PACIFIC JOURNAL OF MATHEMATICS
Vol. 56, No. 2, 1975

GENERATORS FOR THE SCHUR GROUP OF LOCAL AND GLOBAL NUMBER FIELDS

GERALD J. JANUSZ

The main result of this paper gives a set of generators for the Schur group, $S(K)$, for any subfield K of a cyclotomic extension of the rational field. This result is obtained from two reduction theorems which apply to more general fields. In particular we use them to derive in a rather simple way the results of T. Yamada which determine $S(k)$ when k is a p-adic number field.

Some new results are given in the case K is a subfield of $Q(\epsilon_m)$ and $Q(\epsilon_m)$ is unramified over K. An example is given to show how the Riemann hypothesis may enter into the computation of $S(K)$ when $Q(\epsilon_m)$ is ramified over K.

Introduction. For a field K, the Schur group $S(K)$ is the subgroup of the Brauer group of K consisting of those equivalence classes which contain a cyclotomic algebra; that is a crossed product of the form $(K(\epsilon_m)/K, \alpha)$ where ϵ_m is a primitive mth root of unity and α is a factor set whose values are roots of unity.

The Schur group is of particular interest in case K is a subfield of a cyclotomic extension of the rational number field Q. In this case $S(K)$ coincides with the set of elements in the Brauer group of K which contain a K-central simple algebra which is isomorphic to a direct summand of a rational group algebra $Q[G]$ for some finite group G.

The main result in this paper is Theorem 3. It gives a set of generators for $S(K)$ which have a particularly simple form. For certain choices of K, this result makes the computation of $S(K)$ an exercise. Although we do not do this here, it is possible to recover a number of results already in the literature which compute $S(K)$ for various K. The generator theorem is obtained as an application of two theorems (numbered 1 and 2) of a more general nature. Another application of the first of these is the calculation of $S(K)$ when k is a p-adic number field. In this case $S(k)$ has already been determined by Yamada but the proofs given here seem more elementary and the results are stated in a slightly different form.

We also give some results about $S(K)$ when K is a subfield of some $Q(\epsilon_m)$ and $Q(\epsilon_m)$ is unramified over K. We close with an example to indicate how the extended Riemann hypothesis may enter into the computation of $S(K)$ in case the least cyclotomic field $Q(\epsilon_m)$ containing K is ramified over K. (See note added to the end of the paper.)

1. Two reduction theorems. For a field K and a positive integer n, let $W(K,n)$ denote the group of roots of unity in K whose multiplicative order divides some power of n. In particular if p is a prime, $W(K,p)$ denotes the roots of unity of p-power order in K.

If L is an extension field of K with Galois group $G = G(L/K)$ and if α is a factor set from $G \times G$ to L, we shall write $\alpha \in W(L,n)$ to mean $\alpha(\sigma,\tau) \in W(L,n)$ for all $\sigma, \tau \in G$. The crossed product made with L and α is denoted by $(L/K,\alpha)$. This is the central simple K algebra having L basis u_σ, $\sigma \in G$, subject to the rules

$$u_\sigma u_\tau = \alpha(\sigma,\tau)u_\sigma u_\tau, \; u_\sigma x = \sigma(x)u_\sigma \quad \text{for} \quad x \in L.$$

In case $G = \langle\sigma\rangle$ is cyclic then we write (L,σ,a) for the crossed product in which

$$\begin{aligned}(u_\sigma)^i &= u_{\sigma^i} && 1 \leqq i < |\sigma| \\ &= a && i = |\sigma|.\end{aligned}$$

THEOREM 1. *Let K be a field of characteristic zero, L an extension field and $G(L/K) = G$ an abelian group. Let n be a fixed integer and suppose $W(L,n)$ is finite. Let F be a fixed integer and suppose $W(L,n)$ is finite. Let F be a subfield of L containing K such that*

(i) *$G(L/F) = \langle\theta\rangle$ is cyclic,*
(ii) *the norm map $N_{L/F}$ from L to F carries $W(L,n)$ onto $W(F,n)$.*

Let $(L/K,\alpha)$ be a crossed product such that $\alpha \in W(L,n)$. Then there is a crossed product $(F/K,\beta)$ with $\beta \in W(F,n)$ such that $(L/K,\alpha)$ and $(F/K,\beta)$ lie in the same class of the Brauer group of K.

Proof. The outline of the proof is this. We produce an idempotent element e in $A = (L/K,\alpha)$ and show $eAe \cong (F/L,\beta)$ for suitable β. The conclusion follows because A and eAe belong to the same class whenever e is a nonzero idempotent in A.

Let $(L:F) = m$ so that $\theta^m = 1$. Then the element u_θ in $(L/K,\alpha) = A$ satisfies

$$(u_\theta)^m = \zeta \in W(L,n).$$

However since u_θ centralizes $(u_\theta)^m$, ζ must be fixed by θ so $\zeta \in F$. Thus $\zeta \in W(F,n)$ and so by (ii) there is an element $\gamma \in W(L,n)$ with $N_{L/F}(\gamma) = \zeta$. Then

$$(\gamma^{-1}u_\theta)^m = N_{L/F}(\gamma)^{-1}\zeta = 1.$$

We now replace u_{θ^i} with $(\gamma^{-1}u_\theta)^i$ for $1 \leqq i < |\theta|$. This changes the values of the factor set but all values still lie in $W(L, n)$. Hence we may assume at the start that

$$(u_\theta)^m = 1. \tag{1}$$

Now we set $e = 1/m \ \Sigma_{i=0}^{m-1} u_\theta^i$.

We easily obtain the equations

$$u_\theta e = e \tag{2}$$

$$e^2 = e. \tag{3}$$

Next we shall change some of the remaining u_σ to make them centralize e.

For each $\sigma \in G$, let

$$u_\sigma u_\theta u_\sigma^{-1} = \zeta_{\sigma\theta} u_\theta. \tag{4}$$

If $\zeta_{\sigma\theta} = 1$ set $v_\sigma = u_\sigma$. In particular $v_\theta = u_\theta$.

If $\zeta_{\sigma\theta} \neq 1$ proceed as follows. Raise both sides of (4) to the power m and use (1) to get

$$1 = (\zeta_{\sigma\theta} u_\theta)^m = N_{L/F}(\zeta_{\sigma\theta}).$$

We now prove there is an element $\gamma \in W(L, n)$ such that $\gamma\theta(\gamma^{-1}) = \zeta_{\sigma\theta}$. .

To do this we view $W(L, n)$ as a $\langle\theta\rangle$ module. Let $N = N_{L/F}$ and $\Delta = 1 - \theta$ viewed as endomorphisms of $W(L, n)$. Since $W(L, n)$ is finite, Herband's theory [4, p. 142] implies $\ker \Delta/\operatorname{Im} N$ and $\ker N/\operatorname{Im} \Delta$ have the same order. Our assumption (ii) implies $\ker \Delta = \operatorname{Im} N$ so also $\ker n = \operatorname{Im} \Delta$. Since $\zeta_{\sigma\theta}$ is in $\ker N$ it follows that $\Delta(\gamma) = \gamma\theta(\gamma^{-1}) = \zeta_{\sigma\theta}$ holds for some $\gamma \in W(L, n)$.

We now set $v_\sigma = \gamma^{-1}u_\sigma$ and observe that $v_\sigma v_\theta = v_\theta v_\sigma$ for each $\sigma \in G$ and $v_\sigma e = e v_\sigma$. The factor set has been changed now but

$$v_\sigma v_\tau = \alpha'(\sigma, \tau) v_{\sigma\tau}$$

implies $\alpha' \in W(L, n)$ still holds. But in fact $\alpha' \in W(F, n)$ because all the v_σ centralize v_θ.

