J. Math. Soc. Japan
Vol. 26, No. 1, 1974

The Schur subgroup of a 2-adic field*

By Toshihiko YAMADA

(Received March 19, 1973)

§ 1. Introduction.

Let k be a field of characteristic 0. If A is a central simple algebra over k then $[A]$ will denote the class of A in the Brauer group $Br(k)$ of k. The *Schur subgroup* $S(k)$ *of* $Br(k)$ consists of those algebra classes $[A]$ of $Br(k)$ such that A is a simple component of the group algebra kG for some finite group G. Let p be a prime number. Denote by Q_p the rational p-adic field. When k is a finite extension of Q_p for an odd prime p, the Schur subgroup $S(k)$ has been completely determined in [3, Theorems 1 and 2].

In this paper we will determine the Schur subgroup $S(k)$ for any finite extension k of the rational 2-adic field Q_2. By a result of Witt [7] it has been known that the order of $S(k)$ is one or two. That is, either $S(k)=1$, or $S(k)$ consists of the two classes of $Br(k)$ whose Hasse invariants are 0 and 1/2 (mod 1). For a positive integer n, ζ_n will denote a primitive n-th root of unity. Let k be a cyclotomic extension of Q_2. Let h be the smallest non-negative integer such that k is contained in $Q_2(\zeta_{2^h m})$ for some odd integer m. We will call h the *height* of k. Clearly, either $h=0$ or $h \geqq 2$. $h=0$ if and only if k/Q_2 is unramified. In this case $k=Q_2(\zeta_{2^f-1})$, f being the residue class degree of k/Q_2, and $k(\zeta_4)/k$ is ramified. Suppose next that $h \geqq 2$. Set $M=k(\zeta_{2^h})$ and let f be the residue class degree of M/Q_2. It will be shown that $M=Q_2(\zeta_{2^h}, \zeta_{2^f-1})$ and that M is the *minimal* cyclotomic field containing k. Furthermore, if E is the maximal unramified extension of k contained in M, then $M=E(\zeta_4)$. It turns out that if $k(\zeta_4)/k$ is *ramified*, then M/E is also ramified and $h \geqq 3$. In this case, let ω be the generator of the Galois group of M over E $(\omega^2=1)$. If

$$\zeta_{2^h}^{\omega}=\zeta_{2^h}^{z} \tag{1}$$

for some integer z, then $z \bmod 2^h$ is determined only by k. Here we state our main result.

THEOREM 1. *Let k be a cyclotomic extension of Q_2 and let h be the height of k.*

* This work was supported in part by The Sakkokai Foundation.

(I) *Suppose that* $k(\zeta_4)/k$ *is ramified. Then, only the following three cases happen:*

i) $h=0$.

ii) $h\geqq 3$ *and* $z\equiv -1 \pmod{2^h}$.

iii) $h\geqq 3$ *and* $z\equiv -1+2^{h-1} \pmod{2^h}$.

For the cases i) *and* ii), $S(k)$ *is the subgroup of order* 2 *of* $Br(k)$. *For the case* iii), $S(k)=1$.

(II) *If* $k(\zeta_4)/k$ *is unramified* (*including the case* $\zeta_4\in k$), *then* $S(k)=1$.

We will mention an example for each of the above cases: (I-i) $k=Q_2$. (I-ii) $k=Q_2(\sqrt{2})\subset Q_2(\zeta_8)$. (I-iii) $k=Q_2(\sqrt{-2})\subset Q_2(\zeta_8)$. (II) $k=Q_2(\sqrt{3})\subset Q_2(\zeta_{12})$, where $k(\zeta_4)=Q(\zeta_{12})$ and $k(\zeta_4)/k$ is unramified of degree 2.

The following two theorems are immediate consequences of Theorem 1.

THEOREM 2. *Keeping the notation of Theorem* 1, *the order of the Schur subgroup* $S(k)$ *is equal to the ramification index of the extension* $k(\zeta_4)/k$ *except the case* (I-iii), *for which* $S(k)=1$.

THEOREM 3. *Let* K *be a finite extension of* Q_2. *Let* k *be the maximal cyclotomic extension of* Q_2 *contained in* K. *Then we have:*

(1) *If* $[K:k]$ *is even, then* $S(K)=1$.

(2) *If* $[K:k]$ *is odd, then* $S(K)\cong S(k)$, *and* $S(k)$ *is determined by Theorem* 1.

Notation and Terminology. Let ζ be a root of unity. Then the field $Q_2(\zeta)$ is called a cyclotomic field (over Q_2). Let δ be an element of $Q_2(\zeta)$ and let K be a finite extension of Q_2. Then the field $K(\delta)$ is called a cyclotomic extension of K. $\varepsilon(K)$ denotes the group consisting of roots of unity contained in K. $\varepsilon_2(K)$ (resp. $\varepsilon'(K)$) denotes the subgroup of $\varepsilon(K)$ consisting of roots of unity in K whose orders are of 2-power (resp. relatively prime to 2). Let K and k be cyclotomic extensions of Q_2 such that $K\supset k$. Then $\mathfrak{G}(K/k)$ is the Galois group of K over k and for $x\in K$, $N_{K/k}(x)$ is the norm of x over k. For $\sigma\in\mathfrak{G}(K/k)$, x^σ is the image of x by σ. For a positive integer n, the multiplicative group of integers modulo n is denoted by $Z \bmod^\times n$. $\langle a, b, \cdots\rangle$ is the group generated by $a, b, \cdots$.

§2. Preliminaries.

For the remainder of the paper k denotes a cyclotomic extension of the rational 2-adic field Q_2. Let n be a positive integer with $n=2^a n'$, $(2, n')=1$. Let f be the smallest positive integer such that $2^f\equiv 1 \pmod{n'}$. It is well-known that $Q_2(\zeta_n)=Q_2(\zeta_{2^a}, \zeta_{2^f-1})$ and that f is the residue class degree of $Q_2(\zeta_n)$ over Q_2.

LEMMA 1. *Let* h *be the height of* k. *Set* $M=k(\zeta_{2^h})$. *Then* M *is a cyclotomic field* (*over* Q_2) *and contained in every cyclotomic field which contains* k.

