J. Math. Soc. Japan
Vol. 23, No. 2, 1971

Characterization of the simple components of the group algebras over the p-adic number field

By Toshihiko YAMADA[1)]

(Received April 27, 1970)

§ 1. Introduction.

Let G be a finite group and K a field of characteristic 0. Then the group algebra $K[G]$ of G with respect to K is semisimple. We can write it as a direct sum

$$K[G] = A_1 \oplus A_2 \oplus \cdots \oplus A_r$$

of simple algebras. Each A_i is in one-to-one correspondence with a family T_i of absolutely irreducible characters $\chi_{i\nu}(\nu = 1, \cdots, t_i)$ of G, taken in the algebraic closure $\bar{K}$ of K and algebraically conjugate to each other over K. Each simple algebra A_i is isomorphic to a complete matrix algebra $M_{\rho_i}(\Delta_i)$ of a certain degree ρ_i with coefficients in a division algebra Δ_i over K. Let $K(\chi_{i\nu})$ denote the field obtained from K by adjoining all values $\chi_{i\nu}(g)$ with $g \in G$ of the character $\chi_{i\nu}$. It turns out that the center Ω_i of Δ_i is isomorphic to $K(\chi_{i\nu})$ for $\chi_{i\nu} \in T_i$. If the dimension of Δ_i over Ω_i is m_i^2, m_i is called the Schur index of the division algebra Δ_i or of the characters $\chi_{i\nu}$ $(\nu = 1, \cdots, t_i)$.

Now we are faced with the problem: Characterize division algebras which appear at simple components of group algebras.

In this paper this problem is solved for division algebras over the p-adic number field $\boldsymbol{Q}_p$, where p is any odd prime number. Namely, we shall prove the following

THEOREM 1. *Let p be an odd prime number. Denote by Ξ the field obtained from $\boldsymbol{Q}_p$ by adjoining all primitive roots of unity ζ_n $(n = 3, 4, 5, \cdots)$. Then, a given (finite dimensional) division algebra Δ over $\boldsymbol{Q}_p$ appears at a simple component of the group algebra $\boldsymbol{Q}_p[G]$ over $\boldsymbol{Q}_p$ of a certain finite group G if and only if* (i) *the center k of Δ is a finite extension field of $\boldsymbol{Q}_p$ contained in Ξ, and* (ii) *the Hasse invariant of Δ is of the form*

$$z/\frac{p-1}{b} \pmod{\boldsymbol{Z}}, \qquad z \in \boldsymbol{Z},$$

where $\boldsymbol{Z}$ is the ring of rational integers and b is the index of tame ramification

1) This work was supported in part by The Sakkokai Foundation.

of the extension $k/\boldsymbol{Q}_p$, i.e., if $\mathfrak{p}$ is the prime ideal of the integer ring in k dividing p, the ramification index of $\mathfrak{p}$ over p is bp^{λ}, $(b, p)=1$, for a certain integer λ.

REMARK. In the above, k is contained in a cyclotomic field $\boldsymbol{Q}_p(\zeta_n)$ for a certain positive integer n, and so b divides $p-1$.

From Theorem 1, we can immediately deduce many facts about irreducible characters or group algebras of finite groups. We state a few of them and use the same notation as in Theorem 1.

Let χ be an absolutely irreducible character of a finite group G, and let b be the index of tame ramification of the extension $\boldsymbol{Q}_p(\chi)/\boldsymbol{Q}_p$. Then the Schur index of χ with respect to $\boldsymbol{Q}_p$ divides $(p-1)/b$. If B is the simple component of the group algebra $\boldsymbol{Q}[G]$ of G over the rational number field $\boldsymbol{Q}$ which corresponds to the character χ, then the center of B is isomorphic to $\boldsymbol{Q}(\chi)$ and the Hasse invariant of B at any prime ideal $\mathfrak{p}$ of $\boldsymbol{Q}(\chi)$ dividing p is of the form $z/\frac{p-1}{b} \pmod{\boldsymbol{Z}}$, $z \in \boldsymbol{Z}$.

Let K be a finite extension field of $\boldsymbol{Q}_p$ and let $Br(K)$ denote the set of all classes of central simple algebras over K, i.e., the Brauer group of K. Let $k=K \cap \boldsymbol{\Xi}$ and b be the index of tame ramification of $k/\boldsymbol{Q}_p$ (at p). Set $s=\left(\frac{p-1}{b}, [K: k]\right)$. Denote by $S(K)$ the subset of $Br(K)$ consisting of all those classes that contain simple components of group algebras $K[G]$ over K of finite groups G. Then we have

THEOREM 2. *$S(K)$ is the finite subgroup of $Br(K)$ of order $\frac{p-1}{bs}$.*

Here we make a remark about the proof of Theorem 1. E. Witt [11] has reduced the question of determining Schur indices of irreducible characters to that of determining indices of 'Kreisalgebren'. Then he noticed that by means of the transfer map in the theory of cohomology, the center of any Kreisalgebra may be assumed to be $\boldsymbol{Q}_p$, and he calculated the index of it. In this paper, we directly calculate the index of any Kreisalgebra $\mathfrak{A}$ whose center k is an extension of $\boldsymbol{Q}_p$. It follows that if the index of tame ramification of $k/\boldsymbol{Q}_p$ (at p) is b, then the index of $\mathfrak{A}$ divides $\frac{p-1}{b}$. From this fact we deduce the 'only if' part of Theorem 1. As for the 'if' part, we construct a simple algebra $\mathfrak{A}$ over $\boldsymbol{Q}_p$ such that (i) the center of $\mathfrak{A}$ is exactly the given field k, (ii) the index of $\mathfrak{A}$ is equal to a given value as in the condition of Theorem 1, (iii) there exists a finite subgroup G in $\mathfrak{A}$ which spans $\mathfrak{A}$ with respect to $\boldsymbol{Q}_p$, i.e., $\mathfrak{A}=\{\sum_{g \in G} \alpha_g g;\ \alpha_g \in \boldsymbol{Q}_p\}$. Such a G is given by a metabelian group.