It is a fairly easy matter now to identify eAe as a crossed product. For $x \in L$ and any σ in G we have

$$\begin{aligned} exv_\sigma e &= \frac{1}{m}\sum_i v_\theta^i x e v_\sigma \\ &= \frac{1}{m}\sum_i \theta^i(x) v_\theta^i e v_\sigma \\ &= \frac{1}{m} T_{L/F}(x) e v_\sigma \end{aligned}$$

where $T_{L/F}$ is the trace map from L to F.

It follows that $eLv_\sigma e = Fv_\sigma e$.

Next select a set of elements $\{\sigma_i\}$ such that $\langle\theta\rangle\sigma_i$ gives all the cosets of $\langle\theta\rangle$ in G. Then any σ has the form $\sigma = \theta^a\sigma_i$ and so

$$Fv_\sigma e = Fv_{\sigma_i} v_\theta^a e = Fv_{\sigma_i} e.$$

It now follows that

$$eAe = \sum_\sigma eLv_\sigma e = \sum_i Fv_{\sigma_i} e.$$

This last expression is a crossed product representation $(F/K, \alpha')$ where

$$v_{\sigma_i} e \cdot v_{\sigma_j} e = \alpha'(\sigma_i, \sigma_j) v_{\sigma_i\sigma_j} e$$

and the coset representatives σ_i are identified with the elements in $G/\langle\theta\rangle = G(F/K)$. Since $\alpha' \in W(F, n)$ we are done.

Next we investigate how certain crossed products made with complicated Galois extensions can be reduced to crossed products over simpler extensions.

Suppose K is a field of characteristic zero, $F_0, F_1, \cdots, F_t$ are extension fields of K which are linearly disjoint over K. Suppose also $G(F_i/K) = \langle\theta_i\rangle$ is cyclic for $i = 1, 2, \cdots, t$ and $G(F_0/K)$ is abelian. The linear disjointness means that the composite $E = F_0F_1 \cdots F_t$ has Galois group over K which can be identified with

$$G(F_0/K) \times \langle\theta_1\rangle \times \cdots \times \langle\theta_t\rangle = G.$$

THEOREM 2. *Let $(E/K, \alpha)$ be a crossed product with factor set $\alpha \in W(F_0, n)$ for some positive integer n. Then the class of $(E/K, \alpha)$ in the Brauer group of K can be expressed as a product of classes of algebras of the following types:*

(a) $(F_0F_i/K, \alpha_i)$ *with* $\alpha_i \in W(F_0, n)$ *and* $i \neq 0$,

(b) $(F_iF_j/K, \alpha_{ij})$ *with* $\alpha_{ij} \in W(K, n)$ *and* $i \neq 0$, $j \neq 0$.

Proof. The basic idea of the proof is to examine certain subalgebras B of $A = (E/K, \alpha)$ and use the relation $A \cong B \otimes C$ when B is K-central simple and C is the centralizer of B in A.

The first step reduces to the case where the values of the factor set are in the center.

Let $A_0 = (F_0/K, \operatorname{res} \alpha) = \Sigma F_0 u_\sigma$. where σ runs through $G(F_0/K)$. This is a subalgebra of A and A_0 is K-central simple. We want an explicit representation of its centralizer as a crossed product. The centralizer, $C_A(A_0)$, of A_0 in A contains $F_1 \cdots F_t$ but need not contain the elements u_{θ_i}. For each i let u_i denote u_{θ_i}. We have

$$u_i x u_1^{-1} = x \quad \text{for} \quad x \in F_0 \tag{5}$$

$$u_i u_\sigma u_i^{-1} = \zeta_{i,\sigma} u_\sigma \quad \text{for} \quad \sigma \in G(F_0/K). \tag{6}$$

In this last equation $\zeta_{i,\sigma}$ is a product of values of α so it lies in $W(F_0, n)$. In particular this implies $u_i A_0 u_i^{-1} = A_0$. Since every automorphism of A_0 fixing K is inner, we know there is an element in A_0 which produces the same automorphism by conjugation as conjugation by u_i. Our next task is to produce such an element.

We can apply Artin's lemma on the independence of characters to obtain an element x in F_0 such that

$$\lambda_i = \sum_{\sigma \in G(F_0/K)} \sigma(x) \zeta_{i,\sigma}^{-1}$$

is not zero. We claim

$$\tau(\lambda_i) = \zeta_{i,\tau} \lambda_i \tag{7}$$

for each τ in $G(F_0/K)$.

To prove this we begin by using (6) several times to obtain the equations

$$\zeta_{i,\tau\sigma} u_{\tau\sigma} = u_i u_{\tau\sigma} u_i^{-1}$$

$$\zeta_{i,\tau} \tau(\zeta_{i,\sigma}) u_\tau u_\sigma = u_i u_\tau u_\sigma u_i^{-1}.$$

Now all values of the factor set α lie in F_0 so are fixed by θ_i. It follows that

$$\zeta_{i,\tau} \tau(\zeta_{i,\sigma}) = \zeta_{i,\tau\sigma}.$$

If we apply τ to λ_i we get

$$\tau(\lambda_i) = \sum_{\sigma} \tau\sigma(x)\,\tau(\zeta_{i0})^{-1}$$

$$= \zeta_{i,\tau} \sum_{\sigma} \tau\sigma(x)\ \zeta_{i,\tau\sigma}^{-1}$$

$$= \zeta_{i,\tau}\lambda_i.$$

This equation implies

$$\lambda_i^{-1}u_\tau\lambda_i = \lambda_i^{-1}\tau(\lambda_i)u_\tau = \zeta_{i,\tau}u_\tau$$
$$= u_i u_\tau u_i^{-1}.$$

Now define v_i by the equation

$$v_i = \lambda_i u_i. \tag{8}$$

We see v_i centralizes F_0 and all the u_σ for σ in $G(F_0/K)$, so v_i centralizes A_0.

Let $H = \langle\theta_1\rangle \times \cdots \times \langle\theta_t\rangle$. For any

$$\theta = \theta_1^{a_1} \cdots \theta_t^{a_t}$$

let $v_\theta = v_1^{a_1} \cdots v_t^{a_t}$. We assert

$$C_A(A_0) = \sum_{\theta \in H} F_1 \cdots F_t v_\theta.$$

We already have seen the right side is contained in the left side. From the equation $A \cong A_0 \otimes C_A(A_0)$ we conclude $C_A(A_0)$ has dimension over K equal to $|H|^2$. This is the dimension of the right side so equality holds.

We have expressed $C_A(A_0)$ as a crossed product but the values of the factor set are much different than those of the original α. In particular the values need not be roots of unity. The rules for the multiplication of the v_θ can be deduced from the following equations:

$$v_i v_j = \epsilon_{ij} v_j v_i \qquad \epsilon_{ij} \in W(K, n), \tag{9}$$

$$v_i^{h_i} = \lambda_i^{h_i}\epsilon_i \qquad h_i = |\theta_i|,\ \epsilon_i \in W(F_0, n). \tag{10}$$

The proof that these hold is straightforward. We need only observe that λ_i is fixed by all θ_j so

$$v_i v_j = \lambda_i\lambda_j u_i u_j = \epsilon_{ij}\lambda_i\lambda_j u_j u_i = \epsilon_{ij} v_j v_i$$

and ϵ_{ij} is a product of values of the original factor set α. Thus $\epsilon_{ij} \in W(F_0, n)$. However ϵ_{ij} also lies in $F_1 \cdots F_t$ because $C_A(A_0)$ is an algebra so ϵ_{ij} is in $W(K, n)$.