That is, M is the minimal cyclotomic field containing k. If the residue class degree of M/Q_2 is f then $M=Q_2(\zeta_{2^h}, \zeta_{2^f-1})$.

PROOF. If $h=0$, the assertions are clear. Suppose that $h \geqq 2$. Let the residue class degree of k/Q_2 be f' and set $K=Q_2(\zeta_{2^h}, \zeta_{2^{f'}-1})$. Then $\zeta_{2^{f'}-1} \in k$, and so $k(\zeta_{2^h}) \supset K$. Let s be an integer such that $L=Q_2(\zeta_{2^h}, \zeta_{2^s-1}) \supset k$. Then $L \supset k(\zeta_{2^h}) \supset K$. Hence f' divides s and every subfield of L over K is of the form $Q_2(\zeta_{2^h}, \zeta_{2^t-1})$, $f'|t$, $t|s$; in particular, so is $k(\zeta_{2^h})$. If f is the residue class degree of $k(\zeta_{2^h})/Q_2$, we conclude that $k(\zeta_{2^h})=Q_2(\zeta_{2^h}, \zeta_{2^f-1})$. If I is a cyclotomic field containing k, then it follows from the definition of the height h of k that $\zeta_{2^h} \in I$, and so $I \supset k(\zeta_{2^h})$. The lemma is proved.

LEMMA 2. *Let h be the height of k. Suppose that $h \geqq 2$. Let $L=Q_2(\zeta_{2^c}, \zeta_{2^s-1})$ $(c \geqq h)$ be a cyclotomic field containing k and let F be the maximal unramified extension of k in L. Then $F(\zeta_4)=Q_2(\zeta_{2^h}, \zeta_{2^s-1})$. In particular, if $c=h$ then $F(\zeta_4)=L$. If $k(\zeta_4)/k$ is unramified, then $F=F(\zeta_4)$. If $k(\zeta_4)/k$ is ramified, then $F(\zeta_4)/F$ is also ramified and $F \cap k(\zeta_4)=k$.*

PROOF. Since the residue class degrees of L and F over Q_2 are the same, ζ_{2^s-1} belongs to F. Recall that the extension $Q_2(\zeta_{2^c})/Q_2(\zeta_4)$ is cyclic and that if I is a subfield of $Q_2(\zeta_{2^c})$ over $Q_2(\zeta_4)$ with $[Q_2(\zeta_{2^c}) : I]=2^r$ then $I=Q_2(\zeta_{2^{c-r}})$. Since $\mathcal{G}(L/Q_2(\zeta_{2^s-1}, \zeta_4))$ is canonically isomorphic to $\mathcal{G}(Q_2(\zeta_{2^c})/Q_2(\zeta_4))$ and $F(\zeta_4) \supset Q_2(\zeta_{2^s-1}, \zeta_4)$, we have $F(\zeta_4)=Q_2(\zeta_{2^s-1}, \zeta_{2^{c-t}})$, where $2^t=[L : F(\zeta_4)]$ $(t \geqq 0)$. Hence $F(\zeta_4)$ is a cyclotomic field containing k. It follows from Lemma 1 that $F(\zeta_4) \supset M=k(\zeta_{2^h})=Q_2(\zeta_{2^h}, \zeta_{2^f-1}) \supset k$, f being the residue class degree of M over Q_2. Clearly, the ramification index of the extension $F(\zeta_4)/M$ is 2^{c-t-h}. We will prove that $F(\zeta_4)/M$ is unramified, so that $c-t=h$. Suppose first that $k(\zeta_4)/k$ is unramified. Then $\zeta_4 \in F$, for F is the maximal unramified extension of k in L. This implies that $F=F(\zeta_4)$ and $F(\zeta_4)/M$ is unramified. Suppose next that $k(\zeta_4)/k$ is ramified. Then $\zeta_4 \notin F$ and $F \cap k(\zeta_4)=k$. It is evident that $F(\zeta_4)/F$ is a ramified extension of degree 2. Since the ramification index of $F(\zeta_4)/k$ is equal to that of $k(\zeta_4)/k$, $F(\zeta_4)/k(\zeta_4)$ is unramified, a fortiori $F(\zeta_4)/M$ is unramified. The lemma is established.

LEMMA 3. *Keeping the notation of Lemma 1, suppose that $h \neq 0$ and $k(\zeta_4)/k$ is ramified. Then $h \geqq 3$. Let E be the maximal unramified extension of k in $M=k(\zeta_{2^h})$. Then $M=E(\zeta_4)$ and M/E is ramified. Let $\langle\omega\rangle=\mathcal{G}(M/E)$ $(\omega^2=1)$ and $\zeta_{2^h}^{\omega}=\zeta_{2^h}^{z}$ for some integer z. Then either $z \equiv -1 \pmod{2^h}$ or $z \equiv -1+2^{h-1}$ $\pmod{2^h}$.*

PROOF. Assume that $h=2$. Then it follows from Lemma 1 that $M=k(\zeta_4)$ $=Q_2(\zeta_4, \zeta_{2^f-1})$, f being the residue class degree of $k(\zeta_4)/Q_2$. Hence, if $k(\zeta_4)/k$ would be ramified, then $k=Q_2(\zeta_{2^f-1})$ and so the height h of k would be equal to 0. This is a contradiction. Thus if $k(\zeta_4)/k$ is ramified, then $h \neq 2$. The second assertion is clear by Lemmas 1 and 2. Recall that $\pm 1 \bmod 2^h$ and

$\pm 1+2^{h-1} \bmod 2^h$ are the only elements of $Z \bmod^{\times} 2^h$ $(h \geqq 3)$ whose (multiplicative) orders divide 2. As $\omega^2=1$, we have $z^2 \equiv 1 \pmod{2^h}$, so that $z \equiv \pm 1$ or $\pm 1+2^{h-1} \pmod{2^h}$. Because $M=E(\zeta_4)=E(\zeta_{2h})$ and $\zeta_4 \notin E$, it follows that $\zeta_4 \neq \zeta_4^{\omega}=\zeta_4^{z}$, and so $z \not\equiv 1,\ 1+2^{h-1} \pmod{2^h}$. Thus we have either $z \equiv -1$ or $-1+2^{h-1} \pmod{2^h}$, proving the lemma.