NOTATION AND TERMINOLOGY. Every group G whose identity is denoted by 1 is assumed to be finite. By an irreducible character χ of G, we always

mean an absolutely irreducible one. For a field K of characteristic 0, $A(\chi, K)$ is the simple component of $K[G]$ that corresponds to χ. $K^\times$ is the multiplicative group of non-zero elements of K. If L is a normal extension of K, $\mathfrak{G}(L/K)$ is the Galois group of L over K. For any element α of L, the image of α by an automorphism $\tau \in \mathfrak{G}(L/K)$ is denoted by α^τ. If H is a subgroup of G and ψ a character of H, ψ^G is the character of G induced from ψ. For $\tau \in \mathfrak{G}(K(\psi)/K)$, ψ^τ is the character of H defined by $\psi^\tau(h) = (\psi(h))^\tau$, $h \in H$. If $G \triangleright H$, i.e., if H is a normal subgroup of G, then for each $g \in G$, ψ^g is the character of H defined by $\psi^g(h) = \psi(ghg^{-1})$, $h \in H$. $\langle g_1, g_2, \cdots \rangle$ is the group generated by $g_1, g_2, \cdots$. The greatest common divisor of integers n and n' is as usual denoted by (n, n'). For a positive integer n, ζ_n is a primitive n-th root of unity. Two simple algebras A and B are said to be similar, if and only if (i) the center of A and that of B are the same field k, and (ii) there exist matrix algebras $M_n(k)$ and $M_{n'}(k)$ such that $A \otimes_k M_n(k)$ and $B \otimes_k M_{n'}(k)$ are isomorphic.

§ 2. Preliminaries.

Let G be a finite group. The group algebra $\boldsymbol{Q}[G]$ of G over the rational number field $\boldsymbol{Q}$ is a direct sum of simple algebras A_i:

$$\boldsymbol{Q}[G] = A_1 \oplus \cdots \oplus A_r .$$

Let $\chi_1, \cdots, \chi_r$ be representatives of the algebraically conjugate classes (over $\boldsymbol{Q}$) of the absolutely irreducible characters of G. If A_i corresponds to χ_i $(i = 1, \cdots, r)$, the center of A_i is isomorphic to the field $\boldsymbol{Q}(\chi_i)$. Let K be any field of characteristic 0. Then we have

$$\begin{aligned} K[G] &\cong \boldsymbol{Q}[G] \otimes_{\boldsymbol{Q}} K \cong A_1 \otimes_{\boldsymbol{Q}} K \oplus \cdots \oplus A_r \otimes_{\boldsymbol{Q}} K , \\ A_i \otimes_{\boldsymbol{Q}} K &\cong (A_i \otimes_{\boldsymbol{Q}(\chi_i)} \boldsymbol{Q}(\chi_i)) \otimes_{\boldsymbol{Q}} K \cong A_i \otimes_{\boldsymbol{Q}(\chi_i)} (\boldsymbol{Q}(\chi_i) \otimes_{\boldsymbol{Q}} K) \\ &\cong A_i \otimes_{\boldsymbol{Q}(\chi_i)} K(\chi_i) \oplus \cdots \oplus A_i \otimes_{\boldsymbol{Q}(\chi_i)} K(\chi_i) , \end{aligned}$$

where the last summands correspond respectively to the algebraic conjugate characters χ_i^σ, $\sigma \in \mathfrak{G}(\boldsymbol{Q}(\chi_i) \cap K/\boldsymbol{Q})$. For an irreducible character χ of G, the above argument shows

$$A(\chi, K) \cong A(\chi, \boldsymbol{Q}) \otimes_{\boldsymbol{Q}(\chi)} K(\chi) .$$

If K is an algebraic number field of finite degree and $\mathfrak{P}$ (resp. $\mathfrak{p}$) is a prime ideal of $K(\chi)$ (resp. $\boldsymbol{Q}(\chi)$) such that $\mathfrak{P}$ divides $\mathfrak{p}$ and that $\mathfrak{p}$ divides a prime number p, then we have

$$\begin{aligned} A(\chi, K) \otimes_{K(\chi)} K(\chi)_{\mathfrak{P}} &\cong (A(\chi, \boldsymbol{Q}) \otimes_{\boldsymbol{Q}(\chi)} K(\chi)) \otimes_{K(\chi)} K(\chi)_{\mathfrak{P}} \\ &\cong A(\chi, \boldsymbol{Q}) \otimes_{\boldsymbol{Q}(\chi)} K(\chi)_{\mathfrak{P}} \\ &\cong A(\chi, \boldsymbol{Q}) \otimes_{\boldsymbol{Q}(\chi)} (\boldsymbol{Q}(\chi)_{\mathfrak{p}} \otimes_{\boldsymbol{Q}(\chi)_{\mathfrak{p}}} K(\chi)_{\mathfrak{P}}) \\ &\cong (A(\chi, \boldsymbol{Q}) \otimes_{\boldsymbol{Q}(\chi)} \boldsymbol{Q}(\chi)_{\mathfrak{p}}) \otimes_{\boldsymbol{Q}(\chi)_{\mathfrak{p}}} K(\chi)_{\mathfrak{P}} . \end{aligned}$$

Here, of course, $K(\chi)_{\mathfrak{P}}$ (resp. $\boldsymbol{Q}(\chi)_{\mathfrak{p}}$) denotes the completion of $K(\chi)$ (resp. $\boldsymbol{Q}(\chi)$) by the $\mathfrak{P}$-adic (resp. $\mathfrak{p}$-adic) topology. Therefore the Hasse invariant of the central simple algebra $A(\chi, K)$ over $K(\chi)$ at the prime ideal $\mathfrak{P}$ is equal to that of the central simple algebra $A(\chi, \boldsymbol{Q})$ over $\boldsymbol{Q}(\chi)$ at the $\mathfrak{p}$ multiplied by $[K(\chi)_{\mathfrak{P}} : \boldsymbol{Q}(\chi)_{\mathfrak{p}}]$. If $m(\chi, \boldsymbol{Q}, \mathfrak{p})$ is the $\mathfrak{p}$-index of the central simple algebra $A(\chi, \boldsymbol{Q})$ over $\boldsymbol{Q}(\chi)$, the $\mathfrak{P}$-index of $A(\chi, K)$ equals

$$\frac{m(\chi, \boldsymbol{Q}, \mathfrak{p})}{(m(\chi, \boldsymbol{Q}, \mathfrak{p}), [K(\chi)_{\mathfrak{P}} : \boldsymbol{Q}(\chi)_{\mathfrak{p}}])} .$$

