J. Math. Soc. Japan
Vol. 34, No. 2, 1982

The Schur index over the 2-adic field

By Toshihiko YAMADA

(Received Sept. 22, 1980)

Let k be a field of characteristic 0 and let B be a cyclotomic algebra over k; that is, a crossed product $(\alpha, k(\zeta)/k)$ in which ζ is a root of unity and α is a factor set on $\mathrm{Gal}(k(\zeta)/k)$ having only roots of unity as values. R. Brauer [**1**], [**2**] and E. Witt [**5**] reduced the problem of determining the Schur index of a character of a finite group to the case of handling the index of a cyclotomic algebra. And E. Witt [**5**] gave a formula of index of it which is central over the rational p-adic field Q_p. But in order to investigate the Schur index and the Schur group of an algebraic number field in detail, it is necessary to obtain the formula of index of a cyclotomic algebra which is central over an arbitrary extension k of Q_p. And this was done by the author [**6**, Theorem 3] for an odd prime p (for the application of the formula, see [**3**], [**6**], [**9**], [**10**]). In [**9**, Theorem 5.6] we also handled the remaining case $p=2$ and obtained a formula when the field k and the factor set α satisfy some conditions.

The purpose of the paper is to settle the case $p=2$ completely. Namely, for any finite extension k of the rational 2-adic field Q_2, we give the formula of index of any cyclotomic algebra $(\alpha, k(\zeta)/k)$ which is central over k (Theorem 2). This will be achieved by embedding the field $k(\zeta)$ into a field L, where the residue class degree of L is sufficiently large and a primitive 2^m-th root of unity ζ_{2^m} belongs to L with a sufficiently large integer m. Thus using this formula for the 2-adic field Q_2 and the formula for the p-adic field Q_p $(p\neq 2)$ in [**6**, Theorem 3], combined with the Brauer-Witt theorem [**9**, p. 31], we can determine the Schur index of a character of a finite group, over an algebraic number field.

NOTATION. For a finite extension field K of the 2-adic numbers Q_2, $\varepsilon_2(K)$ (resp. $\varepsilon'(K)$) is the group of roots of unity whose orders are of 2-power order (resp. relatively prime to 2). For a natural number m, ζ_m is a primitive m-th root of unity. If L is a Galois extension of K then $\mathcal{G}(L/K)$ is the Galois group of L over K. $|\mathcal{G}(L/K)|$ is the order of $\mathcal{G}(L/K)$. $|\sigma|$ is the order of $\sigma\in\mathcal{G}(L/K)$. $\mathcal{T}(L/K)$ is the inertia group of the extension L/K. $e(L/K)=|\mathcal{T}(L/K)|=$the ramification index of L/K. If M is a Galois extension of K such that $M\supset L\supset K$, then for $\sigma\in\mathcal{G}(M/K)$, $\sigma|L$ is the restriction of σ on L. If ζ is a root of unity any subfield of $Q_2(\zeta)$ is called a cyclotomic extension of Q_2.

1. The Schur group.

For the rest of the paper, k is a cyclotomic extension of Q_2. The subset of the Brauer group $\mathrm{Br}(k)$ of k consisting of all those classes containing an algebra which is isomorphic to a simple summand of the group algebra $k[G]$ for some finite group G is a subgroup, $S(k)$, the Schur group of k. It follows from the Brauer-Witt theorem that this is the same group as the set of classes in $\mathrm{Br}(k)$ which contain a cyclotomic algebra over k (cf. [**9**, Corollary 3.11]). In order to state our formula of index of a cyclotomic algebra over k, we need the result on the Schur group of k which was obtained by the author [**7**].

Let h be the smallest nonnegative integer such that k is contained in a cyclotomic field $Q_2(\zeta_{2^h t})$ for some odd integer t. We will call h the height of k. It is clear that either $h=0$ or $h\geqq 2$, and that $h=0$ if and only if k/Q_2 is unramified. Let s be the smallest positive integer such that $2^s\equiv 1 \pmod t$. It is well-known that $Q_2(\zeta_{2^h t})=Q_2(\zeta_{2^h}, \zeta_{2^s-1})$. The following lemmas are easy to prove and their proofs are given in [**7**].

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 $M=Q_2(\zeta_{2^h}, \zeta_{2^f-1})$.*

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

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

Now we can state the theorem which completely determines the Schur group $S(k)$ of k.

THEOREM 1 (Yamada [**7**]). *Let k be a cyclotomic extension of Q_2 and let h be the height of k. Let the notation be as in Lemma* 3. (I) *If $k(\zeta_4)/k$ is unramified (including the case $\zeta_4\in k$), then $S(k)=1$.* (II) *If $k(\zeta_4)/k$ 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* $\mathrm{Br}(k)$. *For the case* (iii), $S(k)=1$.