Lemma 3 proves part of the assertion in Theorem 1, (I).

Let I be a cyclotomic extension of k. As usual, we write $H^2(I/k)$ in place of the 2-cohomology group $H^2(\mathcal{G}(I/k), I^{\times})$. Set $\mathcal{G}=\mathcal{G}(I/k)$. If α is a 2-cocycle of $\mathcal{G}$ with values in $I^{\times}$, then the element of $H^2(I/k)$ represented by α is also denoted by α. The group $\varepsilon(I)$ consisting of roots of unity in I is a multiplicative $\mathcal{G}$-module. We have a canonical homomorphism from the 2-cohomology group $H^2(\mathcal{G}, \varepsilon(I))$ into $H^2(I/k)$. Denote by $C(I/k)$ the image of $H^2(\mathcal{G}, \varepsilon(I))$ by this homomorphism. Let $\varepsilon_2(I)$ (resp. $\varepsilon'(I)$) denote the group of roots of unity in I whose orders are of 2-power (resp. relatively prime to 2). Then $\varepsilon(I)=\varepsilon_2(I) \times \varepsilon'(I)$, and both $\varepsilon_2(I)$ and $\varepsilon'(I)$ are $\mathcal{G}$-modules. We also have a canonical homomorphism from $H^2(\mathcal{G}, \varepsilon_2(I))$ (resp. $H^2(\mathcal{G}, \varepsilon'(I))$ into $H^2(I/k)$, whose image is denoted by $C_2(I/k)$ (resp. $C'(I/k)$). Then it is evident that $C(I/k)=C_2(I/k) \times C'(I/k)$.

Let B be a cyclotomic algebra over k, i.e., B is a crossed product with a factor set β of $k(\zeta)/k$:

$$\begin{aligned} &B=(\beta, k(\zeta)/k)=\sum_{\sigma \in \mathcal{G}} k(\zeta) u_{\sigma} \qquad \text{(direct sum)}, \\ &u_{\sigma} x=x^{\sigma} u_{\sigma} \quad (x \in k(\zeta)), \qquad u_{\sigma} u_{\tau}=\beta(\sigma, \tau) u_{\sigma \tau} \quad (\sigma, \tau \in \mathcal{G}), \end{aligned} \tag{2}$$

where ζ is some root of unity, $\mathcal{G}=\mathcal{G}(k(\zeta)/k)$, and the values of β are in $\varepsilon(k(\zeta))$. In [**5**] we have noticed that the Schur subgroup $S(k)$ consists exactly of those algebra classes of $Br(k)$ which contain a cyclotomic algebra over k. Hence in order to prove Theorem 1 it suffices to show that for the cases (I-iii) and (II) every cyclotomic algebra over k is similar to k and that for the cases (I-i) and (I-ii) there exists a cyclotomic algebra over k with Hasse invariant 1/2. Now the factor set β in (2) is nothing but a 2-cocycle of $\mathcal{G}$ with values in $\varepsilon(k(\zeta)) \subset k(\zeta)^{\times}$, and so determines an element of $C(k(\zeta)/k) \subset H^2(k(\zeta)/k)$, denoted also by β. Let $Q_2(\zeta')$ be a cyclotomic field (over Q_2) containing $k(\zeta)$. Denote by $\alpha=\operatorname{Inf} \beta$ the image of β by the inflation map from $H^2(k(\zeta)/k)$ into $H^2(Q_2(\zeta')/k)$. Then the crossed product

$$A=(\alpha, Q_2(\zeta')/k) \tag{3}$$

is a cyclotomic algebra over k and $[A]=[B]$ in $Br(k)$. Hence we always assume that a cyclotomic algebra over k is of the form in (3). Set $K=Q_2(\zeta')$. For any $\sigma, \tau \in \mathcal{G}(K/k)$, we have $\alpha(\sigma, \tau)=\gamma(\sigma, \tau) \cdot \alpha'(\sigma, \tau)$, $\gamma(\sigma, \tau) \in \varepsilon_2(K)$, $\alpha'(\sigma, \tau)$

$\in \varepsilon'(K)$, so that $\gamma \in C_2(K/k)$, $\alpha' \in C'(K/k)$, and

$$(\alpha, K/k) \sim (\gamma, K/k) \otimes_k (\alpha', K/k)\,. \tag{4}$$

But it follows from a result of Witt [7, p. 243] that $(\alpha', K/k) \sim k$. Thus we may assume that the values of the factor set α in (3) belong to $\varepsilon_2(K)$.

LEMMA 4. *Let L and K be cyclotomic extensions of k such that $L \supset K \supset k$. If $H^2(\mathcal{G}(K/k), \varepsilon_2(K)) \overset{\mathrm{Inf}}{\cong} H^2(\mathcal{G}(L/k), \varepsilon_2(L))$, then $C_2(K/k) \overset{\mathrm{Inf}}{\cong} C_2(L/k)$. If $H^2(\mathcal{G}(K/k), \varepsilon'(K)) \overset{\mathrm{Inf}}{\cong} H^2(\mathcal{G}(L/k), \varepsilon'(L))$, then $C'(K/k) \overset{\mathrm{Inf}}{\cong} C'(L/k)$. Here,* Inf *denotes the inflation map.*

PROOF. The inflation map from $H^2(K/k)$ into $H^2(L/k)$, which is one-to-one, induces an isomorphism (denoted also by Inf) from $C_2(K/k)$ into $C_2(L/k)$. If the inflation map from $H^2(\mathcal{G}(K/k), \varepsilon_2(K))$ into $H^2(\mathcal{G}(L/k), \varepsilon_2(L))$ is surjective, then it is evident that the inflation map from $C_2(K/k)$ into $C_2(L/k)$ is also surjective, so that $C_2(K/k) \overset{\mathrm{Inf}}{\cong} C_2(L/k)$. The proof is identical for $C'(K/k) \overset{\mathrm{Inf}}{\cong} C'(L/k)$.

