Canad. Math. Bull. Vol. **25** (2), 1982

CYCLOTOMIC SPLITTING FIELDS

BY
R. A. MOLLIN

ABSTRACT. Let D be a division algebra whose class $[D]$ is in $B(K)$, the Brauer group of an algebraic number field K. If $[D \otimes_K L]$ is the trivial class in $B(L)$, then we say that L is a *splitting field* for D or L *splits* D. The splitting fields in D of smallest dimension are the *maximal subfields* of D. Although there are infinitely many maximal subfields of D which are cyclic extensions of K; from the perspective of the *Schur Subgroup* $S(K)$ of $B(K)$ the natural splitting fields are the cyclotomic ones. In (*Cyclotomic Splitting Fields*, Proc. Amer. Math. Soc. **25** (1970), 630–633) there are errors which have led to the main result of this paper, namely to provide necessary and sufficient conditions for (D) in $S(K)$ to have a maximal subfield which is a cyclic cyclotomic extension of K, a finite abelian extension of Q. A similar result is provided for quaternion division algebras in $B(K)$.

Introduction. In this paper we are interested in cyclic cyclotomic splitting fields for division algebras. In [6, Th. 4.7, p. 757], [7, Th. 4.2, p. 207], [8, Th. 4, p. 113] and [9] we demonstrated the importance of obtaining such maximal subfields from the point of view of explicit construction of crossed product division algebras. In [11] M. Schacher gave examples of division algebras D of exponent p for each prime p with $[D] \in B(K)$ such that D does *not* have a maximal subfield which is imbedded in a cyclotomic extension of K. However there are errors in the main results of [11] which have led us to formulate the following.

In this paper we present necessary and sufficient conditions for a division algebra D with $[D] \in S(K)$ to have a maximal subfield which is a cyclic cyclotomic extension of K where K is a finite abelian extension of the field Q of rational numbers.

Moreover, for $[D] \in B(K)$ with K a finite non-real abelian extension of Q where D is a quaternion division algebra we provide necessary and sufficient conditions for D to have a maximal subfield which is a cyclic cyclotomic extension of K.

1. Notation and preliminaries. Let K be a field of characteristic zero. The Schur group $S(K)$ may be described as consisting of those equivalence classes

Received by the editors September 16, 1980.
AMS (MOS) Subject Classification Numbers: Primary: 16A26; Secondary: 16A65.
Key Words and Phrases: Cyclotomic field, splitting field, division algebra, maximal subfield.
The author's research is supported by an N.S.E.R.C. University Research Fellowship.

in $B(K)$ which contain a simple component of the group algebra KG for some finite group G. For basic results concerning $S(K)$ the reader is referred to [14].

When K is an algebraic number field the elements $[A]\in B(K)$ are uniquely characterized by their Hasse invariants. A certain subgroup of $B(K)$ has a particularly nice relationship between these invariants. We describe it as follows:

Let K be a finite abelian extension of Q. $U(K)$, called the *absolute uniform distribution group for* K, denotes the subgroup of $B(K)$ consisting of those equivalence classes $[A]$ such that:

(i) If the index of A is n then ε_n is in K, where ε_n denotes a primitive nth root of unity, and

(ii) If P is a K-prime above the rational prime p and $\sigma\in G(K/Q)$, the Galois group of K over Q, with $\varepsilon_n^{\sigma}=\varepsilon_n^{b}$ then the *Hasse P-invariant* of A satisfies:

$$\operatorname{inv}_P A \equiv b \operatorname{inv}_{P^\sigma} A \pmod 1.$$

If $[A]\in U(K)$ and P and P' are K-primes above the rational prime p then $A\otimes_K K_P$ and $A\otimes_K K_{P'}$ have the same index, where K_P denotes the completion of K at p. The common values of the indicies $A\otimes_K K_P$ for all K-primes P above p is called the *p-local index* of A, denoted $\operatorname{ind}_P A$.

We studied the relationship between $S(K)$ and $U(K)$ of which it is a subgroup in [4]–[9].

If $[A]\in B(K)$ and $\operatorname{inv}_P A>0$ for aK-prime P then we say that P is *ramified in* A, (see [10, p. 272]). Since we shall be concerned with K/Q finite abelian then we may say that p is ramified in A where p is the rational prime below P, whenever $\operatorname{inv}_P A>0$ for some K-prime P.

