}$$

where r is a prime with even residue class degree in K/Q and $r \equiv 3 \pmod 4$. Otherwise $\delta = 1$. We note that such an r exists since $|T|_2 = 1$ forces $|K : Q|_2 > 1$ by the Hasse sum theorem.

Now let $C = (K(\beta)/K, \epsilon_{p^a})$. We note that $[C] \in S(K)$ by [**16**]. Moreover $\beta^{p^d} \in K$. Therefore $|K(\beta) : K| \leqq p^d$. But some $q_i \in T$ is ramified of degree p^d in $K(\beta)/K$ so that $|K(\beta) : K| = p^d$. Furthermore; $K(\beta)$ is cyclotomic over K. By Kummer theory $K(\beta) = K(\sqrt[p^d]{\alpha})$ for some $\alpha \in K^*$. By the use of the inflation map we get that

$$C \sim B = (K(\sqrt[p^a]{\alpha})/K, \epsilon_{p^d}).$$

First we show that B has the same Hasse invariants as D. Let $q \neq p$ be a finite prime in T with $\text{ind}_q D = p^b$, and let $\mathfrak{Q}$ be a K-prime above q. Then by properties of the norm and power residue symbols we have:

$$(\alpha, \epsilon_{p^d})_{\mathfrak{Q}} = (\alpha, N(\epsilon_{p^d}))_{\hat{\mathfrak{Q}}}$$

where $\mathfrak{Q} \cap Q(\epsilon_{p^a}) = \hat{\mathfrak{Q}}$ and N denotes the norm in $K_{\hat{\mathfrak{Q}}}/Q_q(\epsilon_{p^a})$. Since $d \leqq a$ then:

$$(\alpha, \epsilon_{p^d})_{\mathfrak{Q}} = (\alpha, \epsilon_{p^d})_{\hat{\mathfrak{Q}}}^{|K_{\mathfrak{Q}} : Q_q(\epsilon_{p^a})|}.$$

However:

$$(\alpha, \epsilon_{p^d})_{\hat{\mathfrak{Q}}} = (\epsilon_{p^d}/\hat{\mathfrak{Q}})^{v_{\hat{\mathfrak{Q}}}(\alpha)} = \epsilon_{p^d}^{[(\hat{N}(\hat{\mathfrak{Q}})-1)/p^a] v_{\hat{\mathfrak{Q}}}(\alpha)}$$

where $\hat{N}$ denotes the norm in $Q(\epsilon_{p^a})/Q$.
Hence:

$$(\alpha, \epsilon_{p^d})_{\mathfrak{Q}} = \epsilon_{p^d}^{[(\hat{N}(\hat{\mathfrak{Q}})-1)/p^a] v_{\hat{\mathfrak{Q}}}(\alpha) |K_{\mathfrak{Q}} : Q_q(\epsilon_{p^a})|}.$$

Now (1) and (2) of the hypothesis guarantees that $(\alpha, \epsilon_{p^d})_{\mathfrak{Q}}$ is a p^b-th root of unity. We have that $\text{ind}_q B = \text{ind}_q D$. By raising B to an appropriate power, say s, we get $\text{inv} B^s = \text{inv}_{\mathfrak{Q}} D$ for a given K-prime $\mathfrak{Q}$ above q.

https://doi.org/10.4153/CJM-1981-082-5 Published online by Cambridge University Press

It remains to show that $\operatorname{ind}_t B = 1$ for all $t \notin T$ and if 2 or ∞ is in T then the local index at 2 and/or ∞ is 2. Since a unit is a norm in an unramified extension then by the choice of B it remains to check for only 2 and ∞. However, $\operatorname{ind}_2 C > 1$ or $\operatorname{ind}_\infty C > 1$ only if we have $p^a = 2$. Thus we assume:

$$B = (K(\sqrt{\alpha})/K, -1) = (K(\delta(\sqrt{\pi q_i}))/K, -1).$$

In what follows $\mathscr{R}$ denotes a K-prime above r, $\mathscr{S}$ denotes a K-prime above 2, and $\mathscr{T}$ denotes a K-prime above ∞. We note that from (1) of the hypothesis it follows that $\beta_i = -q_i$ where $q_i \equiv 3 \pmod 4$ for each i such that $q_i \in T$ is odd. Now we treat the remaining cases.