LEMMA 5. *Let G be a finite group and let W be a finite G-module. Let H be a normal subgroup of G. Suppose that H is cyclic. Set $N = \sum_{h \in H} h$. If the image $N(W)$ of W by N equals W^H, the subset of elements of W fixed by every element of H, then we have*

$$H^2(G/H, W^H) \cong H^2(G, W)\,.$$

The inflation map gives this isomorphism.

PROOF. Let n be any non-negative integer. As H is cyclic, $H^n(H, W)$ depends only on the evenness or oddness of n. If n is even then $H^n(H, W) = W^H/N(W)$. Since W is finite, the Herbrand quotient of the H-module W equals 1, and so the orders of $H^n(H, W)$ and $H^{n+1}(H, W)$ are the same. Thus if $N(W) = W^H$ then $H^n(H, W) = 0$ for every non-negative integer n. (For the above arguments, see [2, VIII, § 4].) Now we have

$$0 \longrightarrow H^2(G/H, W^H) \xrightarrow{\mathrm{Inf}} H^2(G, W) \xrightarrow{\mathrm{Res}} H^2(H, W) \qquad \text{(exact)}$$

because $H^1(H, W) = 0$ (cf. [2, Proposition 5, p. 126]). As $H^2(H, W) = 0$, it follows that the above inflation map is an isomorphism from $H^2(G/H, W^H)$ onto $H^2(G, W)$.

LEMMA 6. *Let L and K be cyclotomic extensions of k such that $L \supset K \supset k$ and L/K is cyclic. If $N_{L/K}(\varepsilon_2(L)) = \varepsilon_2(K)$ then $C_2(K/k) \overset{\mathrm{Inf}}{\cong} C_2(L/k)$. If $N_{L/K}(\varepsilon'(L)) = \varepsilon'(K)$ then $C'(K/k) \overset{\mathrm{Inf}}{\cong} C'(L/k)$.*

PROOF. If $N_{L/K}(\varepsilon_2(L))=\varepsilon_2(K)$ then it follows from Lemma 5 that $H^2(\mathcal{G}(K/k), \varepsilon_2(K)) \overset{\textbf{Inf}}{\cong} H^2(\mathcal{G}(L/k), \varepsilon_2(L))$, and so by Lemma 4, we have $C_2(K/k) \overset{\text{Inf}}{\cong} C_2(L/k)$. The same proof holds for $C'(K/k) \overset{\text{Inf}}{\cong} C'(L/k)$.

The following fact is well-known:

LEMMA 7. *Let K be an unramified extension of k. Then $C(K/k)=1$.*

PROOF. The Galois group $\mathcal{G}=\mathcal{G}(K/k)$ of K over k is cyclic. Let φ be a generator of $\mathcal{G}$. Set $s=[K:k]$. Let α be any element of $C(K/k)$. Then α can be regarded as a factor set of K/k such that $\alpha(\sigma, \tau)\in\varepsilon(K)$ for any $\sigma, \tau\in\mathcal{G}$. Consider a crossed product B with the factor set α:

$$B=(\alpha, K/k)=\sum_{\sigma\in\mathcal{G}} Ku_\sigma \qquad \text{(direct sum)},$$

$$u_\sigma u_\tau=\alpha(\sigma, \tau)u_{\sigma\tau}, \qquad u_\sigma x=x^\sigma u_\sigma \qquad (x\in K).$$

Then we have

$$B=\sum_{t=0}^{s-1} Ku_\varphi^t=(u_\varphi^s, K/k, \varphi),$$

$$u_\varphi^s=\alpha(\varphi, \varphi)\alpha(\varphi^2, \varphi)\cdots\alpha(\varphi^{s-1}, \varphi)\alpha(1, 1)\in\varepsilon(K).$$

This cyclic algebra is similar to k, because u_φ^s is a unit of k and so a norm of an element of K. This implies that as an element of $C(K/k)\subset H^2(K/k)$, α is equal to 1.

LEMMA 8. *Let l and a be positive integers such that $2\leqq a\leqq l$. Set $K=Q_2(\zeta_{2^l})$ and $k=Q_2(\zeta_{2^a})$. Then $N_{K/k}(\zeta_{2^l})$ is a primitive 2^a-th root of unity, i.e., $N_{K/k}(\langle\zeta_{2^l}\rangle)=\langle\zeta_{2^a}\rangle$.*

PROOF. This fact is also well-known, and so we will sketch the proof. The extension K/k is cyclic of degree 2^{l-a}. A generator of its Galois group is given by $\phi: \zeta_{2^l}\mapsto\zeta_{2^l}^r$, $r=1+2^a$. The number t defined by

$$t=1+r+\cdots+r^{2^{l-a}-1}=(r^{2^{l-a}}-1)/(r-1) \qquad (a\geqq 2)$$

is exactly divisible by 2^{l-a}. Because $N_{K/k}(\zeta_{2^l})=\zeta_{2^l}^t$, it follows that $N_{K/k}(\zeta_{2^l})$ is a primitive 2^a-th root of unity, proving the lemma.

§ 3. Proof of Theorem 1.

PROPOSITION 1. *Let I be a cyclotomic extension of k. Then $C'(I/k)=1$, so that $C(I/k)=C_2(I/k)$. The order of $C(I/k)$ is at most 2. If $k(\zeta_4)/k$ is unramified, then $C(I/k)=1$.*

PROOF. Let L be a cyclotomic field over Q_2 containing I and ζ_4. We may write $L=Q_2(\zeta_{2^c}, \zeta_{2^s-1})$ for some $c\geqq 2$ and s. For simplicity, set $q=2^s$. The inflation map from $H^2(I/k)$ into $H^2(L/k)$ is one-to-one and maps $C'(I/k)$,