Let $L_{c,s}=Q_2(\zeta_{2^c}, \zeta_{2^s-1})$, ($c\geqq 2$) be a cyclotomic field containing k. Let $\iota_{c,s}\in \mathcal{G}(L_{c,s}/Q_2)$ be such that $\iota_{c,s}(\zeta_{2^c})=\zeta_{2^c}^{-1}$, $\iota_{c,s}(\zeta_{2^s-1})=\zeta_{2^s-1}$. We see easily that if for some c and s, $\iota_{c,s}\in\mathcal{G}(L_{c,s}/k)$ then $\iota_{c',s'}\in\mathcal{G}(L_{c',s'}/k)$ for any c' and s' such that

$L_{c',s'}=Q_2(\zeta_{2^{c'}},\zeta_{2^{s'}-1})\supset k$, $(c'\geqq 2)$. It is clear that Theorem 1 is equivalent to the following

THEOREM 1′ ([8]). *Let k be a cyclotomic extension of Q_2. Then only the following two cases happen: (1) For any c and s such that $L_{c,s}\supset k$ $(c\geqq 2)$, $\iota_{c,s}\in \mathcal{G}(L_{c,s}/k)$ and $S(k)$ is the subgroup of order 2 of $\mathrm{Br}(k)$. (2) For any c and s, $\iota_{c,s}\notin \mathcal{G}(L_{c,s}/k)$ and $S(k)=1$.*

Put $L=L_{c,s}\supset k$, $\iota=\iota_{c,s}$. Note that $\iota\in\mathcal{G}(L/k)$ if and only if $\iota|k=1\in\mathcal{G}(k/Q_2)$. It is well-known that ι is the norm residue symbol $(-1, L/Q_2)\in\mathcal{G}(L/Q_2)$, $\iota|k=(-1, k/Q_2)$. Therefore, $\iota|k=1\in\mathcal{G}(k/Q_2)$ if and only if $-1\in N_{k/Q_2}(k^*)$, where N_{k/Q_2} is the norm of k over Q_2. Hence if $\iota\in\mathcal{G}(L/k)$ then $-1\in N_{k/Q_2}(k^*)$. Conversely, if $-1\in N_{k/Q_2}(k^*)$ then $\iota_{c,s}\in\mathcal{G}(L_{c,s}/k)$ for any c and s such that $L_{c,s}\supset k$. Thus Theorem 1′ is equivalent to the following, as is noted by F. Lorenz.

THEOREM 1″. *Let k be a cyclotomic extension of Q_2. Let N_{k/Q_2} be the norm of k over Q_2. If $-1\in N_{k/Q_2}(k^*)$ then $S(k)$ is the subgroup of order 2 of $\mathrm{Br}(k)$. If $-1\notin N_{k/Q_2}(k^*)$ then $S(k)=1$.*

2. Formula of index.

Let B be a cyclotomic algebra over k:

$$B=(\alpha, k(\zeta)/k)=\sum_{\sigma\in\mathcal{G}} k(\zeta)u_\sigma\,, \qquad (u_1=1)\,,$$

$$u_\sigma x=\sigma(x)u_\sigma \quad (x\in k(\zeta))\,, \qquad u_\sigma u_\tau=\alpha(\sigma,\tau)u_{\sigma\tau} \quad (\sigma,\tau\in\mathcal{G})\,,$$

where ζ is a root of unity and $\mathcal{G}=\mathcal{G}(k(\zeta)/k)$. Let $\alpha(\sigma,\tau)=\beta(\sigma,\tau)\gamma(\sigma,\tau)$, $\beta(\sigma,\tau)\in\varepsilon_2(k(\zeta))$, $\gamma(\sigma,\tau)\in\varepsilon'(k(\zeta))$, $\sigma,\tau\in\mathcal{G}$. Then $B\sim(\beta, k(\zeta)/k)\otimes_k(\gamma, k(\zeta)/k)$. It is known by Witt [**5**] that $(\gamma, k(\zeta)/k)\sim k$ (see also [**9**, Proposition 5.1]), so $B\sim(\beta, k(\zeta)/k)$. Let K be the minimal cyclotomic field containing $k(\zeta)$. Then $K=Q_2(\zeta_{2^n},\zeta_{2^r-1})$ for some integers n and r. If $n\leqq 1$, then K/Q_2 is unramified, a fortiori, $k(\zeta)/k$ is unramified, so $(\beta, k(\zeta)/k)\sim k$. Hence we assume $n\geqq 2$.