Equation (10) follows in a similar way using

$$\epsilon_i = u_i^{h_i}.$$

Let β denote the factor set determined by (9) and (10).

The first step of the proof is done. Next it is necessary to decompose $C_A(A_0)$ as a tensor product of certain subalgebras.

Let $E_t = F_1 \cdots F_{t-1}$ and $H_t = \langle \theta_1, \cdots, \theta_{t-1} \rangle$ so that $H = H_t \times \langle \theta_t \rangle$.

We work entirely inside $C_A(A_0)$ which can be written as a crossed product

$$(E_t F_t / K, \beta) = C.$$

Consider the subalgebra

$$B_t = \sum_{\theta \in H_t} E_t v_\theta = (E_t / K, \operatorname{res} \beta).$$

This is a K-central simple subalgebra of C so as above we want to identify its centralizer, $C_C(B_t)$, in C. Clearly F_t centralizes B_t because the subgroup H_t fixes F_t. However v_t need not centralize all of B_t; v_t fixes E_t since θ_t fixes E_t. However v_t need not centralize the v_i for $1 \leqq i \leqq t-1$, as we can see from equation (9).

We shall find an element in B_t that carries out the same automorphism on B_t as v_t does.

Let x_i be an element of F_i which gives a normal basis of F_i over K. Then the element

$$\Omega_{ti} = \sum_j (\epsilon_{ti})^{-j} \theta_i^j (x_i)$$

is a nonzero element in F_i. Moreover

$$\theta_i(\Omega_{ti}) = \epsilon_{ti} \Omega_{ti}, \tag{11}$$

$$\theta_j(\Omega_{ti}) = \Omega_{ti}, \qquad j \neq i. \tag{12}$$

For later use note for $h_t = |\theta_t|$, equation (9) implies ϵ_{ti} has order dividing h_t. This means $(\Omega_{ti})^{h_t}$ is left fixed by θ_i as well as all θ_j for $j \neq i$. This yields

$$(13)\qquad (\Omega_{ti})^{h_t} \in K.$$

Now we set $\Omega_t = \Omega_{t1}\Omega_{t2}\cdots\Omega_{t,t-1}$. Then Ω_t is an element in $E_t = F_1\cdots F_{t-1}$ and satisfies

$$(14)\qquad \theta_i(\Omega_t) = \epsilon_{ti}\Omega_t \qquad 1 \leqq i \leqq t-1.$$

This equation follows from (11) and (12). Now we observe $\Omega_t v_t$ centralizes each v_i because of (9) and (11), and centralizes E_t also. Thus $\Omega_t v_t$ centralizes B_t. Again by dimension counting we obtain

$$C_C(B_t) = \sum_i F_t(\Omega_t v_t)^i.$$

Since $(\Omega_t v_t)^{h_t} = \Omega_t^{h_t}\lambda_t^{h_t}\epsilon_t = b_t$ by (10) we obtain a presentation of $C_C(B_t)$ as the cyclic algebra (F_t, θ_t, b_t). So we have to this point

$$A \cong (F_0/K, \text{res }\alpha)\otimes(F_t, \theta_t, b_t)\otimes(F_1\cdots F_{t-1}/K, \beta).$$

The proceedure used to split off B_t from C can be applied again to B_t in place of C. The result can be stated as follows.

Let x_i give a normal basis of F_i over K and let

$$(15)\qquad \Omega_{ri} = \sum_j (\epsilon_{ri})^{-j}\theta_i^j(x_i), \quad \text{and}$$

$$(16)\qquad \begin{aligned} &\Omega_r = \Omega_{r1}\cdots\Omega_{r,r-1} \quad \text{if} \quad r \geqq 2 \\ &\Omega_1 = 1. \end{aligned}$$

We have inclusions analogous to (13) of the form

$$(17)\qquad (\Omega_{ri})^{h_r} \in K, \qquad 1 \leqq i < r \leqq t.$$

The original algebra $A = (E/K, \alpha)$ is now expressed as a product of $A_0 = (F_0/K, \text{res }\alpha)$ and the cyclic algebras

$$A_r = (F_r, \theta_r, (\Omega_r\lambda_r)^{h_r}\epsilon_r)$$

for $1 \leqq r \leqq t$.

This is the end of the second step of the proof. Next (and lastly) we show each of these algebras is similar to a product of algebras of type (a) and (b) in the theorem.

The algebra A_0 is easy to deal with because we have $\alpha \in W(F_0, n)$. We can inflate α to any convenient composite F_0F_i so A_0 is similar to an algebra of type (a).

Now we consider A_r for $1 \leqq r \leqq t$. The relation $(F_r, \theta_r, ab) \sim (F_r, \theta_r, a) \otimes (F_r, \theta_r, b)$ can be applied to A_r by using (16) and (17) to get A_r is similar to the product of the algebras

$$P_r = (F_r, \theta_r, \lambda_r^{h_r} \epsilon_r) \quad \text{and} \quad Q_{rj} = (F_r, \theta_r, \Omega_{rj}^{h_r}), \qquad 1 \leqq j \leqq r - 1.$$

These cyclic algebras are well defined because of (17). In the case $r = 1$, A_r is already equal to P_r.

Now we show how to transform each of these algebras into similar algebras of types (a) or (b). The algebra P_r is similar to

$$P_r \otimes (F_0/K, 1) = \Big(\sum_j F_r v_r^j\Big) \otimes \Big(\sum_\sigma F_0 w_\sigma\Big)$$

where the "1" represents the trivial factor set so that $w_\sigma w_\tau = w_{\sigma\tau}$ for σ, $\tau \in G(F_0/K)$. Note that λ_r is in F_0 so we may replace the element $v_r \otimes 1$ with $v_r \otimes \lambda_r^{-1} = w_r$. Identify $1 \otimes w_\sigma$ with w_σ so we now have the following multiplication rules:

$$w_r^{h_r} = \epsilon_r,$$

$$w_r w_\sigma = 1 \otimes \lambda_r \sigma(\lambda_r)^{-1} w_\sigma w_r = 1 \otimes \zeta_{r\sigma}^{-1} w_\sigma w_r.$$

We use (7) to obtain the last equality. Finally identify $F_r \otimes F_0$ with the composite F_rF_0 and observe ϵ_r, $\zeta_{r\sigma}$ lie in $W(F_0, n)$ by the condition on α and (6) and (10). This finally gets P_r is similar to $(F_0F_r/K, \alpha_{or})$ where $\alpha_{or} \in W(F_0, n)$ which is of type (a).

The algebra Q_{rj} is treated in a similar way. We have Q_{rj} is similar to

$$Q_{rj} \otimes (F_j, \theta_j, 1) = \Big(\sum_i F_r v_r^i\Big) \otimes \Big(\sum_i F_j w_j^i\Big).$$

Identify $F_r \otimes F_j$ with the composite F_rF_j, use the fact that $\Omega_{rj} \in F_j$ and set $w_r = v_r \otimes \Omega_{rj}^{-1}$. Then we have

$$w_r^{h_r} = 1, \qquad w_j^{h_j} = 1$$

$$w_r w_j = \Omega_{rj}^{-1}\, \theta_j(\Omega_{rj})\, w_j w_r = \epsilon_{rj} w_j w_r.$$

Here the ϵ_{rj} comes from (15) and (9) and $\epsilon_{rj} \in W(K, n)$. It follows that Q_{rj} is similar to $(F_rF_j/K, \alpha_{rj})$ with $\alpha_{rj} \in W(K, n)$ which is an algebra of type (b).