The *norm-residue symbol* at P is denoted $(*,*)_P$ and the *Legendre symbol* is denoted $(/)$.

Throughout the remainder of the paper we shall be concerned with finite abelian extensions K of Q. A field extension K of F shall be denoted K/F. Since the decomposition of an F-prime in K essentially depends on the rational prime q which sits below it then we shall write F_q to denote the completion of K at an F-prime above q. Similarly K_q shall denote the completion of a K-prime above the given F-prime.

If G is a group and p is a prime then G_p shall denote the Sylow p-subgroup of G. If $m=p^a t$ where p and t are relatively prime then $|m|_p=p^a$, i.e. $|m|_p$ denotes the highest power of p dividing the integer m.

A crossed product algebra is denoted by $(L/K,\beta)$. This is the central simple K-algebra having L-basis u_τ with $\tau\in G(L/K)=G$ subject to:

$$u_\tau u_\sigma=\beta(\tau,\alpha)u_{\tau\sigma},\qquad \tau,\sigma\in G$$

and

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

https://doi.org/10.4153/CMB-1982-031-3 Published online by Cambridge University Press

Moreover a crossed product of the form $(K(\varepsilon)/K, \beta)$ where ε is a root of unity and the values of β are roots of unity in $K(\varepsilon)$ are called *cyclotomic algebras*. These are the algebras which characterize $S(K)$, (see [14]).

When G is cyclic then $(L/K, \beta)$ denotes the cross product in which:

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

For further information on crossed products the reader is referred to [10]. Finally equivalence in $B(K)$ will be denoted by $\sim$.

2. Splitting fields for quaternion division algebras. Let K/Q be finite abelian and let D be a division algebra with $[D] \in B(K)$. We note that to ask whether D has a maximal subfield which can be imbedded in a cyclotomic extension of K is rendered, by the Kronecker-Weber theorem, to be equivalent to asking whether D has a maximal subfield which is abelian over Q. We commence by asking whether a quaternion division algebra D has a maximal subfield abelian over Q. The answer is negative in general as the following counterexample illustrates.

Let $K = Q(\sqrt{-1}, \sqrt{3})$ and let $[D] \in B(K)$ (in fact $[D] \in U(K)$), with $\text{ind}_2 D = 2 = \text{ind}_3 D$, and $\text{ind}_p D = 1$ for all primes $p \ne 2, 3$. If a maximal subfield L of D exists such that L/Q is abelian then either:

(1) $G(L/Q) = Z_2 \oplus Z_2 \oplus Z_2$ or,

(2) $G(L/Q) = Z_2 \oplus Z_4$.

If (1) then $G(L_3/Q_3) = Z_2 \oplus Z_2 \oplus Z_2$. However, by [13, 6–5–4] this is not possible since Q_3 has only three quadratic extensions. Thus (2) holds and so one of $Q(\sqrt{-1})$, $Q(\sqrt{3})$ or $Q(\sqrt{-3})$ is imbedded in a cyclic extension of degree 4. By [1, Th. 6, p. 106], -1 must be a norm from one of these three fields. However, -1 cannot be a norm from an imaginary quadratic field. Therefore -1 must be a norm from $Q(\sqrt{3})$. Thus, by the Hasse norm theorem -1 must be a norm everywhere locally. However, $(3, -1)_3 = (-\frac{1}{3}) = -1$; i.e. -1 is not a norm from $Q_3(\sqrt{3})$, a contradiction which establishes the counterexample.

The above example is similar to [11, p. 632]. However the example therein is incorrect. We shall come back to this once we have the first result at our disposal. The following theorem provides necessary and sufficient conditions for a quaternion division algebra to have a maximal subfield abelian over Q. In what follows we shall use the term *maximal cyclic p-extension* of F in K to mean a proper subfield M of K such that $G(M/F)_p$ is cyclic, and if $F \subseteq M \subseteq N \subseteq K$ with $G(N/F)_p$ cyclic then $|N:M|_p = 1$.