Let $\sigma_i'\in\mathcal{G}(K/k)$ and $\sigma_i=\sigma_i'|k(\zeta)$, $(i=1, 2)$. Define $\beta_0(\sigma_1',\sigma_2')=\beta(\sigma_1,\sigma_2)\in\langle\zeta_{2^n}\rangle$. Then β_0 is a factor set of K/k and $(\beta, k(\zeta)/k)\sim(\beta_0, K/k)$. In fact, if β is regarded as an element of the cohomology group $H^2(k(\zeta)/k)=H^2(\mathcal{G}(k(\zeta)/k), k(\zeta)^*)$, β_0 is the image of the inflation map $\mathrm{Inf}: H^2(k(\zeta)/k)\to H^2(K/k)$. Hereafter, we simply write $\beta_0=\mathrm{Inf}\,\beta$.

We know that

$$\mathcal{G}(K/Q_2)=\langle\iota_0\rangle\times\langle\theta_0\rangle\times\langle\xi\rangle\,,$$

$$\iota_0(\zeta_{2^n})=\zeta_{2^n}^{-1},\quad \theta_0(\zeta_{2^n})=\zeta_{2^n}^5,\quad \iota_0(\zeta_{2^r-1})=\theta_0(\zeta_{2^r-1})=\zeta_{2^r-1}\,,$$

$$\xi(\zeta_{2^r-1})=\zeta_{2^r-1}^2,\quad \xi(\zeta_{2^n})=\zeta_{2^n}\,.$$

(If $n=2$ then $\theta_0=1$. If $r=1$ then $\xi=1$.) The Galois group $\mathcal{G}(K/k)$ is a subgroup of $\mathcal{G}(K/Q_2)$. The inertia group $\mathcal{T}(K/Q_2)=\langle\iota_0\rangle\times\langle\theta_0\rangle$ and $\mathcal{T}(K/k)=(\langle\iota_0\rangle\times\langle\theta_0\rangle)\cap\mathcal{G}(K/k)$. It follows from Theorem 1′ that if $\iota_0\notin\mathcal{G}(K/k)$ then $(\beta, k(\zeta)/k)\sim(\mathrm{Inf}\,\beta, K/k)\sim k$. Hence we may assume that $\mathcal{T}(K/k)=\langle\iota_0\rangle\times\langle\theta_0^{2^\lambda}\rangle$ for some integer λ $(0\leqq\lambda\leqq n-2)$, so $\zeta_4\notin k$. If the order of ζ is not divisible by 4, then $k(\zeta)/k$ is unramified, and $(\beta, k(\zeta)/k)\sim k$. So we assume $\zeta_4\in k(\zeta)$.

Let f be the residue class degree of k/Q_2. Then a Frobenius automorphism η' of K/k is of the form $\iota_0^\nu\theta_0^\mu\xi^f$ for some integers ν, μ such that $\nu=0, 1$ and $0\leqq\mu<2^{n-2}$. Since $\iota_0\eta'$ is also a Frobenius automorphism of K/k, we may assume $\eta'=\theta_0^\mu\xi^f$. The residue class degree of K/k is r/f and $|\xi|=r$. So $\mathcal{T}(K/k)\ni(\eta')^{r/f}=\theta_0^{\mu r/f}\xi^{fr/f}=\theta_0^{\mu r/f}$. Since $\mathcal{T}(K/k)=\langle\iota_0\rangle\times\langle\theta_0^{2^\lambda}\rangle$, then $2^\lambda|(\mu r/f)$. Put $\iota=\iota_0|k(\zeta)$, $\tau=\theta_0^{2^\lambda}|k(\zeta)$ and $\eta=\eta'|k(\zeta)$. Then $\mathcal{T}(k(\zeta)/k)=\langle\iota\rangle\times\langle\tau\rangle$ and η is a Frobenius automorphism of $k(\zeta)/k$. So $\mathcal{G}(k(\zeta)/k)=(\langle\iota\rangle\times\langle\tau\rangle)\cdot\langle\eta\rangle$.

LEMMA 4. *Notation and assumption being as above,* $\varepsilon_2(k(\zeta))=\varepsilon_2(K)=\langle\zeta_{2^n}\rangle$.

PROOF. Let F be the maximal unramified extension of $k(\zeta)$ in K. Since K is the minimal cyclotomic field containing $k(\zeta)$ and $\zeta_4\in k(\zeta)$, then Lemmas 1 and 2 imply that $K=F(\zeta_4)=F$, so $K/k(\zeta)$ is unramified. Consequently, $e(k(\zeta)/k)=e(K/k)=2^{n-\lambda-1}$, and $\mathcal{T}(K/k)=\langle\iota_0\rangle\times\langle\theta_0^{2^\lambda}\rangle$ is canonically isomorphic to $\mathcal{T}(k(\zeta)/k)=\langle\iota\rangle\times\langle\tau\rangle$. In particular, $|\tau|=|\theta_0^{2^\lambda}|=2^{n-2-\lambda}$. Let $\varepsilon_2(k(\zeta))=\langle\zeta_{2^m}\rangle$ and $\varepsilon'(k(\zeta))=\langle\zeta_t\rangle$. Then $2\leqq m\leqq n$, $k(\zeta)=k(\zeta_{2^m}, \zeta_t)$, t divides 2^r-1. Now $\tau(\zeta_{2^m})=\theta_0^{2^\lambda}(\zeta_{2^m})=\zeta_{2^m}^{5^{2^\lambda}}$, $\tau(\zeta_t)=\theta_0^{2^\lambda}(\zeta_t)=\zeta_t$. So $|\tau|=2^{m-2-\lambda}$. Thus $n=m$, proving the lemma.