Note that $m(\chi, \boldsymbol{Q}, \mathfrak{p})$ is equal to the index of the simple component $A(\chi, \boldsymbol{Q}_p)$ of $\boldsymbol{Q}_p[G]$ which corresponds to χ, because

$$A(\chi, \boldsymbol{Q}) \otimes_{\boldsymbol{Q}(\chi)} \boldsymbol{Q}(\chi)_{\mathfrak{p}} \cong A(\chi, \boldsymbol{Q}) \otimes_{\boldsymbol{Q}(\chi)} \boldsymbol{Q}_p(\chi) \cong A(\chi, \boldsymbol{Q}_p) .$$

If Ω is a finite extension field of $\boldsymbol{Q}_p$, the simple component $A(\chi, \Omega)$ of $\Omega[G]$ is:

$$\begin{aligned} A(\chi, \Omega) &\cong A(\chi, \boldsymbol{Q}) \otimes_{\boldsymbol{Q}(\chi)} \Omega(\chi) \\ &\cong (A(\chi, \boldsymbol{Q}) \otimes_{\boldsymbol{Q}(\chi)} \boldsymbol{Q}_p(\chi)) \otimes_{\boldsymbol{Q}_p(\chi)} \Omega(\chi) \\ &\cong A(\chi, \boldsymbol{Q}_p) \otimes_{\boldsymbol{Q}_p(\chi)} \Omega(\chi) . \end{aligned}$$

In order to determine the Schur index $m(\chi, \boldsymbol{Q}_p)$ of χ with respect to $\boldsymbol{Q}_p$ (i.e., the index of $A(\chi, \boldsymbol{Q}_p)$), it suffices to determine the l-part $m_l(\chi, \boldsymbol{Q}_p)$ of $m(\chi, \boldsymbol{Q}_p)$ for every prime number l. R. Brauer [2] and E. Witt [11] independently reduced this question to the corresponding question for hyperelementary subgroups at l of G. Here we call a group H a hyperelementary group at the prime l, if H is a semi-direct product $\langle a \rangle B$ of an l-group B and a cyclic normal subgroup $\langle a \rangle$ whose order is not a multiple of l.

THEOREM (Brauer-Witt). *If χ is an irreducible character of a group G, if K is a field of characteristic 0, then for every prime l there exist a hyperelementary subgroup at l and an irreducible character ξ of H such that the l-part of the Schur index of χ with respect to K is equal to the Schur index of ξ with respect to $K(\chi)$. If we take $K = \boldsymbol{Q}$ and determine the character ξ in this case, the same character ξ can be used for every field of characteristic 0.*

By this Theorem, the l-part m_l of the Schur index m of χ with respect to $\boldsymbol{Q}$ is equal to the Schur index of ξ with respect to $\boldsymbol{Q}(\chi)$, and for any prime number p, the l-part $m_l(\chi, \boldsymbol{Q}_p)$ of the index $m(\chi, \boldsymbol{Q}_p)$ of $A(\chi, \boldsymbol{Q}_p)$ is equal to the index of $A(\xi, \boldsymbol{Q}_p(\chi))$. The index of $A(\xi, \boldsymbol{Q}_p(\chi))$ is equal to

$$\frac{m(\xi, \boldsymbol{Q}_p)}{(m(\xi, \boldsymbol{Q}_p), [\boldsymbol{Q}_p(\xi, \chi) : \boldsymbol{Q}_p(\xi)])} ,$$

where $m(\xi, \boldsymbol{Q}_p)$ is the index of $A(\xi, \boldsymbol{Q}_p)$. As was mentioned before, the index $m(\xi, \boldsymbol{Q}_p)$ of $A(\xi, \boldsymbol{Q}_p)$ equals the $\mathfrak{p}$-index of $A(\xi, \boldsymbol{Q})$ for any $\mathfrak{p}$ of $\boldsymbol{Q}(\xi)$ that divides p. Therefore we simply need to compute the $\mathfrak{p}$-index of $A(\xi, \boldsymbol{Q})$ for

every prime ideal $\mathfrak{p}$ of $\boldsymbol{Q}(\xi)$.

R. Brauer [**1**] and E. Witt [**11**] independently reduced the question of the Schur indices of a hyperelementary group to the case of a group R which has a cyclic normal subgroup S such that R/S is an abelian group. Further, they determined the factor sets of the corresponding simple algebras of R. (R. Brauer did not publish the proof.) Here we shall give a simple proof of their results.

Let $H=\langle a\rangle B$ be a hyperelementary group at the prime l, where B is an l-Sylow subgroup of H and $\langle a\rangle$ is a normal subgroup of H whose order is relatively prime to l. Let ξ be an irreducible character of H. It is known that ξ is monomial and the degree of ξ is l-th power. For the proof of these facts, see, for instance, Feit [**6**, 10.2 and 9.13] or Huppert [**7**, 18.4 and 17.10]. We see easily that every subgroup N of H whose index $(H: N)$ is l-th power, necessarily contains the normal subgroup $\langle a\rangle$. Consequently, if ξ is induced from a linear character of a subgroup N of H, then N contains the normal subgroup $\langle a\rangle$.

PROPOSITION 1. *Let $H=\langle a\rangle B$ be a hyperelementary group (at l) and ξ an irreducible character of H. Then we are able to find subgroups F and N of H and a linear character ψ of N such that* (i) *ξ is induced from ψ, i.e., $\xi=\psi^H$,* (ii) *$F\rhd N\supset\langle a\rangle$,* (iii) *for every $f\in F$, the character ψ^f of N defined by $\psi^f(n)=\psi(fnf^{-1})$, $n\in N$, is an algebraic conjugate of ψ, i.e., $\psi^f=\psi^{\tau(f)}$ for some $\tau(f)\in\mathfrak{G}(\boldsymbol{Q}(\psi)/\boldsymbol{Q})$,* (iv) *$\boldsymbol{Q}(\psi^F)=\boldsymbol{Q}(\xi)$.*

PROOF.[2] Let T be a minimal normal subgroup of H such that i) there exists a character θ of T from which ξ is induced, ii) for each $h\in H$, $\theta^h=\theta^{\tau(h)}$ for some $\tau(h)\in\mathfrak{G}(\boldsymbol{Q}(\theta)/\boldsymbol{Q})$. Assume first that θ is a linear character of T. Then, by setting $F=H$, $T=N$ and $\psi=\theta$, all the conditions of Proposition 1 are satisfied. Assume next that θ is non-linear. We note that a subgroup of index l of a hyperelementary group (at l) is a normal subgroup. From the remarks before Proposition 1 it follows that T is a hyperelementary group (at l) containing the normal subgroup $\langle a\rangle$, and that there are a subgroup S of T and a character ρ of S such that $(T: S)=l$ and $\rho^T=\theta$. As S is normal in T and ρ induces θ, it follows that θ vanishes outside S. Let U be the intersection of all conjugates hSh^{-1} $(h\in H)$ of S in H. Since $\langle a\rangle\subset S$ and $\langle a\rangle\lhd H$, we have $\langle a\rangle\subset U$. Thus $U\lhd H$ and H/U is an l-group. Consequently there exists a normal subgroup Y of H such that $U\subset Y\subset T\subset H$ and $(T: Y)=l$. Since for every $h\in H$, θ^h is an algebraic conjugate of θ and θ vanishes outside S, it follows that θ vanishes outside U, a fortiori outside Y. From the equation