$C_2(I/k)$ and $C(I/k)$ into $C'(L/k)$, $C_2(L/k)$ and $C(L/k)$ respectively. Hence it suffices to prove that if $k(\zeta_4)/k$ is unramified then $C(L/k)=1$ and that if $k(\zeta_4)/k$ is ramified then $C'(L/k)=1$ and the order of $C(L/k)$ is at most 2. Let h be the height of k. Let F be the maximal unramified extension of k in L. If $h=0$ then F/Q_2 is unramified, so that $F=Q_2(\zeta_{q-1})$ and $F(\zeta_4)=Q_2(\zeta_{q-1}, \zeta_4)$. If $h\geqq 2$, then by Lemma 2, $F(\zeta_4)=Q_2(\zeta_{2^h}, \zeta_{q-1})$. Hence for any h, the extension $L/F(\zeta_4)$ is totally ramified and cyclic of degree 2^a, where $a=c-2$ for $h=0$ and $a=c-h$ for $h\geqq 2$. For simplicity, put $K=F(\zeta_4)$. We have

$$N_{L/K}(\varepsilon'(L))=\langle\zeta_{q-1}^{2^a}\rangle=\langle\zeta_{q-1}\rangle=\varepsilon'(K)\,, \qquad (2, q-1)=1\,.$$

Since the Galois group $\mathcal{G}(L/K)$ is canonically isomorphic to $\mathcal{G}(Q_2(\zeta_{2^c})/Q_2(\zeta_{2^{c-a}}))$ and $c-a\geqq 2$, Lemma 8 implies that

$$N_{L/K}(\varepsilon_2(K))=N_{L/K}(\langle\zeta_{2^c}\rangle)=\langle\zeta_{2^{c-a}}\rangle=\varepsilon_2(K)\,.$$

It follows from Lemma 6 that $C'(K/k)\overset{\text{Inf}}{\cong} C'(L/k)$, $C_2(K/k)\overset{\text{Inf}}{\cong} C_2(L/k)$, and consequently $C(K/k)\overset{\text{Inf}}{\cong} C(L/k)$. If $k(\zeta_4)/k$ is unramified, then $h\geqq 2$ and Lemma 2 implies that $K=F$. Hence K/k is unramified, and so by Lemma 7, $C(L/k)\cong C(K/k)=1$. Suppose that $k(\zeta_4)/k$ is ramified. Then K/F is also ramified with $[K: F]=2$, and $N_{K/F}(\varepsilon'(K))=\langle\zeta_{q-1}^2\rangle=\langle\zeta_{q-1}\rangle=\varepsilon'(F)$. Hence by Lemma 6, we have $C'(F/k)\overset{\text{Inf}}{\cong} C'(K/k)$, so that $C'(F/k)\overset{\text{Inf}}{\cong} C'(L/k)$. As F/k is unramified, it follows from Lemma 7 that $C'(F/k)=1$, and consequently $C'(L/k)=1$. Denote by Res the restriction homomorphism of $H^2(K/k)$ into $H^2(K/k(\zeta_4))$. Then Res maps $C(K/k)$ into $C(K/k(\zeta_4))$. For any element α of $C(K/k)$, we have $\operatorname{inv}(\operatorname{Res}(\alpha))=[k(\zeta_4): k]\cdot\operatorname{inv}(\alpha)=2\operatorname{inv}(\alpha)$, where $\operatorname{inv}(\operatorname{Res}(\alpha))$ (resp. $\operatorname{inv}(\alpha)$) denotes the (Hasse) invariant of $\operatorname{Res}(\alpha)$ (resp. α). (See [**2**, p. 175].) Since $K/k(\zeta_4)$ is unramified, it follows from Lemma 7 that $C(K/k(\zeta_4))=1$, and so $\operatorname{inv}(\operatorname{Res}(\alpha))=0$. Hence $\operatorname{inv}(\alpha)=0$ or $1/2$. This implies that the order of $C(K/k)\cong C(L/k)$ is at most 2.

Proposition 2. *Let h be the height of k. Set $l=h$ for $h\geqq 2$ and $l=2$ for $h=0$. Then any cyclotomic algebra $(\beta, k(\zeta)/k)$ over k (defined by* (2)*) is similar to a cyclotomic algebra of the form $(\alpha, K/k)$, where $K=Q_2(\zeta_{2^l}, \zeta_{2^s-1})$, s being some integer. The values of the above factor set α may be assumed to be in $\varepsilon_2(K)$.*

Proof. Let $L=Q_2(\zeta_{2^c}, \zeta_{2^s-1})$ be a cyclotomic field containing $k(\zeta)$ and ζ_4, where c $(\geqq 2)$ and s are some integers. Let F be the maximal unramified extension of k in L. Then from the proof of Proposition 1 it follows that $F(\zeta_4)=K=Q_2(\zeta_{2^l}, \zeta_{2^s-1})$ and that $C(K/k)\overset{\text{Inf}}{\cong} C(L/k)$. The factor set β determines an element of $C(k(\zeta)/k)$, denoted also by β. Let β' be the image of β by the inflation map from $C(k(\zeta)/k)$ into $C(L/k)$: $\beta'=\operatorname{Inf}\beta$. Then there exists an element α of $C(K/k)$ such that $\beta'=\operatorname{Inf}\alpha$, the inflation map being from $C(K/k)$ onto $C(L/k)$. Therefore we have $(\alpha, K/k)\sim(\beta', L/k)\sim(\beta, k(\zeta)/k)$. Since $C(K/k)=C_2(K/k)$, the values of α may be assumed to be in $\varepsilon_2(K)$.

PROPOSITION 3. *The order of the Schur subgroup $S(k)$ of k is at most* 2. *If $k(\zeta_4)/k$ is unramified then $S(k)=1$.*

PROOF. As was already mentioned, $S(k)$ consists exactly of those algebra classes of $Br(k)$ that are represented by a cyclotomic algebra over k. Let $B=(\beta, k(\zeta)/k)$ (defined by (2)) be any cyclotomic algebra over k. Then the factor set β determines an element of $C(k(\zeta)/k)$, denoted also by β. Then Proposition 1 implies that the invariant of β (i.e., the Hasse invariant of B) is 0 or 1/2 and that if $k(\zeta_4)/k$ is unramified then the invariant of β is 0. As B is an arbitrary cyclotomic algebra over k, the proposition is proved.