THEOREM 2.1. *Let K/Q be finite non-real abelian, and let D be a quaternion division algebra with $[D] \in B(K)$. D has a maximal subfield which is abelian* *over Q if and only if for each odd prime q which ramifies in D with $G(K_q/Q_q)_2$ non-cyclic, there exists a maximal cyclic 2-extension F of Q in K such that:*

(a) -1 *is a norm in F/Q and,*

(b) q *is not completely split in F/Q.*

Proof. First we prove the necessity of (a) and (b). Suppose there exists a maximal subfield L of D such that L/Q is abelian. If q is an odd prime which ramifies in D with $G(K_q/Q_q)$ non-cyclic then by [13, 6-5-4], $G(L_q/Q_q)_2$ must be of the form $Z_{2^{m(1)}}\oplus Z_{2^{m(2)}}$ where $m(1)$ and $m(2)$ are positive integers. Thus there exist maximal cyclic 2-extension M_i of Q in L with $|M_i:Q|_2\geq 2^{m(i)}$ for $i=1,2$. One of M_1 or M_2 is not contained in K, say $M=M_1$. Therefore, if $M\cap K=F$ then $|M:F|=2$ and F is a maximal cyclic 2-extension of Q in K. By [1, Th. 6, p. 106] -1 is a norm in F/Q. Moreover since $G(K_q/Q_q)_2$ is non-cyclic then q is not completely split in F.

Conversely suppose (a) and (b) hold. Let $q(i)$ for $i=1,2,\ldots,m$ be all rational primes which ramify in D but do not ramify in K/Q. Set $\alpha(i)=q(i)$ for $i=1,2,\ldots,m$. Since $q(i)$ is ramified in $K(\sqrt{\alpha(1)\alpha(2)\cdots\alpha(m)})/K$ then $K(\sqrt{\alpha(1)\alpha(2)\cdots\alpha(m)})$ splits D at each $q(i)$ for $i=1,2,\ldots,m$.

Now consider $T=\{q(m+1),q(m+2),\ldots,q(n)\}$ where $q(i)$ is odd, ramified in D and, $G(K_{q(i)}/Q_{q(i)})_2$ is not cyclic for $i=m+1,m+2,\ldots,n$. We note that $q(i)$ splits in $K(\sqrt{\alpha(1)\alpha(2)\cdots\alpha(m)})/K$ for $i=m+1,m+2,\ldots,n$ since otherwise we would have a degree 8 extension of Q_q with Galois group of the form $Z_2\oplus Z_2\oplus Z_2$ which would contradict [13, 6-5-4]. Now, by hypothesis, for each $q(i)\in T$ there exists a maximal cyclic 2-extension $F^{(i)}$ of Q in K satisfying (a) and (b). Not all such $F^{(i)}$ are necessarily distinct, so we let $F^{(j)}$ for $j=m+1,\ldots,r$ with $m+1\leq r\leq n$ be all distinct such fields. Now we rearrange the elements of T as follows. Let

$$R(j)=\{q(i,j)\in T: i=m(j-1)+1,\ldots,m(j) \text{ with } m(m)=m \text{ and } m(r)=n\}$$

where $j=m+1,\ldots,r$, be the set of all elements of T which are not completely split in $F^{(j)}$ and which do not already appear in $R(k)$ for $m+1\leq k<j$. Since $G(K_{q(i)}/Q_{q(i)})_2$ is not cyclic for $i=m+1,\ldots,n$ then it is possible to ensure as well that $q(i,j)$ is completely split in $F^{(h)}$ for all $h\neq j$. Now, by hypothesis -1 is a norm from $F^{(j)}$ for $j=m+1,\ldots,r$. By [1, Th. 6, p. 106] $F^{(j)}$ is contained in $M^{(j)}$ where $|M^{(j)}:F^{(j)}|=2$ and $M^{(j)}$ is cyclic over Q. Since $F^{(j)}$ is a maximal cyclic 2-extension Q in K then $|M^{(j)}K:K|=2$ and by Kummer theory $M^{(j)}K=K\sqrt{\beta_j})$ for some $\beta_j\in K^*$. We note that since K/Q is abelian and $M^{(j)}/Q$ is cyclic then $M^{(j)}K/Q$ is abelian. Therefore by Kronecker-Weber $K(\sqrt{\beta_j})$ is contained in a cyclotomic extension of K. Now we choose $\alpha(m(j-1)+1=\beta_j$ and $\alpha(m(j-1)+2)=\cdots=\alpha(m(j))=1$ for $j=m+1,\ldots,r$, and set $\alpha(r+1)=\alpha(r+2)=\cdots=\alpha(n)=1$.