2) The following proof is substantially due to Solomon [**9**]. In Propositions 1-3, the same assertions hold true by replacing $\boldsymbol{Q}$ with any field K of characteristic 0.

$$\frac{1}{|Y|}\sum_{Y\supset y}\theta(y)\theta(y^{-1})=\frac{l}{|T|}\sum_{T\supset t}\theta(t)\theta(t^{-1})=l\,,$$

we see easily that there exists an irreducible character ϕ of Y such that

$$\theta\,|\,Y=\sum_{j=0}^{l-1}\phi^{x^j}$$

where $1, x, \cdots, x^{l-1}$ is a set of representatives for T mod Y and the characters ϕ^{x^j} of Y are distinct from each other. Namely the inertial group of ϕ is Y and the index of ramification of θ with respect to Y is equal to 1. Thus ϕ induces θ and so ϕ induces ξ, too. Let E be the subgroup of all $h\in H$ such that ϕ^h is algebraically conjugate to ϕ over $\boldsymbol{Q}$. By minimality of T, E is a proper subgroup of H which contains $\langle a\rangle$. From the same argument as in the proof of [**13**, Theorem 2] we conclude that $\boldsymbol{Q}(\phi^E)=\boldsymbol{Q}(\phi^H)=\boldsymbol{Q}(\xi)$. Thus we have proved that if θ is non-linear, there exist a proper subgroup $E(\supset\langle a\rangle)$ of H and a character $\eta(=\phi^E)$ of E such that η induces ξ and that $\boldsymbol{Q}(\eta)=\boldsymbol{Q}(\xi)$. Using these arguments successively, we are able to find subgroups F and N and a linear character ψ of N satisfying the conditions (i)—(iv) of Proposition 1.

In the next two propositions we use the same notation as in Proposition 1.

PROPOSITION 2. *If the simple component $A(\psi^F, \boldsymbol{Q})$ of $\boldsymbol{Q}[F]$ is isomorphic to $M_r(D)$ for a central division algebra D over $\boldsymbol{Q}(\psi^F)$, the simple component $A(\xi, \boldsymbol{Q})$ of $\boldsymbol{Q}[H]$ is isomorphic to $M_{rs}(D)$, where $s=(H\colon F)$.*

PROOF. This is an immediate consequence of [**13**, Theorem 1].

PROPOSITION 3. *Let $Nf_1, \cdots, Nf_t$ $(f_1=1)$ be all the distinct cosets of N in F and $f_if_j=n_{ij}f_{\nu(i,j)}$, $n_{ij}\in N$. Set $\tau(f_i)=\tau_i$ and $\beta(\tau_i, \tau_j)=\psi(n_{ij})$, $1\leqq i, j\leqq t$. Then we have* (i) *$F/N\cong\{\tau_1, \cdots, \tau_t\}\cong\mathfrak{G}(\boldsymbol{Q}(\psi)/\boldsymbol{Q}(\psi^F))$,* (ii) *$\beta$ is a factor set of the Galois group $\mathfrak{G}(\boldsymbol{Q}(\psi)/\boldsymbol{Q}(\psi^F))$ consisting of roots of unity,* (iii) *the simple algebra $A(\psi^F, \boldsymbol{Q})$ is isomorphic to the crossed product*

$$(\beta(\tau_i, \tau_j), \boldsymbol{Q}(\psi)/\boldsymbol{Q}(\psi^F))=\sum_{i=1}^{t}\boldsymbol{Q}(\psi)u_{\tau_i}\qquad\text{(direct sum)}$$

whose defining relations are $u_{\tau_i}u_{\tau_j}=\beta(\tau_i, \tau_j)u_{\tau_i\tau_j}$, $u_{\tau_i}xu_{\tau_i}^{-1}=x^{\tau_i}$, $x\in\boldsymbol{Q}(\psi)$.

PROOF. This follows at once from [**13**, Theorem 2].

Thus we only need to compute the $\mathfrak{p}$-index of the crossed product $(\beta(\tau_i, \tau_j), \boldsymbol{Q}(\psi)/\boldsymbol{Q}(\psi^F))$ at every prime ideal $\mathfrak{p}$ of $\boldsymbol{Q}(\psi^F)$. Note that $\boldsymbol{Q}(\psi)$ is a cyclotomic field because ψ is a linear character of N. Let $\mathfrak{P}$ be a prime ideal of $\boldsymbol{Q}(\psi)$ which divides $\mathfrak{p}$. Since $\boldsymbol{Q}(\psi)/\boldsymbol{Q}$ is abelian, we denote by $\mathfrak{G}_\mathfrak{p}$ the decomposition group of $\mathfrak{P}$ over $\mathfrak{p}$ and write $\boldsymbol{Q}(\psi)_\mathfrak{P}=\boldsymbol{Q}(\psi)^\mathfrak{p}$, so that $\mathfrak{G}_\mathfrak{p}=\mathfrak{G}(\boldsymbol{Q}(\psi)^\mathfrak{p}/\boldsymbol{Q}(\psi^F)_\mathfrak{p})$. Then

$$\begin{aligned}A(\psi^F, \boldsymbol{Q}_p)&\cong(\beta(\tau, \tau'), \boldsymbol{Q}(\psi)/\boldsymbol{Q}(\psi^F))\otimes_{\boldsymbol{Q}(\psi^F)}\boldsymbol{Q}(\psi^F)_\mathfrak{p}\\&\sim(\beta(\tau, \tau')_{\mathfrak{G}_\mathfrak{p}}, \boldsymbol{Q}(\psi)^\mathfrak{p}/\boldsymbol{Q}(\psi^F)_\mathfrak{p})\,,\qquad\mathfrak{p}\,|\,p\,,\end{aligned}$$

where $\beta(\tau, \tau')_{\mathfrak{G}_\mathfrak{p}}$ denotes the factor set of $\mathfrak{G}_\mathfrak{p}$ with $\tau, \tau' \in \mathfrak{G}_\mathfrak{p} \subset \mathfrak{G}(\boldsymbol{Q}(\psi)/\boldsymbol{Q}(\psi^F))$.