Case 1. $2 \in T$ and $|T|_2 > 1$. By [**2**], op. cit.

(a) If $\infty \in T$:

$$(\alpha, -1)_{\mathscr{S}} = (-2\pi q_i, -1)_2 = (-1, -1)_2(2, -1)_2\pi(q_i, -1)_2 = (-1, -1)_2 = -1$$

since the number of q_i is even and $(2, -1)_2 = 1$. $(\alpha, -1)_{\mathscr{T}} = -1$ since $\alpha < 0$.

(b) If $\infty \notin T$:

$$(\alpha, -1)_{\mathscr{S}} = (2\pi q_i, -1)_2 = (2, -1)_2\pi(q_i, -1)_2 = -1$$

since the number of q_i is odd. $(\alpha, -1)_{\mathscr{T}} = 1$ since $\alpha > 0$.

Case 2. $2 \in T$ and $|T|_2 = 1$.

(a) If $\infty \in T$:

$$(\alpha, -1)_{\mathscr{S}} = (-r\pi q_i, -1)_{\mathscr{S}} = (-r\pi q_i, -1)_2 = -(r, -1)_2\pi(q_i, -1)_2 = -1$$

since the number of q_i is odd and $r \equiv 3 \pmod 4$.

$$(\alpha, -1)_{\mathscr{T}} = -1 \quad \text{since } \alpha < 0.$$

$$(\alpha, -1)_{\mathscr{R}} = (\alpha, 1)_r = 1$$

since r has even residue class degree in K over Q.

(b) If $\infty \notin T$:

$$(\alpha, -1)_{\mathscr{S}} = (r\pi q_i, -1)_{\mathscr{S}} = (r\pi q_i, -1)_2 = (r, -1)_2\pi(q_i, -1)_2 = (r, -1)_2 = -1$$

since the number of q_i is even.

$$(\alpha, -1)_{\mathscr{T}} = 1 \quad \text{since } \alpha > 0.$$

$$(\alpha, -1)_{\mathscr{R}} = (\alpha, 1)_r = 1$$

since r has even residue class degree in K over Q.

Case 3. $2 \notin T$ and $|T|_2 = 1$.

(a) If $\infty \in T$:

$$(\alpha, -1)_{\mathscr{S}} = (-r\pi q_i, -1)_{\mathscr{S}} = (-r\pi q_i, \pm 1)_2 = 1$$

https://doi.org/10.4153/CJM-1981-082-5 Published online by Cambridge University Press

since the number of q_i is even.

$$(\alpha, -1)_{\mathscr{T}} = -1 \quad \text{since } \alpha < 0.$$

$$(\alpha, -1)_{\mathscr{R}} = (\alpha, 1)_r = 1$$

since r has even residue class degree in K over Q.

(b) $\infty \notin T$:

$$(\alpha, -1)_s = (r\pi q_i, -1)_s = (r\pi q_i, -1)_2 = 1$$

since the number of q_i is odd and $r \equiv 3 \pmod 4$.

$$(\alpha, -1)_{\mathscr{T}} = 1 \quad \text{since } \alpha > 0.$$

$$(\alpha, -1)_{\mathscr{R}} = (\alpha, 1)_r = 1$$

since r has even residue class degree in K over Q.

Case 4. $2 \notin T$ and $|T|_2 > 1$.

(a) If $\infty \in T$:

$$(\alpha, -1)_{\mathscr{S}} = (-\pi q_i, -1)_{\mathscr{S}} = (-\pi q_i, \pm 1)_2 = 1$$

since the number of q_i is odd.

$$(\alpha, -1)_{\mathscr{T}} = -1 \text{ since } \alpha < 0.$$

(b) $\infty \notin T$:

$$(\alpha, -1)_{\mathscr{S}} = (\pi q_i, -1)_{\mathscr{S}} = (\pi q_i, \pm 1)_2 = 1$$

since the number of q_i is even.

$$(\alpha, -1)_{\mathscr{T}} = 1 \text{ since } \alpha > 0.$$

We have proved that B and D have the same invariants. Thus $C \sim B \sim D$, since C is a division algebra then C is K-isomorphic to D. However, C is a cyclotomic division algebra. This completes the proof.