Finally we consider those remaining $q(i)$ for $i=n+1,\ldots,s$ which ramify in D. First we consider those $q(i)$ which are either odd or for which $G(K_{q(i)}/Q_{q(i)})_2$ is cyclic. If $q(i)$ does not split in $K(\sqrt{\alpha(1)\cdots\alpha(i-1)})/K$ then set $\alpha(i)=1$. Otherwise choose a prime $p(i)$ which is relatively prime to the discriminant of $K(\sqrt{\alpha(1)\cdots\alpha(i-1)})$ and such that $q(i)$ is inert in $Q(\sqrt{p(i)})$ while $q(j)$ splits in $Q(\sqrt{p(i)})$ for all $j<i$. Such $p(i)$ exist by Chinese remainder theorem considerations.

The only possible remaining case is $q(s)=2$ where $G(K_2/Q_2)_2$ is not cyclic. If 2 does not split in $K(\sqrt{\alpha(1)\cdots\alpha(s-1)})/K$ then set $\alpha(s)=1$. Let $\gamma=\alpha(1)\cdots\alpha(s-1)$.

Otherwise if $\sqrt{-1}\notin K$ set $\alpha(s)=\sqrt{-1}$ or $\alpha(s)=\sqrt{2}$ according as 2 is nonsplit in $K(\sqrt{-1\gamma})/K$ or $K(\sqrt{2\gamma})/K$. We note that 2 cannot be split in $K(\gamma)/K$, $K(\sqrt{-1\gamma})/K$ and $K(\sqrt{2\gamma})/K$ since in that case 2 could be split in $K(\varepsilon_8)/K$ contradicting $\sqrt{-1}\notin K$. If $\sqrt{-1}\in K$ and ε_{2^a} for $a>1$ is the largest 2-power root of unity in K then 2 does not split in $K(\varepsilon_{2^{a+1}}\gamma)/K$. In this case set $\alpha(s)=\varepsilon_{2^a}$.

By construction $L=K(\sqrt{\alpha(1)\cdots\alpha(s)})$ splits D at all primes which ramify in D, and L is abelian over Q. It follows that L is a maximal subfield of D which secures the theorem. Q.E.D.

We isolate a special case of Theorem 2.1 since it has a bearing on [11].

COROLLARY 2.2. *Let K be a biquadratic extension of Q. Then every quaternion division algebra in $U(K)$ has a maximal subfield which can be imbedded in a cyclotomic extension of Q if and only if either:*

(a) $|K_q:Q_q|=4$ *for at most one prime q, or*

(b) -1 *is a norm from one of the quadratic subfields of K.*

For example, for $K=Q(\sqrt{-1},\sqrt{7})$ then only prime q with $|K_q:Q_q|=4$ is $q=7$. Therefore by Corollary 2.2 every quaternion division algebra in $U(K)$ has a maximal subfield which is abelian over Q. This shows that the example [11, p. 632] is false, and that no such algebra $[D]\in U(K)$ can be found. The error stems from Schacher's claim that "... one easily checks that $G(K_2/Q_2)=G(K_7/Q_7)=Z_2\oplus Z_2$." In fact one checks that $G(K_2/Q_2)=Z_2$ since 2 splits in $Q(\sqrt{-7})$.

That K is restricted to being non-real in Theorem 2.1 is a result of problems which occur at 2 and the infinite rational primes. Similar problems were encountered in [8, Th. 1, p. 108] but resolved by a suitable restriction [8, Th. 2, p. 112]. In §3 we shall overcome the problem by considering a special subgroup $S(K)$ of $B(K)$.

3. Splitting fields and $S(K)$. In this section we restrict our attention to division algebras D with $[D]\in S(K)$ where K/Q is finite abelian.