§ 3. The index of the Kreisalgebra.

Let us consider a $\mathfrak{p}$-adic 'Kreisalgebra'

$$\mathfrak{A} = (\beta(\sigma, \tau), K/k) = \sum_\sigma K u_\sigma$$

with the following properties:

i) K is a cyclotomic field $\boldsymbol{Q}_p(\zeta_n)$ over the p-adic number field $\boldsymbol{Q}_p$, where ζ_n is a primitive n-th root of unity for a natural number n,

ii) the subfield k of $K/\boldsymbol{Q}_p$ is the center of $\mathfrak{A}$ and $\mathfrak{p}$ is the prime ideal of the integer ring in k that divides p,

iii) $\beta(\sigma, \tau)$ is a factor set consisting of roots of unity,

iv) the defining relations of the crossed product $\mathfrak{A}$ are

$$u_\sigma \lambda = \lambda^\sigma u_\sigma \quad (\lambda \in K), \qquad u_\sigma u_\tau = \beta(\sigma, \tau) u_{\sigma\tau},$$

v) σ, τ are automorphisms of K/k.

In the preceding paragraph the problem of determining the Schur index was reduced to the case of the above Kreisalgebra. Now we shall calculate its index explicitly. Recall that the index of the crossed product $(\beta(\sigma, \tau), K/k)$ is equal to the order of the 2-cocycle $\beta(\sigma, \tau)$ in the second cohomology group $H^2(\mathfrak{G}(K/k), K^\times)$.

Let $K = \boldsymbol{Q}_p(\zeta_n)$, $n = p^h t$, $(p, t) = 1$, $N_{k/\boldsymbol{Q}_p}(\mathfrak{p}) = q$, where $N_{k/\boldsymbol{Q}_p}$ is the norm of k over $\boldsymbol{Q}_p$. In the case $h = 0$, the index of the simple algebra $\mathfrak{A}$ equals one, because the factor set $\beta(\sigma, \tau)$ consists of units and the ramification index of K/k equals one. So, throughout this paragraph, we assume that $h \geqq 1$. Let the ramification index of K/k be equal to e and the residue class degree of K/k be equal to f. Denote by U the (finite) group consisting of all the roots of unity contained in K. The p-Sylow subgroup of U is generated by a primitive p^h-th root of unity ζ_{p^h}, and the subgroup of U consisting of all the roots of unity whose orders are relatively prime to p, is generated by a primitive $(q^f - 1)$-th root of unity ζ_{q^f-1}. Then

$$U = \langle \zeta_{q^f-1} \rangle \times \langle \zeta_{p^h} \rangle \qquad \text{(direct product)}.$$

For every $\sigma, \tau \in \mathfrak{G}(K/k)$, let

$$\beta(\sigma, \tau) = \alpha(\sigma, \tau)\gamma(\sigma, \tau),$$

$$\alpha(\sigma, \tau) \in \langle \zeta_{q^f-1} \rangle, \qquad \gamma(\sigma, \tau) \in \langle \zeta_{p^h} \rangle.$$

Then we have

$$\mathfrak{A} = (\beta, K/k) \sim (\alpha, K/k) \otimes_k (\gamma, K/k).$$

Now assume that p is an odd prime number. The multiplicative group $\boldsymbol{Z} \bmod^\times p^h$ of integers modulo p^h is cyclic, and the inertia group $\mathfrak{T}$ of K/k is

isomorphic to a subgroup of $\boldsymbol{Z} \bmod^{\times} p^h$. Fix a generator ω of the cyclic group $\mathfrak{T}: \mathfrak{T} = \langle \omega \rangle$. Denote by η a Frobenius automorphism of K/k. Then $\mathfrak{G}(K/k) \cong \langle \omega, \eta \rangle$.

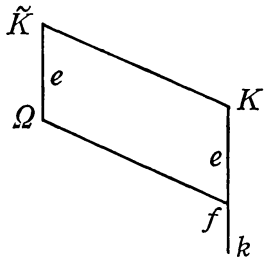
THEOREM 3. *Let p be an odd prime number. Let c be the index of tame ramification of $\mathfrak{p}$ over p, namely, $p = \mathfrak{p}^{cp^\lambda}$, $(c, p) = 1$, $\mathfrak{p} \subset k$, for a certain integer λ. Then the number*

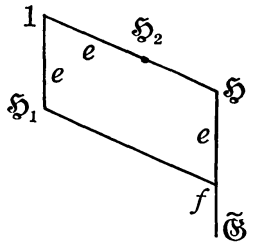
$$\delta = (\alpha(\omega, \eta)/\alpha(\eta, \omega))^{\frac{e}{q-1}} \alpha(\omega, \omega)\alpha(\omega^2, \omega) \cdots \alpha(\omega^{e-1}, \omega)$$

belongs to the field k, so that we can write it as $\delta = \zeta_{q-1}^{v}$ for a certain integer v. It turns out that the index of the crossed product $(\beta(\sigma, \tau), K/k)$ is equal to

$$\frac{(p-1)/c}{(v, (p-1)/c)}.$$

PROOF. First we shall calculate the order of the 2-cocycle $\alpha(\sigma, \tau)$ in the second cohomology group $H^2(\mathfrak{G}(K/k), K^{\times})$. We fix an unramified extension Ω of k such that i) Ω contains a $(q-1)$-th root $\sqrt[q-1]{\alpha(\sigma, \tau)}$ of $\alpha(\sigma, \tau)$ for every $\sigma, \tau \in \mathfrak{G}(K/k)$, ii) $ef \mid z = [\Omega : k]$. As unramified extensions are uniquely determined by their degrees, $\Omega = k(\zeta_{q^z-1})$ and $[\Omega \cap K : k] = f$. The composition field $\tilde{K} = \Omega K = \boldsymbol{Q}_p(\zeta_{p^h}, \zeta_{q^z-1})$ of Ω and K is an abelian extension of k and $[\tilde{K} : k] = ze$. $\tilde{K}/\Omega$ is totally ramified of degree e and