In the following corollary $S(K, q)$ denotes the subgroup of $S(K)$ consisting of all elements having t-local index equal to 1 for all primes $t \neq q$. The following is immediate from the theorem.

COROLLARY 1. *If $[D] \in S(K, q)$ then D is a cyclotomic division algebra if and only if for each prime p, dividing* $\operatorname{ind}_q D$ *we have:*

$$q \not\equiv 1 \pmod{p^{a+1}} \quad \textit{and} \quad |K_{\mathscr{Q}} : Q_q(\epsilon_{p^a})|_p = 1$$

for each K-prime $\mathscr{Q}$ above q.

We note that when K/Q is abelian the above is linked to the existence of a splitting field for an absolutely irreducible character of a finite group of given exponent, (see [**13**]).

The following is immediate from Corollary 1.

COROLLARY 2. *If $[D] \in S(K, q)$ is a cyclotomic division algebra then $D = C \otimes K$ where $[C] \in S(Q(\epsilon_{p^a}))$ and C is a cyclotomic division algebra.*

https://doi.org/10.4153/CJM-1981-082-5 Published online by Cambridge University Press

We now show that the converse of Corollary 2 does not hold. In the following example $K = Q(\epsilon_{12})$, $q = 5$, $p = 2$ and $C = (Q(\epsilon_{20})/Q(\epsilon_4), \epsilon_4)$. From [**16**, Lemma 8.5] we have that $\text{ind}_5\, C = 4$ and $\text{ind}_r\, C = 1$ for all $r \neq 5$. Since $|K_{\mathfrak{Q}} : Q_5(\epsilon_4)| = 2$ then

$$\text{ind}_5\,(C \otimes K) = 2 \quad \text{and} \quad \text{ind}_r\,(C \otimes K) = 1 \quad \text{for all} \quad r \neq 5;$$

i.e., $[C \otimes K] \in S(K, 5)$ is a quaternion division algebra. Moreover C is clearly a cyclotomic division algebra by Corollary 1. However $C \otimes K$ is not cyclotomic since $|K_{\mathfrak{Q}} : Q_5(\epsilon_4)|_2 > 1$. This completes the example.

Now we prove a result which we link to the main result. This provides necessary and sufficient conditions for $S(k_{\hat{\mathfrak{Q}}})_p$ to be induced from $S(F_{\mathfrak{Q}})_p$ where F is a subfield of K and $\hat{\mathfrak{Q}}$ is a K-prime with $\hat{\mathfrak{Q}} \cap F = \mathfrak{Q}$. In the following theorem $f(\hat{\mathfrak{Q}})$ denotes the residue class degree of $\hat{\mathfrak{Q}}$ in K/F, and $\hat{\mathfrak{Q}} \cap Q = (q)$.

THEOREM 2. *If* $S(K_{\hat{\mathfrak{Q}}})_p \neq 1$ *then:*
$S(K_{\hat{\mathfrak{Q}}})_p = S(F_{\mathfrak{Q}})_p \otimes K_{\hat{\mathfrak{Q}}}$ *if and only if:*
(i) $|f(\hat{\mathfrak{Q}})|_p = 1$ *when* $q \neq 2$;
(ii) $|K_{\hat{\mathfrak{Q}}} : F_{\mathfrak{Q}}|_p = 1$ *when* $q = 2$.