For the remainder of the paper we will use the same notation as in Theorem 1. We have just proved part (II) of Theorem 1. Next we will deal with the case (I)-iii). Namely, suppose that $k(\zeta_4)/k$ is ramified and that $h\geqq 3$ and $z\equiv -1+2^{h-1} \pmod{2^h}$. Let B be any cyclotomic algebra over k. We need to show that $B\sim k$. By Proposition 2 we may write

$$B=(\alpha, K/k)=\sum_{\sigma\in\mathcal{G}} Ku_\sigma\,, \qquad K=Q_2(\zeta_{2h}, \zeta_{2^s-1})\,, \tag{5}$$

where $\mathcal{G}=\mathcal{G}(K/k)$ and s is some integer. We may also assume that $\alpha(\sigma, \tau)\in\varepsilon_2(K)=\langle\zeta_{2h}\rangle$ for every $\sigma, \tau\in\mathcal{G}$. Let F be the maximal unramified extension of k in K. Then by Lemma 2, $K=F\cdot k(\zeta_4)$ and $F\cap k(\zeta_4)=k$. Recall that the field $M=k(\zeta_{2h})=Q_2(\zeta_{2h}, \zeta_{2f-1})$ is the minimal cyclotomic field containing k, f being the residue class degree of $k(\zeta_{2h})/Q_2$, and that if E is the maximal unramified extension of k in M then $\mathcal{G}(M/E)=\langle\omega\rangle$ with $\zeta_{2h}^\omega=\zeta_{2h}^z$. Since $\mathcal{G}(K/F)$ is canonically isomorphic to $\mathcal{G}(M/E)$, we may write

$$\mathcal{G}(K/F)=\langle\omega\rangle\,, \qquad \zeta_{2h}^\omega=\zeta_{2h}^z\,, \qquad z\equiv -1+2^{h-1} \pmod{2^h}\,.$$

Set $t=[K: k(\zeta_4)]=[F: k]$ and let φ be a generating automorphism of $K/k(\zeta_4)$. Then $\mathcal{G}(K/k)=\langle\omega\rangle\times\langle\varphi\rangle$, $\omega^2=\varphi^t=1$, and

$$B=\sum_{i=0}^{1}\sum_{j=0}^{t-1} k(\zeta_4)\cdot Fu_\omega^i u_\varphi^j\,. \tag{6}$$

We may assume that $u_1=1$, i.e., $\alpha(\sigma, 1)=\alpha(1, \sigma)=1$ for any $\sigma\in\mathcal{G}(K/k)$. Since the values of α are in $\varepsilon_2(K)=\langle\zeta_{2h}\rangle$, it follows that

$$\begin{aligned} &\alpha(\omega, \varphi)/\alpha(\varphi, \omega)=\zeta_{2h}^a\,, \qquad \alpha(\omega, \omega)=\zeta_{2h}^{b'}\,, \\ &\alpha(\varphi, \varphi)\alpha(\varphi^2, \varphi)\cdots\alpha(\varphi^{t-1}, \varphi)=\zeta_{2h}^c \end{aligned} \tag{7}$$

for some integers a, b', c. Then we have

$$u_\omega u_\varphi = \zeta_{2^h}^a u_\varphi u_\omega\,, \qquad u_\omega^2 = \zeta_{2^h}^{b'}\,, \qquad u_\varphi^t = \zeta_{2^h}^c\,. \tag{8}$$

Because $h \geqq 3$ and

$$\zeta_{2^h}^{b'(-1+2^{h-1})} = (\zeta_{2^h}^{b'})^\omega = u_\omega u_\omega^2 u_\omega^{-1} = \zeta_{2^h}^{b'}$$

it follows that 2^{h-1} divides b', and so $u_\omega^2 = (-1)^b$ for some integer b. Since α is a factor set of K/k, the above integers a, b and c must satisfy some relations. This subject has been studied in [**6**, Section 1]. By [**6**, (1.11)] we have

$$1 = ((-1)^b)^{\varphi-1} = (\zeta_{2^h}^{-a})^{1+\omega} = \zeta_{2^h}^{-a2^{h-1}} = (-1)^a\,.$$

Hence 2 divides a. Consider the following congruence with the indeterminate X:

$$2(2^{h-2}-1)X \equiv -a \pmod{2^h}\,. \tag{9}$$

Since 2 divides a, this congruence has a solution $X = x$, which is unique mod 2^{h-1}. For this integer x, we have

$$\begin{aligned} u_\omega(\zeta_{2^h}^x u_\varphi) &= \zeta_{2^h}^{x(-1+2^{h-1})} u_\omega u_\varphi = \zeta_{2^h}^{x(-1+2^{h-1})+a} u_\varphi u_\omega \\ &= \zeta_{2^h}^{x+x(-2+2^{h-1})+a} u_\varphi u_\omega = (\zeta_{2^h}^x u_\varphi) u_\omega\,. \end{aligned}$$

That is, u_ω commutes with $\zeta_{2^h}^x u_\varphi$. Since each element of $k(\zeta_4)$ (resp. F) commutes with $\zeta_{2^h}^x u_\varphi$ (resp. u_ω), we have

$$\begin{aligned} B &= \sum_{i=0}^{1} \sum_{j=0}^{t-1} k(\zeta_4) \cdot F u_\omega^i (\zeta_{2^h}^x u_\varphi)^j \\ &= \Big[\sum_{i=0}^{1} k(\zeta_4) u_\omega^i\Big] \cdot \Big[\sum_{j=0}^{t-1} F(\zeta_{2^h}^x u_\varphi)^j\Big] \\ &\cong (u_\omega^2,\, k(\zeta_4)/k,\, \omega) \otimes_k ((\zeta_{2^h}^x u_\varphi)^t,\, F/k,\, \varphi)\,. \end{aligned} \tag{10}$$

We will show that the above cyclic algebras are both similar to k. From the assumption $h \geqq 3$ it follows that k/Q_2 is ramified and so $[k : Q_2]$ is even. Recall that $u_\omega^2 = \pm 1$ and that the index of the cyclic algebra $(\pm 1, k(\zeta_4)/k, \omega)$ is equal to the order of the (local) norm residue symbol $(\pm 1, k(\zeta_4)/k)$. But $(\pm 1, k(\zeta_4)/k) = (N_{k/Q_2}(\pm 1), k(\zeta_4)/Q_2) = (1, k/Q_2) = 1$, for $[k : Q_2]$ is even. Hence $(u_\omega^2, k(\zeta_4)/k, \omega) \sim k$. Next we note that

$$(\zeta_{2^h}^x u_\varphi)^t = \zeta_{2^h}^{x(1+\varphi+\cdots+\varphi^{t-1})} u_\varphi^t = \zeta_{2^h}^{x(1+\varphi+\cdots+\varphi^{t-1})+c} \in \langle \zeta_{2^h} \rangle\,.$$

Since F/k is unramified, we conclude that the second cyclic algebra in (10) is similar to k. This proves Theorem 1 for the case (I)-iii).