When all the pieces are put together we reach a representation of A as a product of algebras of type (a) and (b) up to similarity.

2. The generators for $S(K)$. In this section K denotes an algebraic number field which is a subfield of some cyclotomic extension of Q, the rationals. We select an integer m such that $K \subseteq Q(\epsilon_m)$ and keep m fixed throughout this section.

PROPOSITION 2.1. (Yamada, [11]). *Let p be a prime integer. Each class in $S(K)_p$ contains a crossed product $(Q(\epsilon_n)/K, \alpha)$ with $\alpha \in W(Q(\epsilon_n), p)$ and $n = mp_1 \cdots p_t$ where $p_1, \cdots, p_t$ are distinct odd primes not dividing m in the cases $p \neq 2$ or $p = 2$ and 4 divides m; in the case $p = 2$ and m odd, $n = 4mp_1 \cdots p_t$ with the p_i distinct odd primes not dividing m.*

Proof. Let the class $[A]$ in $S(K)_p$ contain a crossed product $(K(\epsilon_s)/K, \beta)$ with $\beta \in W(K(\epsilon_s), p)$. By inflating the factor set we find $[A]$ also contains a crossed product $(Q(\epsilon_N)/K, \inf \beta)$ where m divides N. Let $p_1, \cdots, p_t$ be the odd primes which divide N but not m. Define n as in the theorem so we have the inclusions

$$K \subseteq F = Q(\epsilon_n) \subseteq L = Q(\epsilon_N).$$

Now every prime divisor of N also divides n so $G(L/F)$ is cyclic. (This is most easily seen by considering $G(L/Q)$ and $G(F/Q)$.) It is an easy exercise to verify $N_{L/F}$ carries $W(L,p)$ onto $W(F,p)$. The proof which is well-known in case $L = Q(\epsilon_{p^a})$, $F = Q(\epsilon_{p^b})$, $a > b \geqq 1$ and $b \geqq 2$ if $p = 2$, works equally well in our case here. Hence the hypothesis of Theorem 1 is satisfied and its conclusion completes the proof of this proposition.

This brings us to the main theorem.

THEOREM 3. *Let $K \subseteq Q(\epsilon_m)$ and p a prime integer. For odd p, or $p = 2$ and 4 divides m, $S(K)_p$ is generated by classes which contain algebras of the following types:*

(a) $(Q(\epsilon_{mq})/K, \alpha)$, $\alpha \in W(Q(\epsilon_m), p)$, *$q$ is a prime not dividing m;*

(b) $(K(\epsilon_{qr})/K, \beta)$, $\beta \in W(K, p)$, *q, r are distinct primes not dividing m.*

In case $p = 2$, and m odd $S(K)_2$ is generated by classes which contain algebras of type (b) *and of type*

(a′) $$(Q(\epsilon_{4mq})/K, \alpha),\ \alpha \in W(Q(\epsilon_4), 2),$$

q an odd prime not dividing m.

Proof. Any class in $S(K)_p$ contains a crossed product as described in Proposition 2.1. Keep all the notation from there. Set $F_i = K(\epsilon_{p_i})$ for $1 \leqq i \leqq t$ and set $F_0 = Q(\epsilon_m)$ if p is odd or if $p = 2$ and 4 divides m. In the remaining case set $F_0 = Q(\epsilon_{4m})$. Now the fields F_0, $F_1, \cdots, F_t$ are linearly disjoint over K and the algebra $A = (Q(\epsilon_n)/K, \alpha)$ has factor set with values which are p-power roots of 1. We may ignore the case where A is split. Then A has p-power index $\neq 1$. By the theorem of Benard-Schacher **[2]** (see also Janusz **[5]**) **[5]**) ϵ_p is in K. Thus p divides m, or $4m$ when $p = 2$ and m odd. This means $\alpha \in W(F_0, p)$. So Theorem 2 can be applied. The algebras $(F_iF_j/K, \alpha_{ij})$ are of type (a) or (a′) when $i = 0$ or $j = 0$ and of type (b) if $i \neq 0$ and $j \neq 0$. Since $Q(\epsilon_n) = F_0F_1 \cdots F_t$, we see A is in the group generated by classes containing algebras of type (a) and (b) or (a′) and (b), and the theorem holds.

The reader should find no difficulty applying this theorem to determine $S(K)$ when K is one of the fields Q, $Q(\epsilon_{p^a})$, or $Q(\epsilon_m)$. Of course the determination of the index of the generating algebras requires the local results in the next section.

3. The local case. The effect of Theorem 3 is to give us generators for $S(K)_p$ but unfortunately these are not independent generators. The relations between the generators can be found in some special cases by the use of local invariants.

Crucial to this procedure is the identification of the Schur group of a local field. This has been done by Yamada in a series of papers **[8]**, **[9]**, **[10]**. He has given several proofs of the local results but in all cases he has used some fairly deep results usually derived in the study of local class field theory. We shall give still another proof which we believe is more elementary. This is especially true in the case of a 2-adic local field.

To fix the notation let q be a prime integer, Q_q the complete q-adic rationals, and k a subfield of $Q_q(\epsilon_m)$ for some positive integer m.

We begin with a lemma that helps compute the index of cyclic algebras over k.

LEMMA 3.1. *Let E be a Galois extension of k with ramification index $e = e(E/k)$. Let ζ be a root of unity in k having order relatively prime to q. Then $\zeta = N_{E/k}(x)$ for some x in E if and only if ζ is the e'th power of a root of unity in k.*

Proof. Suppose F is the maximal unramified extension of k in E. Then $(E: F) = e$. Now assume $\zeta = \gamma^e$ for some root of unity γ in k. Since ζ has order prime to q it may be assumed that γ also has order prime to q. It is well known that $N_{F/k}$ maps the roots of unity in F of order prime to q onto the roots of unity in k of order prime to q. Hence there is an x in F with $N_{F/k}(x) = \gamma$. It follows $N_{E/k}(x) = \gamma^e = \zeta$ as required.

Conversely suppose $\zeta = N_{E/k}(x)$ for some x in E. Let π be a prime element of E and let bars denote residual classes mod π. Then $\bar{E} = \bar{F}$ so there exists an element y in F such that $\bar{x} = \bar{y}$. In fact y may be taken as a root of unity with order prime to q since all nonzero elements in $\bar{F}$ are roots of unity. Now we have

$$\zeta = N_{E/k}(x) \equiv N_{E/k}(y) = N_{F/k}(y)^e$$

with the congruence taken mod (π). This means $\zeta N_{F/k}(y)^{-e}$ is a root of unity in k of order prime to q whose image in $\bar{k}$ is $\bar{1}$. The only such root of unity is 1 so we have $\zeta = \gamma^e$ with $\gamma = N_{F/k}(y)$, a root of unity in k. This completes the proof.

THEOREM 4. (Yamada [8]). *Suppose q is an odd prime. Then $S(k)$ is a cyclic group of order $(q-1)/e_0$ where e_0 is the largest factor of $e(k/Q_q)$ which is prime to q. A generator for $S(k)$ is the class containing a cyclic algebra $(k(\epsilon_{q^a}), \sigma, \zeta)$ where a is any integer ≥ 1, $\langle\sigma\rangle = G(k(\epsilon_{q^a})/k)$ and ζ is a generator of the group of roots of unity in k whose order is prime to q.*

During the proof of Theorem 4 we shall also obtain a proof of the following.