We recall that

$$\iota(\zeta_{2^n})=\zeta_{2^n}^{-1}, \qquad \tau(\zeta_{2^n})=\zeta_{2^n}^{5^{2^\lambda}}, \qquad \eta(\zeta_{2^n})=\zeta_{2^n}^{5^\mu},$$

and for any $\sigma, \tau\in\mathcal{G}(k(\zeta)/k)$, $\beta(\sigma, \tau)\in\langle\zeta_{2^n}\rangle=\varepsilon_2(k(\zeta))=\varepsilon_2(K)$. Since $\beta(\iota, \iota)=u_\iota^2=u_\iota u_\iota^2 u_\iota^{-1}=\iota(\beta(\iota, \iota))$, it follows that $\beta(\iota, \iota)=\pm 1$. Let

$$\beta(\tau, \eta)/\beta(\eta, \tau)=\zeta_{2^n}^a, \qquad \beta(\iota, \eta)/\beta(\eta, \iota)=\zeta_{2^n}^b,$$

$$\beta(\tau, \iota)/\beta(\iota, \tau)=\zeta_{2^n}^c, \qquad \beta(\iota, \iota)=(-1)^d.$$

We shall see that the integers a, b, c and d determine the Hasse invariant of the cyclotomic algebra $B\sim(\beta, k(\zeta)/k)$.

Let ρ denote a primitive $2^{n+\lambda+2}$-th root of unity $\zeta_{2^{n+\lambda+2}}$ and put $L=Q_2(\rho, \zeta_{2^s-1})\supset K\supset k(\zeta)\supset k\supset Q_2$, where $s=2^n r$. We have $\mathcal{G}(L/Q_2)=\langle\iota_1\rangle\times\langle\theta_1\rangle\times\langle\xi_1\rangle$,

$$\iota_1(\rho)=\rho^{-1}, \quad \theta_1(\rho)=\rho^5, \quad \iota_1(\zeta_{2^s-1})=\theta_1(\zeta_{2^s-1})=\zeta_{2^s-1},$$

$$\xi_1(\zeta_{2^s-1})=\zeta_{2^s-1}^2, \quad \xi_1(\rho)=\rho\,.$$

Then $\iota_1|K=\iota_0$, $\theta_1|K=\theta_0$, $\xi_1|K=\xi$, so $\iota_1|k(\zeta)=\iota$, $\theta_1^{2^\lambda}|k(\zeta)=\tau$, $\theta_1^\mu\xi_1^f|k(\zeta)=\eta$. For simplicity, put $\omega=\theta_1^{2^\lambda}$, $\phi=\theta_1^\mu\xi_1^f$. Then $\omega, \phi\in\mathcal{G}(L/k)$, and ϕ is a Frobenius automorphism of L/k. We have $\omega(\rho)=\rho^{5^{2^\lambda}}$, $\phi(\rho)=\rho^{5^\mu}$. Since $e(L/k)=e(L/Q_2)/e(k/Q_2)=2^{n+1}$, then $\mathcal{T}(L/k)=\langle\iota_1\rangle\times\langle\omega\rangle$. Recall that 2^λ divides $\mu r/f$.

We have

$$\phi^{s/f}=\theta_1^{\mu s/f}\xi_1^{fs/f}=\theta_1^{2^n\mu r/f}=1\,,$$

because $|\theta_1|=2^{n+\lambda}$. Thus the order of the Frobenius automorphism ϕ of L/k is equal to the residue class degree s/f of L/k. This implies that

$$\mathcal{G}(L/k)=\langle\iota_1\rangle\times\langle\omega\rangle\times\langle\phi\rangle\,.$$

For simplicity, put $z=s/f$.