In [8] we considered the following situation. Let χ be a complex irreducible character of a finite group G of exponent n. Let $A(\chi, Q)$ denote the simple component of QG corresponding to χ. We note that $[A(\chi, Q)] \in S(Q(\chi))$. R. Brauer's well known theorem which states that $Q(\varepsilon_n)$ is a splitting field for χ, inspired the following demanding question: Does the division algebra underlying $A(\chi, Q)$ have a maximal subfield L contained in $Q(\varepsilon_n)$? In general the answer is negative, and in [8] we provided sufficient conditions for such an L to exist. However, for each result which we obtained we were able to find counterexamples to the necessity of such conditions. In this paper we relax the demands on L. We merely require that L/Q be abelian, i.e. L may be imbedded in *any* cyclotomic extension of Q. In [2] B. Fein found counterexamples to the existence of such an L for each prime p. We now present for the first time necessary and sufficient conditions for such an L to exist.

THEOREM 3.1. *Let K/Q be finite abelian and let D be a division algebra of index m with $[D] \in S(K)$. D has a maximal subfield cyclic over K and abelian over Q if and only if for each odd prime q which ramifies in D and for each prime p dividing m with $G(K_q/Q_q)_p$ non-cyclic there exists a maximal cyclic p-extension F of $Q(\varepsilon_{p^c})$ in K where $|\mathrm{ind}_q D|_p = p^c$ such that*

(a) *ε_{p^c} is a norm in $F/Q(\varepsilon_{p^c})$ and*

(b) *q is not completely split in $F/Q(\varepsilon_{p^c})$.*

Proof. We note that if $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ where the p_i's are distinct primes then $D \sim D_1 \otimes \cdots \otimes D_r$ in $S(K)$ where the index of D_i is $p_i^{a_i}$ for $i = 1, 2, \ldots, r$. Thus it follows that we may assume without loss of generality that $m = p^b$.

First we prove the necessity of (a) and (b). Suppose $G(K_q/Q_q)_p$ is non-cyclic for odd q with $\mathrm{ind}_q D = p^c$ where $c \le b$. By [5, Th. 1.1, p. 273] $q \equiv 1 \pmod{p^c}$. If D has a maximal subfield abelian over Q and cyclic over K then by [13, 6-5-4] $G(L_q/Q_q)_p$ is forced to be of the form $Z_{p^{m(1)}} \oplus Z_{p^{m(2)}}$ where one of $m(1)$ or $m(2)$ is greater than c, say $m = m(1) > c$ and $m(2) > 0$. Therefore there exists a maximal cyclic p-extension M of $Q(\varepsilon_{p^c})$ in L with $|M:Q|_p > p^c$. Thus $M \cap K = F$ is a maximal cyclic p-extension of $Q(\varepsilon_{p^c})$ in K with $|M:F|_p = p^c$. By [1, Th. 6, p. 106] ε_{p^c} is a norm in $F/Q(\varepsilon_{p^c})$ and since $m > c$ then q is not completely split in $F/Q(\varepsilon_{p^c})$. This establishes the necessity.

Suppose $\mathrm{ind}_{q(i)} D = p^{c(i)}$ with $q(i)$ unramified in K/Q for $i = 1, 2, \ldots, m$. That there exists a subfield L_i of $K(\varepsilon_{q(i)})$ with $|L:K| = p^{c(i)}$ can be verified by exactly the same argument as in [8, Th. 1, p. 109]. By [14, Prop. 6.2, p. 89] we have $\varepsilon_{p^{c(i)}}$ is in K and so $L_i = K(\gamma(i))$ where $\gamma(i)^{p^{c(i)}} \in K$ for $i = 1, 2, \ldots, m$. Since $q(i)$ ramifies in L_i/K then L_i splits D at $q(i)$ for $i = 1, 2, \ldots, m$.

Now consider those primes $q(i)$ with $\mathrm{ind}_{q(i)} D = p^{c(i)}$ for $i = m+1, \ldots, n$ such that $q(i)$ is odd, and $G(K_{q(i)}/Q_{q(i)})_p$ is non-cyclic. Using (a) and (b) of the hypothesis we can use exactly the same kind of argument as in Theorem 2.1 to obtain fields L_i abelian over Q and cyclic over K such that L_i splits D at $q(i)$ for $i = m+1, \ldots, n$. Set $L_i = K(\gamma(i))$.