PROPOSITION 3.2. (Witt [7]). *Suppose $q = 2$ and ϵ_4 is in k. Then $S(k)$ has order one.*

Proof. We shall prove the theorem by determining the p-primary parts, $S(k)_p$, for each prime p.

Suppose first $p \neq q$. Any class in $S(k)_p$ can be represented by a crossed product

$$A = (L/k, \alpha), \qquad \alpha \in W(L,p)$$
$$L = Q_q(\epsilon_{q^a}, \epsilon_m), \qquad (q, m) = 1.$$

Now let $F = k(\epsilon_{q^a})$. Then $L = F(\epsilon_m)$ is unramified over F so $G(K/F)$ is cyclic and $N_{L/F}$ carries $W(L,p)$ onto $W(F,p)$. By Theorem 1, A is similar a crossed product $(F/k, \beta)$ with $\beta \in W(F,p)$. Since $G(F/k)$ is isomorphic to a subgroup of $G(Q_q(\epsilon_{q^a})/Q_q)$, it follows $G(F/k)$ is cyclic. This is also true if $q = 2$ when ϵ_4 is in k. Thus $(F/k, \beta)$ can be written as $(k(\epsilon_{q^a}), \sigma, \epsilon)$ with ϵ in $W(k,p)$. In particular this algebra is similar to a power of $B = (k(\epsilon_{q^a}), \sigma, \zeta)$ where ζ generates the group $W(k,p)$. This algebra has index p^b if p^b is the least power of ζ which is a norm from $k(\epsilon_{q^a})$. By Lemma 3.1 p^b is the p-factor dividing $e(k(\epsilon_q a)/k)$. Since the p-factor of $e(k(\epsilon_{q^a})/Q_q)$ equals the p-factor of $(q-1)/e_0$ as given in the theorem. Notice that for $q = 2$ and ϵ_4 in k, $S(k)_p = 1$ when $p \neq 2$.

The computation of the index of B did not depend upon a so long as $a \geqq 1$. By combining this calculation for all primes $p \neq q$ we have proved the theorem except for the last step which is to show $S(k)_q$ has order one.

Now let

$$A = (L/k, \alpha),\ \alpha \in W(L,q)$$

$$L = Q_q(\epsilon_{q^a}, \epsilon_m),\quad (q,m) = 1.$$

Suppose A has index $q^c \neq 1$. Then by the root of unity theorem **[2]**, **[5]** we find ϵ_q is in k. In the case $q = 2$ we are assuming ϵ_4 is in k.

Now let $F = k(\epsilon_m)$ so $L = F(\epsilon_{q^a})$.

We again have $G(L/F)$ cyclic, and $N_{L/F}$ carries $W(L,q)$ onto $W(F,q)$ because ϵ_q is in F (or ϵ_4 is in F). It follows from Theorem 1 that A is similar to a crossed product $(F/k, \beta)$ with β in $W(F,q)$. But F/k is unramified so this algebra is split and $S(k)_q$ is trivial. This proves both the theorem and the proposition.

We now have left the case of $S(k)$ for $q = 2$ and ϵ_4 not in k. In this case we see any element in $S(k)$ is split by $k(\epsilon_4)$ because $S(k(\epsilon_4))$ has order one. Since $(k(\epsilon_4){:}\ k) = 2$ it follows that each element of $S(k)$ has order at most 2. Subgroups of the Brauer group of k which have an exponent are cyclic so we now know $S(k)$ has order 1 or 2. Before we state the criterion which determines when $S(k)$ has order two, we need some notation.

Let h be the least positive integer which satisfies the conditions

(i) $h \geqq 2$
(ii) $k \subseteq Q_2(\epsilon_{2^h}, \epsilon_c)$, c some odd integer.

LEMMA 3.3. *If $k \subseteq L = Q_2(\epsilon_{2^h}, \epsilon_c)$ with h as above, then $k(\epsilon_{4c}) = L$.*

Proof. Let $G(L/Q_2) = \langle \sigma_{-1}, \sigma_5 \rangle \times \langle \phi \rangle$ where ϕ fixes $\epsilon_2 h$, σ_x fixes ϵ_c, and $\sigma_x(\epsilon_{2^h}) = \epsilon_{2^h}^x$ for $x = -1, 5$. If $G(L/k(\epsilon_4 c))$ is not of order 1 then it must contain $\tau = (\sigma_5)^{2^{h-1}}$ because this is the only element of order 2 fixing ϵ_{4c}. But then $k(\epsilon_4)$ belongs to the fixed field $Q_2(\epsilon_2 h - 1, \epsilon_c)$ of τ contrary to the choice of h.

Now we can state the theorem originally proved by Yamada **[9, 10]** in a slightly different form.

THEOREM 5. *Let k be a subfield of $Q_2(\epsilon_m)$ for some m. $S(k)$ has order 1 or 2 in all cases and has order 2 if and only if there is an odd integer n such that the following hold*:

(i) *$k(\epsilon_4)/k$ is ramified*;

(ii) $k(\epsilon_{4n}) = Q_2(\epsilon_{2^h}, \epsilon_n)$

(iii) $(k(\epsilon_n): k) = 2^r w$, *$w$ odd*, $r \geqq 1$;

(iv) *the automorphism of order 2 in $G(k(\epsilon_{4n})/k(\epsilon_n))$ carries ϵ_{2^h} to its inverse*;

(v) *if $r \leqq h-1$, then any root of unity in $k(\epsilon_{4n})$ whose order divides 2^{h-r+1} already lies in $k(\epsilon_4)$.*

Proof. First suppose $(k: Q_2)$ is odd. Then k/Q_2 is unramified so $k = Q_2(\epsilon_r)$ for some odd r. If we set $n = 5r$ then conditions (i)-(v) hold. The factor 5 is inserted to make certain (iii) holds. Moreover the oddness of $(k: Q_2)$ insures that

$$k \otimes (Q_2(\epsilon_4), \sigma, -1) \cong (k(\epsilon_4), \sigma, -1)$$

is an algebra in $S(k)$ of index 2.

From now on we assume $(k: Q_2)$ is even. We shall use several times in the proof that $(k(\epsilon_4), \sigma, -1)$ is split.

Suppose $S(k)$ has a class of order 2 containing

$$A' = (k(\zeta)/k, \alpha'),\ \zeta \text{ a root of unity.}$$

By inflating α' to a larger field and then applying Theorem 1 we may replace A' by an equivalent algebra

$$A = (L/k, \alpha) \quad \alpha \in W(L, 2)$$
$$L = Q_2(\epsilon_{2^h}, \epsilon_n),$$

where n is odd and h is the minimal integer described before Lemma 3.3.

We may apply Lemma 3.3 to conclude $L = k(\epsilon_{4n})$ so (ii) holds. If $k(\epsilon_4)/k$ were unramified, then L/k would be unramified and so A would be split. Thus $k(\epsilon_4)/k$ is ramified—in in fact totally ramified. So (i) holds. We cannot have $L = k(\epsilon_4)$ because $(k(\epsilon_4), \sigma, -1)$ is split. Thus $k(\epsilon_4)$ and $k(\epsilon_n)$ are nontrivial extensions of k and they are linearly disjoint over k because one is totally ramified and one is unramified. This allows us to describe the Galois group:

$G(L/k) = \langle\sigma\rangle \times \langle\tau\rangle$ where

$$\sigma(\epsilon_n) = \epsilon_n \quad \tau(\epsilon_4) = \epsilon_4$$

$$\sigma(\epsilon_4) = -\epsilon_4 \quad \tau = \text{Frobenius automorphism on } k(\epsilon_n)/k,$$

ρ has order $2, \tau$ has order t.