Let Inf denote the inflation map from $H^2(k(\zeta)/k)$ into $H^2(L/k)$, and put $\beta'=\mathrm{Inf}\,\beta$. Then $B\sim(\beta,\,k(\zeta)/k)\sim(\beta',\,L/k)$. We have

$$(\beta',\,L/k)=\sum_{\sigma\in\mathcal{G}(L/k)}Lv_\sigma=\sum_{i=0}^{1}\sum_{j=0}^{2^n-1}\sum_{l=0}^{z-1}Lv_{\iota_1}^iv_\omega^jv_\phi^l\,,$$

$$v_\omega v_\phi=(\beta'(\omega,\,\phi)/\beta'(\phi,\,\omega))v_\phi v_\omega=\zeta_{2^n}^a v_\phi v_\omega\,,$$

$$v_{\iota_1}v_\phi=(\beta'(\iota_1,\,\phi)/\beta'(\phi,\,\iota_1))v_\phi v_{\iota_1}=\zeta_{2^n}^b v_\phi v_{\iota_1}\,,$$

$$v_\omega v_{\iota_1}=(\beta'(\omega,\,\iota_1)/\beta'(\iota_1,\,\omega))v_{\iota_1}v_\omega=\zeta_{2^n}^c v_{\iota_1}v_\omega\,,$$

$$v_{\iota_1}^2=\beta'(\iota_1,\,\iota_1)=(-1)^d\,.$$

In the above, we recall that $\beta'(\omega,\,\phi)/\beta'(\phi,\,\omega)=\beta(\tau,\,\eta)/\beta(\eta,\,\tau)=\zeta_{2^n}^a$, etc.

Let L' and L'' be the fixed fields of the subgroups $\langle\omega\rangle$ and $\langle\iota_1\rangle\times\langle\phi\rangle$ of $\mathcal{G}(L/k)$, respectively, in the sense of Galois theory. Then $L=L'L''$ and $L'\cap L''=k$. We identify $\mathcal{G}(L'/k)$ with $\langle\iota_1\rangle\times\langle\phi\rangle$, and $\mathcal{G}(L''/k)$ with $\langle\omega\rangle$. Since $5^{2^\lambda}\equiv1$ (mod $2^{\lambda+2}$), $5^{2^\lambda}\not\equiv1$ (mod $2^{\lambda+3}$), we choose a primitive $2^{n+\lambda+2}$-th (resp. 2^n-th) root of unity $\rho=\zeta_{2^{n+\lambda+2}}$ (resp. ζ_{2^n}) such that $\zeta_{2^n}=\rho^{5^{2^\lambda}-1}$. Then, $\rho^{5^{2^\lambda}}=\rho\cdot\zeta_{2^n}$. We have

$$v_\omega(\rho^{-c}v_{\iota_1})=\rho^{-c5^{2^\lambda}}v_\omega v_{\iota_1}=\rho^{-c5^{2^\lambda}}\zeta_{2^n}^c v_{\iota_1}v_\omega=(\rho^{-c}v_{\iota_1})v_\omega\,,$$

$$v_\omega(\rho^{-a}v_\phi)=\rho^{-a5^{2^\lambda}}v_\omega v_\phi=\rho^{-a5^{2^\lambda}}\zeta_{2^n}^a v_\phi v_\omega=(\rho^{-a}v_\phi)v_\omega\,.$$

Note that v_ω commutes with each element of L'. Also, $\rho^{-c}v_{\iota_1}$ and $\rho^{-a}v_\phi$ commute with each element of L''. Thus we have

$$\begin{aligned}(\beta',\,L/k)&=\sum_{j=0}^{2^n-1}\sum_{i=0}^{1}\sum_{l=0}^{z-1}L''L'v_\omega^j(\rho^{-c}v_{\iota_1})^i(\rho^{-a}v_\phi)^l\\&=\Big[\sum_{j=0}^{2^n-1}L''v_\omega^j\Big]\cdot\Big[\sum_{i=0}^{1}\sum_{l=0}^{z-1}L'(\rho^{-c}v_{\iota_1})^i(\rho^{-a}v_\phi)^l\Big]\\&\cong(v_\omega^{2^n},\,L''/k,\,\omega)\otimes_k\Big[\sum_{i=0}^{1}\sum_{l=0}^{z-1}L'(\rho^{-c}v_{\iota_1})^i(\rho^{-a}v_\phi)^l\Big]\,,\end{aligned}$$

$$v_\omega^{2^n}=\beta'(\omega,\,\omega)\beta'(\omega^2,\,\omega)\cdots\beta'(\omega^{2^n-1},\,\omega)\in\langle\zeta_{2^n}\rangle\cap k=\{\pm1\}\,,$$

because $\zeta_4\notin k$.