$\tilde{K}/K$ is unramified of degree z/f. Set $\mathfrak{G}(\tilde{K}/k) = \tilde{\mathfrak{G}}$, $\mathfrak{G}(\tilde{K}/K) = \mathfrak{H}$, and $\mathfrak{G}(\tilde{K}/\Omega) = \mathfrak{H}_1$. $\mathfrak{H}$ is a cyclic group of order z/f. The inertia group of $\tilde{K}/k$ is $\mathfrak{H}_1$, and the inertia group of K/k is isomorphic to $\mathfrak{H}_1\mathfrak{H}/\mathfrak{H} \cong \mathfrak{H}_1/\mathfrak{H}_1 \cap \mathfrak{H} \cong \mathfrak{H}_1$. Take a generator θ of $\mathfrak{H}_1$ such that the restriction of θ on the field K induces the automorphism ω, i.e., $\theta\mathfrak{H} = \omega$. Also we fix a Frobenius automorphism φ of $\tilde{K}/k$ such that the restriction of φ on K induces the Frobenius automorphism η of K/k. Let $\mathfrak{H}_2$ be the cyclic subgroup of $\mathfrak{H}$ of order e. Then $\mathfrak{H}_1 \cap \mathfrak{H}_2 = 1$ because $\mathfrak{H}_1 \cap \mathfrak{H} = 1$. Since the factor groups $\tilde{\mathfrak{G}}/\mathfrak{H}_1$ and $\tilde{\mathfrak{G}}/\mathfrak{H}_2$ are both of order z, φ^z is in $\mathfrak{H}_1 \cap \mathfrak{H}_2 = 1$. Hence $\varphi^z = 1$. Note that z is the residue class degree of $\tilde{K}/k$. Therefore $\tilde{\mathfrak{G}}$ is a split extension of $\mathfrak{H}_1$ by $\langle \varphi \rangle$: $\tilde{\mathfrak{G}} = \mathfrak{H}_1 \times \langle \varphi \rangle = \langle \theta \rangle \times \langle \varphi \rangle$. Let L be the subfield of $\tilde{K}/k$ which corresponds to the subgroup $\langle \varphi \rangle$ of $\tilde{\mathfrak{G}}$ in the sense of Galois theory: $\mathfrak{G}(\tilde{K}/L) = \langle \varphi \rangle$. Then L is a totally ramified extension of k of degree e and $L\Omega = \tilde{K}$ and $L \cap \Omega = k$.

Denote by $\tilde{\alpha}(\tilde{\sigma}, \tilde{\tau}) = (\mathrm{Inf}\,\alpha)(\tilde{\sigma}, \tilde{\tau})$, $\tilde{\sigma}, \tilde{\tau} \in \mathfrak{G}(\tilde{K}/k)$, the image of the cocycle $\alpha(\sigma, \tau)$ by the inflation map: $H^2(\mathfrak{G}(K/k), K^\times) \to H^2(\mathfrak{G}(\tilde{K}/k), \tilde{K}^\times)$. Since the inflation map is injective, the order of the 2-cocycle $\alpha(\sigma, \tau)$ in $H^2(\mathfrak{G}(K/k), K^\times)$ is equal to that of the 2-cocycle $\tilde{\alpha}(\tilde{\sigma}, \tilde{\tau})$ in $H^2(\mathfrak{G}(\tilde{K}/k), \tilde{K}^\times)$. So we are going to calculate the index of the crossed product

$$\tilde{\mathfrak{A}} = (\tilde{\alpha}(\tilde{\sigma}, \tilde{\tau}), \tilde{K}/k) = \sum_{\tilde{\sigma} \in \tilde{\mathfrak{G}}} \tilde{K} u_{\tilde{\sigma}},$$

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

whose factor set is $\tilde{\alpha}(\tilde{\sigma}, \tilde{\tau})$. As $\tilde{\mathfrak{G}} = \langle \theta \rangle \times \langle \varphi \rangle$, it follows that

$$\tilde{\mathfrak{A}} = \sum_{\substack{1 \leqq \nu \leqq e \\ 1 \leqq \mu \leqq z}} \tilde{K} u_\theta^\nu u_\varphi^\mu .$$

Set

$$\gamma = \sqrt[q-1]{\alpha(\theta, \varphi)/\tilde{\alpha}(\varphi, \theta)} .$$

Since $\theta \mathfrak{H} = \omega$ and $\varphi \mathfrak{H} = \eta$, we have

$$\gamma = \sqrt[q-1]{\alpha(\omega, \eta)/\alpha(\eta, \omega)} .$$

From the construction of Ω it follows that $\gamma \in \langle \zeta_{q^z-1} \rangle \subset \Omega$, and so $\gamma u_\theta = u_\theta \gamma$. We get

$$u_\theta u_\varphi = \frac{\tilde{\alpha}(\theta, \varphi)}{\tilde{\alpha}(\varphi, \theta)} u_\varphi u_\theta = \gamma^{q-1} u_\varphi u_\theta , \qquad (\gamma u_\theta) u_\varphi = \gamma^q u_\varphi u_\theta = u_\varphi (\gamma u_\theta) .$$

From the fact that γu_θ commutes with u_φ and each element of Ω (resp. L) commutes with γu_θ (resp. u_φ), it follows that

$$\tilde{\mathfrak{A}} = \sum_{\substack{1 \leqq \nu \leqq e \\ 1 \leqq \mu \leqq z}} \Omega L (\gamma u_\theta)^\nu u_\varphi^\mu = \{ \sum_{1 \leqq \nu \leqq e} L (\gamma u_\theta)^\nu \} \{ \sum_{1 \leqq \mu \leqq z} \Omega u_\varphi^\mu \}$$

$$\cong ((\gamma u_\theta)^e, L/k, \theta) \otimes_k (u_\varphi^z, \Omega/k, \varphi) \sim (\gamma^e u_\theta^e, L/k, \theta) .$$

In the above, $(u_\varphi^z, \Omega/k, \varphi) \sim 1$, because $u_\varphi^z = \tilde{\alpha}(\varphi, \varphi)\tilde{\alpha}(\varphi^2, \varphi) \cdots \tilde{\alpha}(\varphi^{z-1}, \varphi)$ is a root of unity and Ω/k is unramified. We see easily that

$$\begin{aligned} \delta &= (\gamma u_\theta)^e = \gamma^e u_\theta^e \\ &= \gamma^e \tilde{\alpha}(\theta, \theta)\tilde{\alpha}(\theta^2, \theta) \cdots \tilde{\alpha}(\theta^{e-1}, \theta) \\ &= (\alpha(\omega, \eta)/\alpha(\eta, \omega))^{\frac{e}{q-1}} \alpha(\omega, \omega)\alpha(\omega^2, \omega) \cdots \alpha(\omega^{e-1}, \omega) . \end{aligned}$$

Since δ is in $\tilde{K}$ and commutes with both u_θ and u_φ, δ is an element of the ground field k. As δ is a root of unity whose order is relatively prime to p, δ is expressed as $\delta = \zeta_{q-1}^v$ for a certain integer v.