The factor set α for A is determined by the equations

(1) $u_\sigma^2 = \epsilon_\sigma$
(2) $u_\tau^t = \epsilon_\tau$
(3) $u_\sigma u_\tau = \epsilon_{\sigma\tau} u_\tau u_\sigma$

where ϵ_σ, ϵ_τ, $\epsilon_{\sigma\tau} \in W(L,2)$.

There are certain restrictions upon these values:

(4) $\epsilon_\sigma = \pm 1$,
(5) $\sigma(\epsilon_{\sigma\tau})\epsilon_{\sigma\tau} = 1$,
(6) $\sigma(\epsilon_\tau)\epsilon_\tau^{-1} = \epsilon_{\sigma\tau}^{tw}$ for some odd integer w determined below.

Equation (4) follows because $\epsilon_\sigma = u_\sigma^2$ centralizes u_σ; that is $\sigma(\epsilon_\sigma) = \epsilon_\sigma$. But the only 2-power roots of unity in $k(\epsilon_n)$, the fixed field of σ, are ± 1 because ϵ_4 is not in $k(\epsilon_n)$. To get equation (5) just use equations (3), (1) and (4) to get

$$\epsilon_\sigma u_\tau = \sigma(\epsilon_{\sigma\tau})\, u_\sigma u_\tau u_\sigma = \sigma(\epsilon_{\sigma\tau})\, \epsilon_{\sigma\tau} u_\tau \epsilon_\sigma$$

from which (5) follows.

In order to establish (6) we first make the following computation. Let $\tau(\epsilon) = \epsilon^v$ when $\epsilon = \epsilon_2 h$. Since $\tau(\epsilon_4) = \epsilon_4$ we obtain $v \equiv 1 \bmod 4$. Thus we have

$$\prod_{i=0}^{t-1} \tau^i(\epsilon) = \epsilon^{1+v+\cdots+v^{t-1}} = \epsilon^x$$

where $x = t$ if $v = 1$ and $x = (v^t - 1)/(v - 1)$ if $v \neq 1$. The condition $v \equiv 1 \bmod 4$ insures that the highest power of 2 in x is the highest power of 2 in t. Thus $\epsilon^x = \epsilon^{tw}$ for some odd w in either case. Now to get (6) we use (3) and (2) to obtain

$$(u_\sigma u_\tau u_\sigma^{-1})^t = \sigma(\epsilon_\tau) = (\epsilon_{\sigma\tau} u_\tau)^t$$
$$= \epsilon_\tau \Pi \tau^i(\epsilon_{\sigma\tau}) = \epsilon_\tau \epsilon_{\sigma\tau}^{tw}.$$

Now suppose $\epsilon_{\sigma\tau} = 1$. Then the subalgebra $(k(\epsilon_4), \sigma, \epsilon_\sigma)$ of A has $k(\epsilon_n)$ and u_τ in its centralizer. So by dimension count we obtain

$$A \cong (k(\epsilon_4), \sigma, \epsilon_\sigma) \otimes (k(\epsilon_n), \tau, \epsilon_\tau).$$

This algebra is split; the first factor is split because $(k: Q_2)$ is even; the second because $k(\epsilon_n)/k$ is unramified.

So now we assume $\epsilon_{\sigma\tau} \neq 1$. We must consider separate cases. Let $\zeta = \epsilon_{2^h}$. Then σ induces an automorphism of the cyclic group $\langle \zeta \rangle$ which inverts ϵ_4. There are only two possibilities:

Case (a) $\sigma(\zeta) = \zeta^{-1}$
Case (b) $\sigma(\zeta) = \zeta^{-1+2^{h-1}}$, $h \geqq 3$.

Assume case (b) holds. It is easily seen that only even powers of ζ are inverted by σ, so in view of (5) we have

$$\epsilon_{\sigma\tau} = \zeta^{2b}, \quad \text{some} \quad b.$$

If we let $c = b(1 + 2^{h-2})$ then

$$\zeta^{-1}\sigma(\zeta^c)\epsilon_{\sigma\tau} = 1.$$

Now let $v_\tau = \zeta^c u_\tau$. The last equation implies

$$u_\sigma v_\tau = \sigma(\zeta^c)\epsilon_{\sigma\tau}\zeta^{-c} v_\tau u_\sigma = v_\tau u_\sigma.$$

As in the case just above with $\epsilon_{\sigma\tau} = 1$ we again have

$$A = (k(\epsilon_4), \sigma, \epsilon_\sigma) \otimes (k(\epsilon_n), \tau, \epsilon)$$

where $\epsilon = v_\tau^t = (\zeta^c u_\tau)^t = \epsilon_\tau \, N_{L/k(\epsilon_4)}(\zeta^c)$. Since this is a root of unity we get A is split for the same reasons as above. Thus case (b) does not occur if A has index 2.

Now assume case (a) so σ inverts all 2-power roots of unity. Thus (iv) holds. Let $x = \epsilon_4(1 - \epsilon_{\sigma\tau})$. Since $\epsilon_{\sigma\tau} \neq 1$, we have $x \neq 0$. Also

$$\sigma(x) = -\epsilon_4(1 - \epsilon_{\sigma\tau}^{-1}) = \epsilon_4 \epsilon_{\sigma\tau}^{-1}(1 - \epsilon_{\sigma\tau}) = \epsilon_{\sigma\tau}^{-1} x.$$

Set $v_\tau = x u_\tau$. This last equation implies $u_\sigma v_\tau = v_\tau u_\sigma$. For the third time now

$$A \cong (k(\epsilon_4), \sigma, \epsilon_\sigma) \otimes (k(\epsilon_n), \tau, a)$$

where $a = v_\tau^t = \epsilon_\tau N_{L/k(\epsilon_4)}(x)$.

The first factor on the right is split because $(k: Q_2)$ is even. The second factor might not be split however. The previous reasoning does not apply because a is not a root of unity. Suppose $\pi = \pi_k$ is a prime element of k, and $a = \pi^q w$, w a unit in the valuation ring of k. Since every unit of the valuation ring is a norm from $k(\epsilon_n)$ we obtain the similarity

$$A \sim (k(\epsilon_n), \tau, \pi^q).$$

This algebra is split if and only if $t = (k(\epsilon_n) \colon k)$ divides q. So we must compute q.

Consider first $\epsilon_{\sigma\tau} = -1$ so $x = -2\epsilon_4$. Then $a = 2^t$ (except for units). If $2 = \pi^e$ then we conclude $et = q$ so t divides q and A is split.