Denote by C the above cyclic algebra $(v_\omega^{2^n}, L''/k, \omega)$. We will show $C\sim k$. If $v_\omega^{2^n}=1$, then $C\sim k$. Suppose that $v_\omega^{2^n}=-1$. The index of the cyclic algebra $(-1, L''/k, \omega)$ is the order of the norm residue symbol $(-1, L''/k)\in\mathcal{G}(L''/k)$. If $[k:Q_2]$ is divisible by 2, then $(-1, L''/k)=(N_{k/Q_2}(-1), L''/Q_2)=(1, L''/Q_2)=1\in\mathcal{G}(L''/Q_2)$, and so $C\sim k$. If $[k:Q_2]$ is not divisible by 2, then k/Q_2 is unramified and hence $\mathcal{G}(L/k)=\langle\theta_1\rangle\times\langle\iota_1\rangle\times\langle\phi\rangle$, $(\lambda=0, \omega=\theta_1)$. Consequently, $\xi_1^f=\phi\theta_1^{-\mu}$ is also a Frobenius automorphism of L/k, and so we may assume $\phi=\xi_1^f$. Then $L''=k\cdot k_0$, $k_0=Q_2(\zeta_{2^n}+\zeta_{2^n}^{-1})$, $k\cap k_0=Q_2$, $\langle\theta_1\rangle\cong\mathcal{G}(L''/k)\cong\mathcal{G}(k_0/Q_2)$. Hence we have

$$(-1, L''/k, \theta_1)\cong(-1, k_0/Q_2, \theta_1)\otimes_{Q_2}k\,.$$

The index of the cyclic algebra $(-1, k_0/Q_2, \theta_1)$ is equal to the order of the norm residue symbol $(-1, k_0/Q_2)$. But k_0 is the fixed field of the norm residue symbol $(-1, Q_2(\zeta_{2^n})/Q_2)\in\mathcal{G}(Q_2(\zeta_{2^n})/Q_2)$, and so $(-1, k_0/Q_2)=(-1, Q_2(\zeta_{2^n})/Q_2)|k_0=1\in\mathcal{G}(k_0/Q_2)$. This implies $(-1, k_0/Q_2, \theta_1)\sim Q_2$, and $(-1, L''/k, \theta_1)\sim k$. Thus

$$B\sim(\beta', L/k)\sim\sum_{i=0}^{1}\sum_{l=0}^{z-1}L'(\rho^{-c}v_{\iota_1})^i(\rho^{-a}v_\phi)^l\,.$$

We have

$$\begin{aligned}(\rho^{-c}v_{\iota_1})(\rho^{-a}v_\phi)&=\rho^{-c+a}v_{\iota_1}v_\phi=\rho^{-c+a}\zeta_{2^n}^b v_\phi v_{\iota_1}\\&=\rho^{-c+a+(5^{2^\lambda}-1)b}v_\phi v_{\iota_1}=\rho^{-c+a+(5^{2^\lambda}-1)b}v_\phi\rho^c\rho^{-c}v_{\iota_1}\\&=\rho^{2a+(5^{2^\lambda}-1)b+(5^\mu-1)c}(\rho^{-a}v_\phi)(\rho^{-c}v_{\iota_1})\,.\end{aligned}$$

Put

$$h'=2a+(5^{2^\lambda}-1)b+(5^\mu-1)c\,,\quad w_{\iota_1}=\rho^{-c}v_{\iota_1}\,,\quad w_\phi=\rho^{-a}v_\phi\,.$$

Then $w_{\iota_1}w_\phi=\rho^{h'}w_\phi w_{\iota_1}$ and so $\rho^{h'}=w_{\iota_1}w_\phi w_{\iota_1}^{-1}w_\phi^{-1}$. Since v_ω commutes with w_{ι_1} and w_ϕ, it follows that $v_\omega\rho^{h'}v_\omega^{-1}=\rho^{h'}$ and

$$\rho^{h'(5^{2^\lambda}-1)}=\omega(\rho^{h'})\rho^{-h'}=v_\omega\rho^{h'}v_\omega^{-1}\cdot\rho^{-h'}=\rho^{h'}\rho^{-h'}=1\,.$$

Therefore, h' is divisible by 2^n. Put $h=h'/2^n$. ρ^{2^n} is a primitive $2^{\lambda+2}$-th root of unity, so write $\zeta_{2^{\lambda+2}}=\rho^{2^n}$. Then $\rho^{h'}=\rho^{2^n\cdot h'/2^n}=(\zeta_{2^{\lambda+2}})^h$. Set $y_\phi=(1+\zeta_{2^{\lambda+2}})^h w_\phi$. It follows that

$$w_{\iota_1}y_\phi=(1+\zeta_{2^{\lambda+2}}^{-1})^h\zeta_{2^{\lambda+2}}^h w_\phi w_{\iota_1}=(1+\zeta_{2^{\lambda+2}})^h w_\phi w_{\iota_1}=y_\phi w_{\iota_1}\,.$$