Proof. Assume $S(K_{\hat{\mathfrak{Q}}})_p = S(F_{\mathfrak{Q}})_p \otimes K_{\hat{\mathfrak{Q}}}$. First we assume $q \neq 2$ and set $|q - 1|_p = p^s$. Let c_K (respectively c_F) denote the tame ramification index of $K_{\hat{\mathfrak{Q}}}/Q_q$ (respectively $F_{\hat{\mathfrak{Q}}}/Q_q$) and set $|c_K|_p = p^s$ (respectively $|c_F|_p = p^t$). By [**16**, Theorem 4.4] there exists $[A] \in S(K_{\hat{\mathfrak{Q}}})_p$ with $\text{ind}_q A = p^{d-s}$. Since $A \sim B \otimes K_{\hat{\mathfrak{Q}}}$ where $[B] \in S(F_{\mathfrak{Q}})_p$ by hypothesis, then $\text{ind}_q B \leqq p^{d-t}$ by [**16**, Theorem 4.4′]. Now $S(K_{\hat{\mathfrak{Q}}})_p \neq 1$ guarantees $d > s$. Therefore:

$$1 < p^{d-s} = \text{ind}_q A = \text{ind}_q (B \otimes K_{\mathfrak{Q}}) \leqq \max\{1, (p^{d-t})/|K_{\hat{\mathfrak{Q}}} : F_{\mathfrak{Q}}|_p\}$$
$$= \max\{1, (p^{d-s})/|f(\hat{\mathfrak{Q}})|_p\}.$$

Hence $|f(\hat{\mathfrak{Q}})|_p = 1$ which is (i).

On the other hand if $q = 2$ then $S(K_{\hat{\mathfrak{Q}}})_p \neq 1$ implies $p = 2$, and $S(K_{\hat{\mathfrak{Q}}})_2$ is the subgroup of $B(K_{\hat{\mathfrak{Q}}})_2$ of order 2 by [**16**, Theorem 5.14]. Let $[A] \in S(K_{\hat{\mathfrak{Q}}})_2$ with $\text{ind}_2 A = 2$. By hypothesis $A \sim B \otimes K_{\hat{\mathfrak{Q}}}$ with $[B] \in S(F_{\mathfrak{Q}})$; i.e.,

$$\text{inv}\, A = \text{inv}\, B \otimes K_{\hat{\mathfrak{Q}}} = |K_{\hat{\mathfrak{Q}}} : F_{\mathfrak{Q}}|\ \text{inv}\, B \pmod 1.$$

Clearly then $|K_{\hat{\mathfrak{Q}}} : F_{\mathfrak{Q}}| = 1$ which is (ii).

Conversely if $q \neq 2$ then by [**16**, Theorem 4.4′] $S(K_{\hat{\mathfrak{Q}}})_p$ is the subgroup of $B(K_{\hat{\mathfrak{Q}}})$ of order p^b where $p^b = |(q-1)/c_K|_p$. Since $|f(\hat{\mathfrak{Q}})|_p = 1$ then $S(F_{\mathfrak{Q}})_p \otimes K_{\hat{\mathfrak{Q}}}$ is the subgroup of order p^b; i.e.,

$$S(K_{\hat{\mathfrak{Q}}})_p = S(F_{\mathfrak{Q}})_p \otimes K_{\hat{\mathfrak{Q}}}.$$

When $q = 2$, $S(K_{\hat{\mathfrak{Q}}})_p \neq 1$ implies $p = 2$ and $S(K_{\hat{\mathfrak{Q}}})_2$ is equal to $S(k) \otimes K_{\hat{\mathfrak{Q}}} \cong S(k)$ where k is the maximal cyclotomic extension of Q_2

https://doi.org/10.4153/CJM-1981-082-5 Published online by Cambridge University Press

contained in $K_{\hat{2}}$, by [**16**, Theorem 5.15]. Moreover $|K_{\hat{2}} : k|_2 = 1$. By [**16**, Theorem 5.14] $S(k)$ is the unique subgroup of $B(k)$ of order 2. Since, by hypothesis $|K_{\hat{2}} : F_2|_2 = 1$ we need only verify that $S(F_2 \cap k)$ is the unique subgroup of $B(F_2 \cap k)$ of order 2, because $F_2 \cap k$ is the maximal cyclotomic extension of Q_2 contained in F_2, and $|F_2 : F_2 \cap k|_2 = 1$. Since $S(k) \neq 1$ then there exists a root of unity δ such that the inertia group of $Q_2(\delta)/k$ is not cyclic. Therefore the inertia group of $Q_2(\delta)/(k \cap F_2)$ is not cyclic. Therefore by [**16**, Theorem 5.14] $S(F_2 \cap k)$ is the unique subgroup of $B(F_2 \cap k)$ of order 2.