Now assume $\epsilon_{\sigma\tau}$ has order $2^d \geqq 2^2$. First notice the following fact. If ϵ is a root of unity of order 2^r then the norm from $Q_2(\epsilon_2 r)$ to $Q_2(\epsilon_2 r - 1)$ carries $1 - \epsilon$ to $1 - \epsilon^2$ if $r \geqq 3$ and to 2 if $r = 2$. This provides us with the equation

$$N_{Q_2(\epsilon_2 d)/Q_2}(1 - \epsilon_{\sigma\tau}) = 2.$$

Now use the transitivity of the norm to get

$$N_{L/Q_2}(x) = N_{L/Q_2}(1 - \epsilon_{\sigma\tau}) = 2^{(L:Q_2(\epsilon_2 d))}.$$

Let π_4 be a prime element of $k(\epsilon_4)$ and set $N_{L/k(\epsilon_4)}(x) = \pi_4^s$. We should allow unit factors in this and other equations to follow, but the units will not affect the outcome of the computation of the index so we just drop them from the equations. Then we may write $\pi_4^2 = \pi_k$ and $a = \pi_4^s = \pi_k^q$ implies $2q = s$. Set

$$N_{k/Q_2}(\pi_k) = 2^f, \qquad f = f(k/Q_2).$$

We now obtain from these norm equations

$$2^{(L\cdot Q_2(\epsilon_2 d))} = N_{k/Q_2}N_{k(\epsilon_4)/k}(\pi_4^s) = 2^{sf}.$$

Then

$$\begin{aligned} sf &= (L \colon Q_2(\epsilon_2 d)) = (L \colon Q_2)/2^{d-1} \\ &= (L \colon k(\epsilon_4))2e(k/Q_2)f/2^{d-1}. \end{aligned}$$

Finally

$$s = \frac{2te(k/Q_2)}{2^{d-1}},$$

and

$$q = \frac{te(k/Q_2)}{2^{d-1}}.$$

From Lemma 3.3 we conclude $e(L/Q_2) = 2^{h-1}$ and so $e(k/Q_2) = 2^{h-2}$. This gives us the equation

$$q = t \cdot 2^{h-d-1}.$$

Whenever $d < h$, q is divisible by t and A is split. When $d = h$ then $2q = t$ and so the algebra has index 2 because t does not divide q. We have yet to show condition (iii) holds; it is necessary to show t is even. Since $\epsilon_{\sigma\tau}$ has order 2^h and equation (6) now reads

$$\epsilon_\tau^{-2} = \epsilon_{\sigma\tau}^{tw}, \tag{7}$$

we see the order of $\epsilon_{\sigma\tau}^{tw}$ is at most 2^{h-1} because it is a square. Since w is odd it follows t is even. Thus we have shown conditions (i)–(iv) of the theorem hold.

Finally we must verify (v). From equation (7) and the fact that $\epsilon_{\sigma\tau}$ has order 2^h we find ϵ_τ has order 2^{h-r+1} if $r \leqq h-1$. This follows because 2^r is the exact power of 2 dividing t. Moreover $\epsilon_\tau = u_\tau^t$ centralizes u_τ so ϵ_τ is fixed by τ. Hence roots of unity with order dividing 2^{h-r+1} lie in $k(\epsilon_4)$, the fixed field of τ. This shows the conditions (i)–(v) are necessary.

The computations also show how to prove the converse. We assume conditions (i)–(v) hold. It is necessary to define a factor set α for the extension $k(\epsilon_{4n})/k$ so that the algebra $(k(\epsilon_{4n})/k, \alpha)$ is given by the conditions (1)–(3). It is required that $\epsilon_{\sigma\tau}$ have order 2^h. We set $\epsilon_{\sigma\tau} = \epsilon_{2^h}$, $\epsilon_\sigma = 1$ and ϵ_τ a solution of equation (7). A solution is possible because t is even and such an ϵ_τ is fixed by τ. The odd integer w in (7) is 1 if $\tau(\epsilon_{2^h}) = \epsilon_{2^h}$ and w is the odd integer which satisfies

$$tw \equiv \frac{v^t - 1}{v - 1} \bmod 2^h$$

when $\tau(\epsilon_{2^h}) = \epsilon_{2^h}^v$, $v \neq 1$. Then the equations (1)–(3) do define a factor set and the algebra constructed has index 2. The proof is finally complete.

The five conditions in Theorem 5 can be described in terms of Galois groups. Let $L = Q_2(\epsilon_{2^h}, \epsilon_n)$ with $h \geqq 3$ and n odd. Then

$$G(L/Q_2) = \langle \sigma_{-1}, \sigma_5 \rangle \times \langle \phi \rangle$$

where ϕ fixes ϵ_{2^h}; σ_{-1}, σ_5 fix ϵ_n and σ_{-1} inverts e_{2^h} while $\sigma_5(\epsilon_{2^h}) = \epsilon_{2^h}^5$.

We want to describe which subfields k of L satisfy the conditions in Theorem 5. We give a sketch of the characterization.

The group $G(L/k(\epsilon_n))$ must have order 2 and its generator inverts ϵ_{2^h}. Thus $G(L/k(\epsilon_n)) = \langle\sigma\rangle = \langle\sigma_{-1}\rangle$.

The group $G(L/k(\epsilon_4)) = \langle\tau\rangle$ is a subgroup of $\langle\sigma_5, \phi\rangle$. The conditions (iii) and (v) force

$$\tau = \sigma_5^a \phi^b$$

where the order of ϕ^b is divisible by $2|\sigma_5^a|$.

Now suppose $L = Q_2(\epsilon_4, \epsilon_n)$ with n odd. Let $G(L/Q_2) = \langle\sigma_{-1}\rangle \times \langle\phi\rangle$ with the same definitions as above. The conditions of the theorem require $G(L/k) = \langle\sigma_{-1}\rangle \times \langle\phi^b\rangle$ where ϕ^b has even order.

Summary. The subfields k of $L = Q_2(\epsilon_{2^h}, \epsilon_n)$ which satisfy the conditions of the Theorem 5 are the fields fixed by the groups

(a) $\langle\sigma_{-1}\rangle \times \langle\sigma_5^a\phi^b\rangle$ if $h \geqq 3$ and $2|\sigma_5^a|$ divides $|\phi^b|$;

(b) $\langle\sigma_{-1}\rangle \times \langle\phi^b\rangle$ if $h = 2$ and 2 divides $|\phi^b|$.

4. Global fields.

We return to the study of $S(K)$ when K is a global field. We assume K is a subfield of $Q(\epsilon_m)$ for some positive integer m.

For a rational prime q (either a prime integer or the infinite prime) we denote by $S(K, q)$ the subgroup of $S(K)$ consisting of those classes which are split at every completion of K except possibly at the primes of K over q. As usual $S(K, q)_p$ denotes the p-primary subgroup of $S(K, q)$. It follows from Benard's theorem [1], that $S(K, q)_p$ is a cyclic group (perhaps trivial). When $p \neq 2$, $S(K, q)_p$ can be nontrivial only if q is a finite prime and p divides $q - 1$ by Theorem 4.

For certain K, it is known that $S(K)_p$ is the direct sum of its subgroups $S(K, q)_p$ while, for example, $S(Q)_2$ is not such a direct sum. In fact $S(Q, q)_2$ is trivial for all q while $S(Q)_2$ is infinite. In all the known cases where $S(K)_p$ fails to be the direct sum of the $S(K, q)_p$, it happens that $p = 2$. This suggests an obvious conjecture to which we lend some support.

THEOREM 6. *Let $K \subseteq Q(\epsilon_m)$ and let p be an odd prime integer. Assume K satisfies the following condition: Whenever ρ is a prime of K which ramifies in $Q(\epsilon_m)$, then the rational prime integer r in ρ is not congruent to* 1 mod *p.*

Then $S(K)_p$ is the direct sum of its subgroups $S(K, q)_p$ as q runs through primes $\equiv 1$ mod *p.*

Proof. To prove the theorem it is enough to show each member of a generating set for $S(K)_p$ is the product of elements from distinct subgroups $S(K,q)_p$. We use the generators as described in Theorem 3.