Now we are going to calculate the index of the above cyclic algebra

$$(\delta, L/k, \theta) .$$

We know that the index is equal to the order of the norm residue symbol

$$(\delta, L/k)=\left(\frac{\delta, L/k}{\mathfrak{p}}\right), \quad \mathfrak{p}\subset k .$$

By the local class field theory, the Galois group of L/k is isomorphic to the factor group $k^\times/N_{L/k}(L^\times)$. Here, $N_{L/k}$ is the norm of L over k. So the order of $(\delta, L/k)$ is the smallest positive integer m such that δ^m is in $N_{L/k}(L^\times)$. Recall that L is a totally ramified extension of degree e and that e is also the ramification index of K/k. Since $K=\boldsymbol{Q}_p(\zeta_n)\supset k$, $n=p^h\cdot t$, $h\geqq 1$, $(p, t)=1$, $p=\mathfrak{p}^{cp^\lambda}$, $(c, p)=1$, $k\supset\mathfrak{p}$, the ramification index e of K/k equals $p^{h-1-\lambda}(p-1)/c$. Let π be a prime element of L. It is well known that every element y of $L^\times$ has a unique expression

$$y=\pi^s\zeta_{q-1}^r\rho,\ s\in\boldsymbol{Z},\ r \bmod q-1,\ \rho\text{: principal unit of } L .$$

Therefore we have

$$N_{L/k}(L^\times)=\{N_{L/k}(\pi)^s\zeta_{q-1}^{er}N_{L/k}(\rho);\ s\in\boldsymbol{Z},\ r \bmod q-1,\ \rho\text{: principal unit}\} .$$

As $N_{k/\boldsymbol{Q}_p}(\mathfrak{p})=q$ is a p-power, it follows that $(q-1, p)=1$ and $p-1\mid q-1$. Consequently, we have

$$N_{L/k}(L^\times)=\{N_{L/k}(\pi)^s\zeta_{q-1}^{r'(p-1)/c}N_{L/k}(\rho);\ s\in\boldsymbol{Z},\ 1\leqq r'\leqq(q-1)/\frac{p-1}{c},\ \rho\text{: principal unit}\} .$$

In the above, $N_{L/k}(\rho)$ are principal units of k. If $\delta^x=\zeta_{q-1}^{vx}$ is in $N_{L/k}(L^\times)$ for a certain positive integer x, then

$$\zeta_{q-1}^{vx}=N_{L/k}(\pi)^s\zeta_{q-1}^{r'(p-1)/c}N_{L/k}(\rho)$$

for some s, r' and ρ. From this we see easily that the smallest positive integer m such that δ^m is in $N_{L/k}(L^\times)$, is equal to

$$\frac{(p-1)/c}{(v, (p-1)/c)} .$$

Next we shall prove that the order of the 2-cocycle $\gamma(\sigma, \tau)$ in the second cohomology group $H^2(\mathfrak{G}(K/k), K^\times)$ is equal to one. Denote by $\gamma'(\iota, \kappa)=(\mathrm{Ver}\,\gamma)(\iota, \kappa)$, $\iota, \kappa\in\mathfrak{G}(K/\boldsymbol{Q}_p)$, the image of the cocycle $\gamma(\sigma, \tau)$ by the transfer (Verlagerung): $H^2(\mathfrak{G}(K/k), K^\times)\to H^2(\mathfrak{G}(K/\boldsymbol{Q}_p), K^\times)$. Since the transfer is an injective homomorphism, the order of the 2-cocycle $\gamma(\sigma, \tau)$ in $H^2(\mathfrak{G}(K/k), K^\times)$ is equal to that of the 2-cocycle $\gamma'(\iota, \kappa)$ in $H^2(\mathfrak{G}(K/\boldsymbol{Q}_p), K^\times)$. From the definition of the transfer, it follows that $\gamma'(\iota, \kappa)$, $\iota, \kappa\in\mathfrak{G}(K/\boldsymbol{Q}_p)$, are roots of unity whose orders are p-powers because $\gamma(\sigma, \tau)$, $\sigma, \tau\in\mathfrak{G}(K/k)$ have this property. We must prove that the index of the crossed product:

$$(\gamma'(\iota, \kappa), K/\boldsymbol{Q}_p)=\sum_{\iota\in\mathfrak{G}(K/\boldsymbol{Q}_p)}Ku_\iota ,$$

$$u_\iota u_\kappa = \gamma'(\iota, \kappa)u_{\iota\kappa}, \qquad u_\iota x u_\iota^{-1} = x^\iota, \qquad x \in K,$$

is equal to one. The cyclotomic field $K = \boldsymbol{Q}_p(\zeta_n)$, $n = p^h t$, $(p, t) = 1$ is the composite field $L\Omega$ of $L = \boldsymbol{Q}_p(\zeta_{p^h})$ and of the maximal unramified subfield Ω in $K/\boldsymbol{Q}_p$. $L/\boldsymbol{Q}_p$ is totally ramified and $L \cap \Omega = \boldsymbol{Q}_p$. $L/\boldsymbol{Q}_p$ is cyclic because p is an odd prime number. Of course, $\Omega/\boldsymbol{Q}_p$ is cyclic. Set

$$\mathfrak{G}(\Omega/\boldsymbol{Q}_p) \cong \mathfrak{G}(K/L) = \langle \varphi \rangle,$$

$$\mathfrak{G}(L/\boldsymbol{Q}_p) \cong \mathfrak{G}(K/\Omega) = \langle \theta \rangle.$$

Then we have

$$\mathfrak{G}(K/\boldsymbol{Q}_p) = \langle \varphi \rangle \times \langle \theta \rangle.$$

For any $\iota, \kappa \in \mathfrak{G}(K/\boldsymbol{Q}_p)$, $\gamma'(\iota, \kappa)$ belongs to the set $T = \{\zeta_{p^h}^\nu ; 0 \leqq \nu \leqq p^h - 1\}$. If $\zeta_{p^h}^\theta = \zeta_{p^h}^r$, then r is a primitive root $\bmod p^h$, i.e., $\langle r \bmod^\times p^h \rangle = \boldsymbol{Z} \bmod^\times p^h$. We check easily that $T^{r-1} = T$. Set

$$\gamma'(\varphi, \theta)/\gamma'(\theta, \varphi) = \rho^{r-1}, \qquad \rho \in T.$$