An immediate consequence is the next result which links Theorems 1 and 2, and restates Corollary 2 in different form.

COROLLARY 3. *If $S(K, q)$ is represented by a cyclotomic division algebra then*

$$S(K_{\hat{2}})_p = S(Q_q(\epsilon_{p^a}))_p \otimes K_{\hat{2}}.$$

Now we present a counterexample to the converse of Corollary 3. Let K be the subfield of $Q(\epsilon_{57})$ of degree 3 over $Q(\epsilon_3)$. By Theorem 2 we get

$$S(K_{\hat{2}})_3 = S(Q_{19}(\epsilon_3))_3 \otimes K_{\hat{2}}$$

where $\hat{\mathcal{Q}} \cap Q = (19)$. However $19 \equiv 1 \pmod 9$ implies by Corollary 1 that $S(K, 19)_3$ is not represented by a cyclotomic division algebra.

It is worth noting at this juncture that there does not exist a field K such that $S(K)_p$ has every class represented by a cyclotomic division algebra. This is in contrast to the fact that for every field K, $S(K)$ is represented by a cyclotomic algebra in the sense of [**15**]. To see this let us assume without loss of generality that $m \not\equiv 2 \pmod 4$. Choose a prime q such that $q \equiv 1 \pmod{p^{a+1}}$ where ϵ_{p^a} is the largest p-power root of unity in K, as before. Moreover assume $q \equiv 1 \pmod m$. Now there exists $[C] \in S(Q(\epsilon_{p^a}))_p$ with $\text{ind}_q\, C = p^a$, and by the choice of q, $[C \otimes K] \in S(K)$ with $\text{ind}_q [C \otimes K] = p^a$. However $q \equiv 1 \pmod{p^{a+1}}$, so by Theorem 1, $[C \otimes K]$ cannot be represented by a cyclotomic division algebra. Thus we have presented an example for each prime p to show that there does not exist a field K such that every class of $S(K)_p$ is represented by a cyclotomic division algebra.

Now we set the stage for the final result. Let K be an algebraic number field with no real infinite primes. Then -1 is totally positive and so can be written as a sum of four or fewer squares. The smallest number of squares possible in such a representation of -1 is called the *stufe of* K, and is denoted by $s(K)$. It is well known that $s(K) = 1$, 2 or 4. If $s(K) = 1$ then ϵ_4 is in K. Now we present a result which will link the concept of the stufe of K to the existence of non-trivial $S(K, 2)$.

THEOREM 3. *Let K be an algebraic number field with no real infinite primes. If $S(K, 2)$ is represented by a non-trivial cyclotomic division algebra then $s(K) = 4$.*

Proof. Since $S(K, 2) \neq 1$ then ϵ_4 is not in K, (see [**16**]). Therefore $s(K) = 2$ or 4.

Now, $s(K) = 2$ if and only if -1 is a norm in $K(\sqrt{-1})/K$. By the Hasse norm theorem the latter occurs if and only if $(-1, -1)_{\mathfrak{P}} = 1$ for all K-primes $\mathfrak{P}$. By invoking [**2**] op. cit. we get $(-1, -1)_{\mathfrak{P}} = (-1, N(-1))_p$ where N denotes the norm in $K_{\mathfrak{P}}/Q_p$ and $\mathfrak{P} \cap Q = (p)$. Thus $(-1, N(-1))_p = 1$ for all $p > 2$ and $(-1, N(-1))_2 = 1$ if and only if $|K_{\mathfrak{Q}} : Q_2|_2 > 1$ for all K-primes $\mathfrak{Q}$ above 2. We have shown that $s(K) = 2$ if and only if $|K_{\mathfrak{Q}} : Q_2|_2 > 1$ for all K-primes $\mathfrak{Q}$ above 2. (As a matter of interest this is [**1**, Theorem, p. 20]). Thus $s(K) = 4$ if and only if $|K_{\mathfrak{Q}} : Q_2|_2 = 1$ for some K-prime $\mathfrak{Q}$ above 2. Invoking Corollary 1 now yields the theorem.