Now we consider the remaining odd primes $q(i)$ for $i=n+1,\ldots,s$ with $\operatorname{ind}_{q(i)} D=p^{c(i)}$. If $q(i)$ does not split in $K(\gamma(1)\cdots\gamma(i-1))$ then set $\gamma(i)=1$. Otherwise by [3, Prop. 5.2, p. 275] we may choose a prime $p_i\equiv 1 \pmod p$ such that $q(i)$ is not a pth power modulo p_i but $q(1), q(2),\ldots, q(i-1)$ are $p^{c(i)}$-th powers modulo p_i. Thus there exists a field M_i contained in $K(\varepsilon_{p_i})$ such that $|M_i:K|=p^{c(i)}$ with $q(i)$ inert in M_i/K and $q(j)$ completely split in M_i/K for all $j<i$. By Kummer theory $M_i=K(\gamma_{(i)})$ where $\gamma_{(i)}^{p^{c(i)}}\in K^*$. Set $\gamma'=\gamma(1)\cdots\gamma(s)$. Hence $K(\gamma(1)\cdots\gamma(s))$ splits D at $q(i)$ for $i=1,\ldots,s$.

If $\operatorname{ind}_2 D=2$ and $\operatorname{ind}_\infty D=1$ then set $\gamma'=\alpha$ if 2 does not split in $K(\gamma')/K$ and set $\sqrt{-1}\gamma'=\alpha$ otherwise. We note that by [14, Th. 5.11(II), p. 81] 2 is ramified in $K(\sqrt{-1})/K$. Hence if 2 splits in $K(\gamma')/K$ then 2 ramifies in $K(\sqrt{-1}\gamma)/K$.

If $\operatorname{ind}_\infty D=2$ and $\operatorname{ind}_2 D=1$ then set $\gamma'=\alpha$ if $K(\gamma')$ is non-real, and set $\sqrt{-1}\gamma'=\alpha$ otherwise. Clearly $K(\alpha)$ splits D at ∞.

Suppose $\operatorname{ind}_\infty D=2=\operatorname{ind}_2 D$. If 2 is not split in $K(\gamma')/K$ and $K(\gamma')$ is not real then set $\gamma'=\alpha$. If 2 splits in $K(\gamma')/K$ then 2 ramifies in $K(\sqrt{-1}\gamma')/K$, (ibid.). In this case set $\sqrt{-1}\gamma'=\alpha$. We note that by the choice of γ' it is not possible to have the case where $K(\gamma')$ is non-real but $K(\sqrt{-1}\gamma')$ is real. Hence $K(\alpha)$ splits D at 2, and ∞.

We are left with the case where $\operatorname{ind}_2 D=\operatorname{ind}_\infty D=2$ and 2 does not split in $K(\gamma')/K$, where $K(\gamma')$ is real. Then we consider 2 cases:

(a) 2 does not split in $K(\sqrt{-2\gamma'})/K$. In this case set $\sqrt{-2}\gamma'=\alpha$.

(b) 2 splits in $K(\sqrt{-2}\gamma')/K$. Therefore 2 splits in $K(\sqrt{2})K$. Since K is real then K contains a quadratic subfield $Q(\sqrt{d})$ where d is an even square-free integer. Suppose $Q(\varepsilon_r)$ is the smallest root of unity field containing K, with $|r|_2=2^t$; $t>2$. In this case choose $\sqrt{-1}(\varepsilon_{2^{t+1}}+\varepsilon_{2^{t+1}}^{-1})\gamma'=\alpha$. By [14, Prop. 7.5, p. 103] $K(\alpha)$ is not real and 2 ramifies in $K(\alpha)/K$. Thus $K(\alpha)$ splits D at 2 and ∞.

Since $m=p^b$ then $\operatorname{ind}_{q(i)} D=p^b$ for some i. Thus $|L_i:K|=p^b$ for some i which implies $|K(\alpha):K|=p^b$. By construction $L=K(\alpha)$ splits D at each $q(i)$ for $i=0,1,\ldots,s$, L/K is cyclic, and L/Q is abelian. It follows that L is the required maximal subfield of D. Q.E.D.