A generator $A_q = (Q(\epsilon_{mq})/K, \alpha)$ of type (a) is nonsplit only at those primes of K which ramify in $Q(\epsilon_{mq})$. Let ρ be such a prime and suppose first q is not in ρ. Let r be the rational.prime integer in ρ. Then $K_\rho \otimes A_q$ is an element in $S(K_\rho)_p$. The order of this group divides $r-1$ by Theorem 4. Our assumption is that p does not divide $r-1$ so $K_\rho \otimes A_q$ is split. Hence A_q is nonsplit only at the primes over q. (Since $p \neq 2$, A_q is split at all infinite primes.) Thus $[A_q]$ is in $S(K,q)_p$.

Now consider an algebra $B_{qr} = (K(\epsilon_{qr})/K, \beta)$ of type (b) in Theorem 3. The values of the factor set are p-power roots of unity in K. Suppose ϵ is the generator of $W(K,p)$. Then

$$G(K(\epsilon_{qr})/K) \cong G(Q(\epsilon, \epsilon_{qr})/Q(\epsilon))$$

so it follows that

$$B_{qr} \cong K \otimes (Q(\epsilon, \epsilon_{qr})/Q(\epsilon), \beta).$$

Thus $[B_{qr}]$ lies in the image of $S(Q(\epsilon))_p$ under the map from the Brauer group of $Q(\epsilon)$ to the Brauer group of K. The group $S(Q(\epsilon))_p$ is already known by the results of Benard-Schacher [2] (and can also be easily computed using Theorems 3 and 4). We find $S(Q(\epsilon))_p$ is the direct sum of its subgroups $S(Q(\epsilon),q)_p$. Thus $[B_{qr}]$ is the product of elements in distinct subgroups $S(K,q)_p$. The proof is complete.

Notice the hypothesis of Theorem 6 holds trivially when $K = Q(\epsilon_m)$. However for this case $S(K)_p$ is known [6].

A less trivial case where Theorem 6 applies is a case when $Q(\epsilon_m)$ is unramified over K. In this case Theorem 6 applies for all odd p. The following theorem is really just a restatement of facts already proved.

THEOREM 7. *Suppose $Q(\epsilon_m)$ is an unramified extension of K and p is an odd prime. Then $S(K)_p$ is the direct sum of its subgroups $S(K,q)_p$ where q runs through primes congruent to* 1 mod *p. Moreover $S(K,q)_p$ is cyclic and a generator can be taken as an algebra either of the form $(Q(\epsilon_{mq})/K, \alpha)$ for a suitable factor set $\alpha \in W(Q(\epsilon_m),p)$, or of the form $K \otimes B$ with $[B]$ in $S(Q(\epsilon),q)_p$ for $\langle\epsilon\rangle = W(K,p)$.*

We shall conclude this paper by illustrating the difficulty which prevents us from making progress in cases not covered by Theorem 6.

Let p and t be odd primes with $t \equiv 1 \bmod p^2$. The field $Q(\epsilon_{pt})$ has an automorphism σ of order p which fixes ϵ_p. Let K be the fixed field under $\langle\sigma\rangle$. Then the prime ρ of K which divides t is ramified in $Q(\epsilon_{pt})$ and of course p divides $t-1$.

If we are to compute $S(K)_p$ it will certainly be necessary to decide if there is an algebra class in $S(K)_p$ which is nonsplit at t. This is even weaker than asking if $S(K,t)_p$ has order 1 or not.

If there is a class in $S(K)_p$ nonsplit at t, then one of the generators of $S(K)_p$ is nonsplit at t. The generators listed in Theorem 3 part (b) are all split at t because the divisor ρ of t in K is unramified in $K(\epsilon_{qr})$. Hence we consider generators of type (a). Suppose

$$A = (Q(\epsilon_{ptq})/K, \alpha),\ \alpha \in W(Q(\epsilon_{pt}), p).$$

Suppose $G(Q(\epsilon_{ptq})/K) = \langle\sigma\rangle \times \langle\tau\rangle$ with σ fixing ϵ_{pq} and τ fixing ϵ_{pt}. The important value of the factor set is $\epsilon_{\sigma\tau}$ where

$$u_\sigma u_\tau = \epsilon_{\sigma\tau} u_\tau u_\sigma \quad \text{in} \quad A.$$

Let the Frobenius automorphism of ρ in $K(\epsilon_q)$ be τ^a. After some calculation, one finds the t-local index of A is the order of $\epsilon^a_{\sigma\tau}$. Since there are no p^2 roots of unity in K we see $\epsilon_{\sigma\tau}$ has order at most p and for suitable α we can arrange $\epsilon_{\sigma\tau}$ to have order p. This requires $q \equiv 1 \bmod p$. For such a q and suitable α we find A has t-local index p if p does not divide a, and A is split at t if p divides a.

So the problem rests upon the existence of a suitable q; namely we want a prime q such that $q \equiv 1 \bmod p$ and the Frobenius automorphism of ρ in $K(\epsilon_q)$ is not a pth power of any automorphism in $G(K(\epsilon_q)/K)$.

The assumptions made at the beginning insure $f(\rho/t) = 1$ so the assertion about the Frobenius automorphism of ρ is equivalent to the assertion that the automorphism $\phi_t(\epsilon_q) = \epsilon_p^t$ is not the pth power of any element in $G(Q(\epsilon_q)/Q)$.

The question of whether or not such a q exists for the given p and t is open. It is related to a famous conjecture of Artin, a special case of which says there exist infinitely many primes q such that ϕ_t generates all of $G(Q(\epsilon_q)/Q)$. Of course we require somewhat less of ϕ_t but we require $q \equiv 1 \bmod p$.

Artin's conjecture has been shown to hold by Hooley [3] under the assumption that the extended Riemann hypothesis holds. Without this assumption only very special cases of the conjecture are known to hold.

This suggests that explicit determination of $S(K)$ for general K may depend upon extremely deep properties and results about the distribution on primes which are not yet known.*

* *Note added in proof February,* 1975. This is an embarrassing overstatement of the difficulties of the problem. In fact the existence of the required primes can be proved without reference to Artin's conjecture. The determination of $S(K)_p$ can be made for p and odd prime and K any abelian extension of Q. The details will appear under the title "The Schur group of an algebraic number field".

REFERENCES

1. M. Benard, *The Schur subgroup, I*, J. Algebra, **22,** No. 2 (1972), 374–377.
2. M. Benard and M. Schacher, *The Schur subgroup, II*, J. Algebra, **22**, No. 2 (1972), 378–385.
3. C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math., (1967), 209–220.
4. G. J. Janusz, *Algebraic Number Fields*, Academic Press, New York, 1973.
5. ———, *The Schur index and roots of unity*, Proc. Amer. Math. Soc., **35**, No. 2. (1972), 387–388.
6. ———, *The Schur group of a cyclotomic field*, J. Number Theory, (to appear).
7. E. Witt, *Die algebraische Struktur des Gruppenringes*, J. Reine Angew. Math., **190** (1952), 231–245.
8. T. Yamada, *Characterization of the simple components of the group algebras over the p-adic number field*, J. Math. Soc. Japan, **23** (1971), 295–310.
9. ———, *The Schur subgroup of a 2-adic field*, J. Math. Soc. Japan, **26** (1974), 168–179.
10. ———, *The Schur subgroup of a p-adic field*, (preprint).
11. ———, *The Schur subgroup of the Brauer group, I*, J. Algebra, **27,** No. 3 (1973), 579–589.

Received April 9, 1974. This work was partially supported by NSF grant GP–38916.

UNIVERSITY OF ILLINOIS