Finally we must show that for the cases (I)-i) and (I)-ii), there exists a cyclotomic algebra over k with Hasse invariant 1/2. Suppose that $k(\zeta_4)/k$ is *ramified.* By Lemma 3, either $h=0$ or $h\geqq 3$. If $h\geqq 3$, then put $K=k(\zeta_{2^h})$. By Lemma 2, K is the minimal cyclotomic field containing k and $K=Q_2(\zeta_{2^h}, \zeta_{2^f-1})$, f being the residue class degree of $k(\zeta_{2^h})/Q_2$. If $h=0$, then put $K=k(\zeta_4)$, so that $K=Q_2(\zeta_4, \zeta_{2^f-1})$, f being the residue class degree of k/Q_2. Set $l=h$ for $h\geqq 3$ and $l=2$ for $h=0$. Then we can write $K=Q_2(\zeta_{2^l}, \zeta_{2^f-1})$. Put $L=Q_2(\zeta_{2^l}, \zeta_{2^{2f}-1})$. Then L is the unramified extension of K of degree 2. Denote by F the maximal unramified extension of k in L. By Lemma 2, $L=k(\zeta_4)\cdot F$ and $k(\zeta_4)\cap F=k$. (For $h=0$, this statement is obvious, because $F=Q_2(\zeta_{2^{2f}-1})$ and $k=Q_2(\zeta_{2^f-1})$.) Let E be the maximal unramified extension of k in K ($E=k$ for $h=0$). Then $\mathcal{G}(L/F)$ is canonically isomorphic to $\mathcal{G}(K/E)$, so that for the cases (I)-i) and (I)-ii), we have

$$\mathcal{G}(L/F)=\langle\omega\rangle\,, \qquad \omega^2=1\,, \qquad \zeta_{2^l}^{\omega}=\zeta_{2^l}^{-1}\,. \tag{11}$$

Let φ be a generating automorphism of the unramified extension $L/k(\zeta_4)$. Then $\mathcal{G}(L/k)=\langle\omega\rangle\times\langle\varphi\rangle$. Set $r=[K:k(\zeta_4)]$, so that $[L:k(\zeta_4)]=[F:k]=2r$ and $\varphi^{2r}=1$. We choose the odd numbers $3, 5, \cdots, 2^l-1, 2^l+1$ as a system of representatives of integers $\bmod 2^l$ relatively prime to 2. Let ϕ denote the restriction of φ onto K, i. e., ϕ is the generating automorphism of $K/k(\zeta_4)$ defined by $x^{\phi}=x^{\varphi}$ $(x\in K)$. Then $\mathcal{G}(K/k(\zeta_4))=\langle\phi\rangle$, $\phi^r=1$, and

$$\zeta_{2^l}^{\phi}=\zeta_{2^l}^{\varphi}=\zeta_{2^l}^{t} \tag{12}$$

for some integer t such that $(2, t)=1$ and $3\leqq t\leqq 2^l+1$. Note that $t=1+2^2$ for $h=0$, because $K=k(\zeta_4)$ and $\phi=1$. Write $t=1+2^a m$, $(2, m)=1$, $2\leqq 2^a m\leqq 2^l$. Since $\zeta_4^t=\zeta_4^{\phi}=\zeta_4$, it follows that $2\leqq a(\leqq l)$. Consequently, the order of $t \bmod 2^l$ in $Z \bmod^{\times} 2^l$ equals 2^{l-a}. (For $l\geqq 3$, this fact is well-known and follows easily, for instance, from [4, Lemma 1]. See also [**1**, I, § 4, 5]. For $l=2$, the statement is evident, because $t=1+2^2$, $a=2$.) Hence the order of ϕ, which is equal to r, is divisible by 2^{l-a}. It follows easily from this that $t^{2r}-1=(1+2^a m)^{2r}-1$ is divisible by $2^{l+1}m$. Now we set

$$y=(t^{2r}-1)/2^{l+1}m\,. \tag{13}$$

We will construct a cyclotomic algebra B over k as follows: Set

$$h_{\varphi}=\zeta_{2^a}^{-y}\,, \quad h_{\omega}=1\,, \quad h_{\omega,\varphi}=\zeta_{2^l}\,, \quad h_{\varphi,\omega}=\zeta_{2^l}^{-1}\,, \quad (\zeta_{2^l}^{2^{l-a}}=\zeta_{2^a})\,. \tag{14}$$

Then $\zeta_{2^a}^{\varphi}=\zeta_{2^a}^{t}=\zeta_{2^a}$, and so $(h_{\varphi})^{\varphi}=h_{\varphi}$. Obviously, $(h_{\omega})^{\omega}=h_{\omega}$. We have $h_{\omega}^{\varphi-1}=1$ and $h_{\varphi,\omega}^{1+\omega}=\zeta_{2^l}^{-(1-1)}=1$, so that $h_{\omega}^{\varphi-1}=h_{\varphi,\omega}^{1+\omega}$. Because $1+t+\cdots+t^{2r-1}=(t^{2r}-1)/(t-1)=y2^{l+1-a}$, it follows that

$$h_{\omega,\varphi}^{1+\varphi+\cdots+\varphi^{2r-1}}=\zeta_{2^l}^{1+t+\cdots+t^{2r-1}}=\zeta_{2^a}^{2y}\,.$$

On the other hand, we have $h_{\varphi}^{\omega-1}=(\zeta_{2^a}^{-y})^{-1-1}=\zeta_{2^a}^{2y}$. Consequently, $h_{\varphi}^{\omega-1}=h_{\omega,\varphi}^{1+\varphi+\cdots+\varphi^{2r-1}}$. Thus the elements $h_{\varphi}, h_{\omega}, h_{\omega,\varphi}, h_{\varphi,\omega}$ satisfy the relations of