Let E (resp. F) denote the fixed field of $\langle\iota_1\rangle$ (resp. $\langle\phi\rangle$) in L'/k. Then $L'=E\cdot F$, $E\cap F=k$, $\mathcal{G}(E/k)\cong\langle\phi\rangle$, and $\mathcal{G}(F/k)\cong\langle\iota_1\rangle$. We have

$$\begin{aligned}B&\sim\sum_{i=0}^{1}\sum_{l=0}^{z-1}L'w_{\iota_1}^i w_\phi^l=\sum_{i=0}^{1}\sum_{l=0}^{z-1}E\cdot Fw_{\iota_1}^i y_\phi^l\\&=[\sum_{i=0}^{1}Fw_{\iota_1}^i]\cdot[\sum_{l=0}^{z-1}Ey_\phi^l]\cong(w_{\iota_1}^2, F/k, \iota_1)\otimes_k(y_\phi^z, E/k, \phi)\,,\end{aligned}$$

$$w_{\iota_1}^2=(\rho^{-c}v_{\iota_1})^2=\rho^{-c}v_{\iota_1}\rho^{-c}v_{\iota_1}=\rho^{-c+c}v_{\iota_1}^2=\beta'(\iota_1, \iota_1)$$
$$=\beta(\iota, \iota)=(-1)^d,$$
$$y_\phi^z=\{(1+\zeta_{2^{\lambda+2}})^h w_\phi\}^z=[\prod_{l=0}^{z-1}\{1+\phi^l(\zeta_{2^{\lambda+2}})\}^h]\cdot w_\phi^z,$$
$$w_\phi^z=(\rho^{-a}v_\phi)^z=\{\prod_{l=0}^{z-1}\phi^l(\rho^{-a})\}\beta'(\phi, \phi)\beta'(\phi^2, \phi)\cdots\beta'(\phi^{z-1}, \phi).$$

For a finite extension Ω of Q_2, V_Ω denotes the normalized discrete valuation of Ω. That is, if π is a prime element of Ω, then $V_\Omega(\pi)=1$. The elements

$$1+\phi^l(\zeta_{2^{\lambda+2}}) \qquad (l=0, 1, \cdots, z-1)$$

are prime elements of $Q_2(\zeta_{2^{\lambda+2}})$, and w_ϕ^z is a root of unity contained in L. Since $e(L/k)=2^{n+1}$ and $e(L/Q_2(\zeta_{2^{\lambda+2}}))=2^n$, it follows that

$$2^{n+1}\cdot V_k(y_\phi^z)=V_L(y_\phi^z)=V_L(\prod_{l=0}^{z-1}(1+\phi^l(\zeta_{2^{\lambda+2}}))^h)$$
$$=\sum_{l=0}^{z-1}h\cdot V_L(1+\phi^l(\zeta_{2^{\lambda+2}}))=\sum_{l=0}^{z-1}h\cdot 2^n V_{Q_2(\zeta_{2^{\lambda+2}})}(1+\phi^l(\zeta_{2^{\lambda+2}}))=2^n hz,$$

and consequently, $V_k(y_\phi^z)=hz/2$. Because E/k is an unramified extension of degree z, it follows from the definition of Hasse invariant that the Hasse invariant of the cyclic algebra $(y_\phi^z, E/k, \phi)$ is:

$$\mathrm{inv}(y_\phi^z, E/k, \phi)=V_k(y_\phi^z)/z=h/2.$$

Next consider the cyclic algebra $(-1, F/k, \iota_1)$, whose index is equal to the order of the norm residue symbol $(-1, F/k)=(N_{k/Q_2}(-1), F/Q_2)$. If $2|[k:Q_2]$, then $N_{k/Q_2}(-1)=1$, so $(-1, F/k, \iota_1)\sim k$. It is easy to see that if $2\nmid[k:Q_2]$, then k/Q_2 is unramified, $F=k(\zeta_4)$, and $N_{k/Q_2}(-1)=-1$. But there is no element $\delta\in F$ such that $N_{F/Q_2}(\delta)=-1$, because there is no element $\delta'\in Q_2(\zeta_4)\subset F=k(\zeta_4)$ such that $N_{Q_2(\zeta_4)/Q_2}(\delta')=-1$. Hence the order of the norm residue symbol $(-1, F/Q_2)$ equals 2. Consequently, we have

$$\mathrm{inv}(w_{\iota_1}^2, F/k, \iota_1)=\begin{cases}\dfrac{1}{2}, & \text{if } 2\nmid[k:Q_2] \text{ and } \beta(\iota, \iota)=-1,\\ 0, & \text{otherwise.}\end{cases}$$

Thus we have proved the following theorem.