Now that we have necessary and sufficient conditions for the existence of a maximal subfield L of D to be abelian over Q and cyclic over K we ask: Once we have L, is it possible to find a suitable factor set α such that $D\sim(L/K,\alpha)$ in $S(K)$? The answer is yes in general, see [10]. If, however, we require the more demanding restriction that α be a root of unity in K then the answer is negative in general. Although Yamada [14, p. 33] has shown that every element A with $[A]\in S(K)$ is equivalent to a cyclotomic algebra it is not necessarily the case that the division algebra underlying A is also cyclotomic. This is in fact what we are requiring by our more demanding restriction on α. In Mollin [9] we have provided necessary and sufficient conditions for a division algebra to be cyclotomic.

It is natural to ask whether Theorem 3.1 holds for a larger class of elements

https://doi.org/10.4153/CMB-1982-031-3 Published online by Cambridge University Press

than those in $S(K)$. M. Schacher [11, Th. 1, p. 630] provides a counter-example of exponent p, one for every prime p. However, there is an error in his proof. The following is a counter-example to [11, Th. 1, p. 630].

Let q be an odd prime such that 2 is a primitive root modulo q, and let p be an odd prime such that $q \equiv 1 \pmod{p^2}$. Let K be the unique subfield of $Q(\varepsilon_q)$ which has degree p over Q. We define $[D] \in U(K)$ as follows:

$$\operatorname{ind}_2 D = 1/p \quad \text{and} \quad \operatorname{ind}_q D = 1/p \quad \text{and} \quad \operatorname{ind}_r D = 1 \quad \text{for all} \quad r \neq 2, q.$$

Since $q \equiv 1 \pmod{p^2}$ then K is contained in a subfield L of $Q(\varepsilon_q)$ such that $|L:K| = p$. Since 2 is a primitive root modulo q then $|L_2:K_2| = p$ and clearly $|L_q:K_q| = p$. Thus L is a maximal subfield of D, cyclic over K and abelian over Q, contradicting [11, Th. 1, p. 630].

The error in Schacher's proof arises essentially from one of his references, viz. Serre's [12, Prop. 5, p. 92] in which there is a misprint. Serre's result should read "... $N_0(\xi) = \xi^l$ ..." which translates in Schacher's notation to: $N_0(\xi) = \xi^p$. We see therefore, that if $q \not\equiv 1 \pmod{p^2}$ then his proof fails. We note however that if $q \not\equiv 1 \pmod{p^2}$ then, with the correct interpretation of [12, Prop. 5, p. 92] his proof would hold. Dr. Serre has informed me in a recent letter that the aforementioned misprint has been corrected in the English edition.

References

1. E. Artin and J. Tate, *Class Field Theory* Benjamin, New York, (1968)
2. B. Fein, *Minimal Splitting Fields for Group Representations II*, Pacific J. Math, **77** (2), (1978), 445–449.
3. J. Janusz, *The Schur Group of an Algebraic Number Field*, Annals of Math., **103,** (1976), 253–281.
4. R. Mollin, *Uniform Distribution and the Schur Subgroup*, J. Algebra **42,** (1976), 261–277.
5. R. Mollin, *Algebras with Uniformly Distributed Invariants*, J. Algebra, **44,** (1977), 271–282.
6. R. Mollin, *U(K) for a Quadratic Field K*, Communications in Algebra, **4**(8), (1976), 747–759.
7. R. Mollin, *Uniform Distribution Classified*, Math. Zeitschrift, **165,** (1979), 199–21.
8. R. Mollin, *Splitting Fields and Group Characters J. reine angew Math.* **315,** (1980), 107–114.
9. R. Mollin, *Cyclotomic Division Algebras*. To appear in Canadian J. Math.
10. I. Reiner, *Maximal Orders*, Academic Press, N.Y. (1975).
11. M. Schacher, *Cyclotomic Splitting Fields*, Proc. Amer. Math. Soc., **25,** (1970), 630–633.
12. J. P. Serre, Corps Locaux, Actualités Sci. Indust., No. 1296, Hermann, Paris, 1962.
13. E. Weiss, *Algebraic Number Theory*, McGraw-Hill, New York, (1963).
14. T. Yamada, *The Schur Subgroup of the Brauer Group*, Lecture Notes in Math., No. 397, Springer-Verlag, (1974).

Department of Mathematics and Statistics
Queen's University
Kingston, Ontario
K7L 3N6.

https://doi.org/10.4153/CMB-1982-031-3 Published online by Cambridge University Press