[6, (1.9)-(1.11)] and so give rise to a cyclotomic algebra B over k (cf. [6, Section 1]):

$$B=\sum_{i=0}^{1}\sum_{j=0}^{2r-1} Lu_\omega^i u_\varphi^j \qquad \text{(direct sum)},$$

$$u_\omega u_\varphi=\zeta_{2^l}u_\varphi u_\omega\,, \qquad u_\omega^2=1\,, \qquad u_\varphi^{2r}=\zeta_{2^a}^{-y}\,,$$

$$u_\omega^i u_\varphi^j x=x^{\omega^i\varphi^j}u_\omega^i u_\varphi^j \qquad (x\in L)\,.$$

Because

$$u_\omega\{(1+\zeta_{2^l})u_\varphi\}=(1+\zeta_{2^l}^{-1})\zeta_{2^l}u_\varphi u_\omega=\{(1+\zeta_{2^l})u_\varphi\}u_\omega\,,$$

it follows that u_ω commutes with $(1+\zeta_{2^l})u_\varphi$. Since $L=k(\zeta_4)\cdot F$ and each element of $k(\zeta_4)$ (resp. F) commutes with $(1+\zeta_{2^l})u_\varphi$ (resp. u_ω), we have

$$\begin{aligned}
B&=\sum_{i=0}^{1}\sum_{j=0}^{2r-1} k(\zeta_4)\cdot Fu_\omega^i((1+\zeta_{2^l})u_\varphi)^j\\
&=\Big[\sum_{i=0}^{1}k(\zeta_4)u_\omega^i\Big]\cdot\Big[\sum_{j=0}^{2r-1}F((1+\zeta_{2^l})u_\varphi)^j\Big]\\
&\cong(u_\omega^2,\, k(\zeta_4)/k,\, \omega)\otimes_k((1+\zeta_{2^l})u_\varphi)^{2r},\, F/k,\, \varphi)\sim(\delta,\, F/k,\, \varphi) \qquad (u_\omega^2=1)\,,\\
\delta&=((1+\zeta_{2^l})u_\varphi)^{2r}\\
&=(1+\zeta_{2^l})(1+\zeta_{2^l}^{\varphi})\cdots(1+\zeta_{2^l}^{\varphi^{2r-1}})u_\varphi^{2r}\\
&=\prod_{i=0}^{2r-1}(1+\zeta_{2^l}^{t^i})\zeta_{2^a}^{-y}\in k\,.
\end{aligned}$$

For each i, $-\zeta_{2^l}^{t^i}$ is a primitive 2^l-th root of unity. Because $L=Q_2(\zeta_{2^{2f}-1},\zeta_{2^l})$, it follows that

$$1+\zeta_{2^l}^{t^i}=1-(-\zeta_{2^l}^{t^i}) \qquad (i=0,1,\cdots,2r-1)$$

is a prime element of L. Denote by v_L (resp. v_k) the normalized discrete valuation of L (resp. k), i.e., $v_L(\Pi)=v_k(\pi)=1$, where Π (resp. π) is a prime element of L (resp. k). Then $v_L(x)=2v_k(x)$ for every x of k, for the ramification index of L/k equals 2. Now we have

$$2v_k(\delta)=v_L(\delta)=\sum_{i=0}^{2r-1}v_L(1+\zeta_{2^l}^{t^i})+v_L(\zeta_{2^a}^{-y})=2r$$

and so $v_k(\delta)=r=[F:k]/2$. Because F/k is unramified, it follows from the definition of Hasse invariant that the above cyclic algebra $(\delta, F/k, \varphi)$ has Hasse invariant $v_k(\delta)/[F:k]=1/2$, so that the cyclotomic algebra B has Hasse invariant 1/2. This proves Theorem 1 for the cases (I)-i) and (I)-ii). Thus the proof of Theorem 1 is completed.

PROOF OF THEOREM 3. Keeping the notation of Theorem 3, let $[A]$ be an element of $S(K)$. Then A may be assumed to be a cyclotomic algebra over K: $A=(\alpha, K(\zeta)/K)$, where ζ is a root of unity and the values of the factor set α belong to $\varepsilon(K(\zeta))$, the group of roots of unity contained in $K(\zeta)$. Let ζ' be a generator of the cyclic group $\varepsilon(K(\zeta))$. Then the values of α belong to $\langle\zeta'\rangle\subset k(\zeta')$ and $K(\zeta)=K(\zeta')$. Because k is the maximal cyclotomic extension of Q_2 in K and $k(\zeta')$ is a cyclotomic extension of Q_2, it follows that $k(\zeta')\cap K=k$. Therefore the Galois group of $K(\zeta)/K$ is canonically isomorphic to that of $k(\zeta')/k$, and so α can be regarded as a factor set of $k(\zeta')/k$. Let B be the cyclotomic algebra over k with the factor set $\alpha: B=(\alpha, k(\zeta')/k)$. Then it is evident that $A\sim B\otimes_k K$, $[B]\in S(k)$. This implies that $S(K)\subset S(k)\otimes_k K$. Conversely, for any cyclotomic algebra B over k, $B\otimes_k K$ is also a cyclotomic algebra over K, and consequently we have $S(K)=S(k)\otimes_k K$. From this, Theorem 3 follows immediately.

References

[1] H. Hasse, Zahlentheorie, 2nd edition, Akademie-Verlag, Berlin, 1963.

[2] J.-P. Serre, Corps locaux, 2nd edition, Hermann, Paris, 1968.

[3] 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.

[4] T. Yamada, Central simple algebras over totally real fields which appear in $Q[G]$, J. Algebra, 23 (1972), 382-403.

[5] T. Yamada, The Schur subgroup of the Brauer group, (to appear).

[6] T. Yamada, The Schur subgroup of the Brauer group I, to appear in J. Algebra, 27 (1973).

[7] E. Witt, Die algebraische Struktur des Gruppenringes einer endlichen Gruppe über einem Zahlkörper, J. Reine Angew. Math., 190 (1952), 231-245.

Toshihiko YAMADA

Department of Mathematics
Tokyo Metropolitan University
Fukazawa, Setagaya-ku
Tokyo, Japan