The following is a counterexample to the converse of Theorem 3.

Let $K = Q(\theta)$ where θ is a complex root of $f(x) = x^3 - 11$. It can be verified that 2 splits into two primes $\mathfrak{P}_1$ and $\mathfrak{P}_2$ of K where $\mathfrak{P}_1$, say, has relative degree 1, and $\mathfrak{P}_2$ has relative degree 2. Thus $|K_{\mathfrak{P}_1} : Q_2| = 1$ which implies $s(K) = 4$. However by Corollary 1, $|K_{\mathfrak{P}_2} : Q_2| = 2$ implies that $S(K, 2)$ is not represented by a cyclotomic division algebra. This completes the counterexample.

We now make a suitable restriction on K to render $s(K) = 4$ as a necessary and sufficient condition for $S(K, 2)$ to be represented by a non-trivial cyclotomic division algebra.

COROLLARY 4. *Let K be a finite normal extension of Q, with no real infinite primes. Then $S(K, 2)$ is represented by a non-trivial cyclotomic division algebra if and only if $s(K) = 4$.*

Proof. From the proof of Theorem 3 we have $s(K) = 4$ if and only if $|K_{\mathfrak{Q}} : Q_2|_2 = 1$ for some K-prime $\mathfrak{Q}$ above 2. However since K/Q is normal then $|K_{\mathfrak{Q}} : Q_2|_2 = 1$ for some K-prime above 2 if and only if $|K_{\mathfrak{Q}} : Q_2|_2 = 1$ for all K-primes above 2. By Corollary 1 the proof is complete.

Acknowledgement. The author welcomes the opportunity to thank the referee for remarks which led to a generalization of the results in the paper from abelian extensions of the rationals to arbitrary number fields.

REFERENCES

1. I. Connell, *The Stufe of number fields*, Math. Z. *124* (1972), 20–22.
2. L. J. Goldstein, *Analytic number theory* (Prentice Hall, Englewood Cliffs, N.J., 1971).

3. G. Janusz, *Algebraic number fields* (Academic Press, New York, 1973).
4. R. Mollin, *Uniform distribution and the Schur subgroup*, J. Algebra *42* (1976), 261–277.
5. ——— *Uniform distribution and real fields*, J. Algebra *43* (1976), 155–167.
6. ——— *Algebras with uniformly distributed invariants*, J. Algebra *44* (1977), 271–282.
7. ——— *$U(K)$ for a quadratic field K*, Communications in Algebra *4* (1976), 747–759.
8. ——— *Generalized uniform distribution of Hasse invariants*, Communications in Algebra *5* (1977), 245–266.
9. ——— *Herstein's conjecture, automorphisms and the Schur group*, Communications in Algebra *6* (1978), 237–248.
10. ——— *The Schur group of a field of characteristic zero*, Pacific J. Math. *76* (1978), 471–478.
11. ——— *Uniform distribution classified*, Math. Z. *165* (1979), 199–211.
12. ——— *Induced p-elements in the Schur group*, Pacific J. Math. *90* (1980), 169–176.
13. ——— *Splitting fields and group characters*, J. reine angew Math. *315* (1980) 107–114.
14. ——— *Cyclotomic splitting fields* (to appear: Canadian Mathematical Bulletin).
15. I. Reiner, *Maximal orders* (New York, Wiley Interscience, 1972).
16. T. Yamada, *The Schur subgroup of the Brauer group*, Lecture Notes in Mathematics *397* (Springer, Berlin, Heidelberg, New York, 1974).

Queen's University,
Kingston, Ontario