THEOREM 2. *Let k be a cyclotomic extension of the 2-adic numbers Q_2. Let $B=(\alpha, k(\zeta)/k)$ be a cyclotomic algebra over k. Let $\varepsilon_2(k(\zeta))=\langle\zeta_{2^n}\rangle$, $\varepsilon'(k(\zeta))=\langle\zeta_t\rangle$, so $k(\zeta)=k(\zeta_{2^n}, \zeta_t)$. For $\sigma, \sigma'\in\mathfrak{G}(k(\zeta)/k)$, let $\alpha(\sigma, \sigma')=\beta(\sigma, \sigma')\gamma(\sigma, \sigma')$, $\beta(\sigma, \sigma')\in\langle\zeta_{2^n}\rangle$, $\gamma(\sigma, \sigma')\in\langle\zeta_t\rangle$. Then $B\sim(\beta, k(\zeta)/k)$. If $n<2$, then $B\sim k$. Assume that $n\geqq 2$. If the inertia group $\mathfrak{T}$ of $k(\zeta)/k$ does not contain an automorphism ι such that $\iota(\zeta_{2^n})=\zeta_{2^n}^{-1}$, $\iota(\zeta_t)=\zeta_t$, then $B\sim k$. Suppose that $\iota\in\mathfrak{T}$. Then $\mathfrak{T}$ is of the form:*

$\mathcal{G}=\langle\iota\rangle\times\langle\tau\rangle$, *where* $\tau(\zeta_{2^n})=\zeta_{2^n}^{5^{2^\lambda}}$ $(0\leqq\lambda\leqq n-2)$, $\tau(\zeta_t)=\zeta_t$. *(If* $\lambda=n-2$, $\tau=1$.) *There exists a Frobenius automorphism* η *of* $k(\zeta)/k$ *such that* $\eta(\zeta_{2^n})=\zeta_{2^n}^{5^\mu}$ *for some integer* μ $(0\leqq\mu<2^{n-2})$. *Let*

$$\beta(\tau,\eta)/\beta(\eta,\tau)=\zeta_{2^n}^a, \qquad \beta(\iota,\eta)/\beta(\eta,\iota)=\zeta_{2^n}^b,$$

$$\beta(\tau,\iota)/\beta(\iota,\tau)=\zeta_{2^n}^c, \qquad \beta(\iota,\iota)=(-1)^d,$$

$$h=\{2a+(5^{2^\lambda}-1)b+(5^\mu-1)c\}/2^n.$$

Then h *is an integer and the Hasse invariant of* B *is:*

$$\operatorname{inv}B\equiv\frac{h}{2}+[k:Q_2]2^{(-1)^d} \qquad (\mathrm{mod}\ 1).$$

So the index of B *is* 1 *and* 2 *if the right side is congruent to* 0 *and* 1/2 (mod 1), *respectively.*

When K is a field which is not necessarily cyclotomic, we have

THEOREM 3. *Let* K *be a finite extension of* Q_2 *and let* $B=(\alpha, K(\zeta)/K)$ *be a cyclotomic algebra over* K, *where* ζ *is a root of unity. If the group of roots of unity in* $K(\zeta)$ *is generated by* ζ', *then* $K(\zeta)=K(\zeta')$ *and the values of* α *belong to* $\langle\zeta'\rangle$. *Let* k *denote the maximal cyclotomic extension of* Q_2 *contained in* K. *Then* $\mathcal{G}(K(\zeta)/K)\cong\mathcal{G}(k(\zeta')/k)$ *and* $B\cong(\alpha, k(\zeta')/k)\otimes_k K$. *So* $\operatorname{inv}B=[K:k]\cdot\operatorname{inv}(\alpha, k(\zeta')/k)$, *and* $\operatorname{inv}(\alpha, k(\zeta')/k)$ *is given by Theorem* 2.

PROOF. Put $F=k(\zeta')\cap K$. Then F is a cyclotomic extension of Q_2 contained in K. Hence $F=k$ and $\mathcal{G}(k(\zeta')/k)\cong\mathcal{G}(K(\zeta)/K)$. The rest of the assertions follows immediately.

References

[1] R. Brauer, Representations of groups of finite order, Proc. Int. Cong. Math., **2** (1950), 33-36.

[2] R. Brauer, On the algebraic structure of group rings, J. Math. Soc. Japan, **3** (1951), 237-251.

[3] G.J. Janusz, The Schur group of an algebraic number field, Ann. of Math., **103** (1976), 253-281.

[4] S. Lang, Algebraic Number Theory, Addison-Wesley, Reading, Mass., 1970.

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

[6] 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.

[7] T. Yamada, The Schur subgroup of a 2-adic field, J. Math. Soc. Japan, **26** (1974), 168-179.

[8] T. Yamada, The Schur subgroup of a p-adic field, J. Algebra, **31** (1974), 480-498.

[9] T. Yamada, The Schur Subgroup of the Brauer Group, Lecture Notes in Mathe-

matics, Springer, Berlin-Heidelberg-New York, 1974.
[10] T. Yamada, More on the Schur index and the order and exponent of a finite group, Tokyo J. Math., 1 (1978), 269-273.

Toshihiko YAMADA
Department of Mathematics
Science University of Tokyo
Wakamiya 26, Shinjuku-ku
Tokyo 162, Japan