Then we have

$$u_\varphi u_\theta = (\gamma'(\varphi, \theta)/\gamma'(\theta, \varphi))u_\theta u_\varphi = \rho^{r-1} u_\theta u_\varphi,$$

$$(\rho u_\varphi)u_\theta = \rho^r u_\theta u_\varphi = u_\theta(\rho u_\varphi).$$

Since ρu_φ commutes with u_θ and u_θ (resp. ρu_φ) commutes with each element of Ω (resp. L), it follows that

$$\begin{aligned}(\gamma'(\iota, \kappa), K/\boldsymbol{Q}_p) &= \sum_{\iota \in \mathfrak{G}(K/\boldsymbol{Q}_p)} K u_\iota \\ &= \sum_{1 \leqq \nu \leqq p^h - 1(p-1),\ 1 \leqq \mu \leqq f'} L\Omega u_\theta^\nu (\rho u_\varphi)^\mu \\ &= (\sum_\nu L u_\theta^\nu)(\sum_\mu \Omega(\rho u_\varphi)^\mu) \\ &\cong (\varepsilon_1, L/\boldsymbol{Q}_p, \theta) \otimes_{\boldsymbol{Q}_p} (\varepsilon_2, \Omega/\boldsymbol{Q}_p, \varphi) \sim (\varepsilon_1, L/\boldsymbol{Q}_p, \theta).\end{aligned}$$

Here, $f' = [\Omega : \boldsymbol{Q}_p]$,

$$\varepsilon_1 = u_\theta^{p^{h-1}(p-1)} = \gamma'(\theta, \theta)\gamma'(\theta^2, \theta) \cdots \gamma'(\theta^{p^{h-1}(p-1)-1}, \theta),$$

$$\varepsilon_2 = (\rho u_\varphi)^{f'} = \rho^{f'}\gamma'(\varphi, \varphi)\gamma'(\varphi^2, \varphi) \cdots \gamma'(\varphi^{f'-1}, \varphi), \qquad (\rho u_\varphi = u_\varphi \rho).$$

Since $T \cap \boldsymbol{Q}_p = \{1\}$ and $\varepsilon_1 \in T \cap \boldsymbol{Q}_p$, we conclude that $\varepsilon_1 = 1$ and $(\varepsilon_1, L/\boldsymbol{Q}_p, \theta) \sim 1$. This completes the proof of Theorem 3.

§ 4. The proof of Theorem 1.

Let K be a field of characteristic 0. Let B and C be simple algebras over K. If L (resp. M) is the center of B (resp. C), both L and M contain K. We see easily that the tensor product $B \otimes_K C$ of B and C over K is isomorphic to $[L \cap M : K]$ copies of the central simple algebra

$$(B\otimes_L LM)\otimes_{LM}(C\otimes_M LM)$$

over LM. If $L=M=K$, $B\otimes_K C$ is a central simple algebra over K. Let G_1 and G_2 be finite groups and

$$K[G_1]=B_1\oplus\cdots\oplus B_s\,,\qquad K[G_2]=C_1\oplus\cdots\oplus C_t\,,$$

where the B_i, C_j are simple algebras over K. Then we have

$$K[G_1\times G_2]\cong K[G_1]\otimes_K K[G_2]\cong\sum_{i,j}B_i\otimes_K C_j\qquad\text{(direct sum)}.$$

By the above remark, each $B_i\otimes_K C_j$ is isomorphic to some copies of a simple algebra over K.

LEMMA. *Let L be a finite extension field of K (possibly $L=K$). Denote by $S_K(L)$ the subset of the Brauer group $Br(L)$ of L, consisting of those classes that contain simple components of group algebras $K[G]$ over K. If $S_K(L)$ is non-empty, then it is a subgroup of $Br(L)$.*

REMARK. If $L=K$, then $S_K(K)$ is non-empty, because $K[G]\cong K$ for $G=\{1\}$ and so the identity of $Br(K)$ belongs to $S_K(K)$.

PROOF. Let A_1 and A_2 be central simple algebras over L. If A_i $(i=1,2)$ is similar to a simple component of some group algebra $K[G_i]$ over K, the preceding arguments show that $A_1\otimes_L A_2$ is similar to a simple component of $K[G_1\times G_2]$. In fact, $[L:K]$ copies of a central simple algebra over L which is similar to $A_1\otimes_L A_2$ are contained in $K[G_1\times G_2]$ as simple components. Let G be a finite group and B a simple component of $K[G]$ whose center is L. Denote by U an absolutely irreducible (matrix) representation of G which corresponds to B, and by χ the character of U. Set

$$\tilde{U}(g)={}^tU(g^{-1})\,,\qquad g\in G\,.$$

Then $\tilde{U}$ is an absolutely irreducible representation of G whose character $\tilde{\chi}$ is given by $\tilde{\chi}(g)=\chi(g^{-1})$ so that $K(\tilde{\chi})=K(\chi)\cong L$. B is isomorphic to the enveloping algebra $\mathrm{env}_K(U)=\{\sum_{g\in G}\alpha_g U(g)\,;\ \alpha_g\in K\}$ of U over K whose center is isomorphic to $K(\chi)$. We see easily that by the one-to-one correspondence Φ between $\mathrm{env}_K(U)$ and $\mathrm{env}_K(\tilde{U})$ defined by $\Phi(U(g))=\tilde{U}(g^{-1})$ $(g\in G)$, $\mathrm{env}_K(U)$ is anti-isomorphic to $\mathrm{env}_K(\tilde{U})$. Therefore, the inverse of the class $\{B\}=\{\mathrm{env}_K(U)\}$ in $Br(L)$ belongs to $S_K(L)$. This completes the proof of Lemma.

Now we are ready to prove Theorem 1 and Theorem 2. In the following we shall use the same notation and assumption as in Theorems 1 and 2.

PROOF OF THEOREM 1. Let G be a finite group and A a simple component of $\boldsymbol{Q}_p[G]$. Let χ be an absolutely irreducible character of G which corresponds to A. Then the center of A is isomorphic to $\boldsymbol{Q}_p(\chi)$, which is clearly a subfield of Ξ such that $[\boldsymbol{Q}_p(\chi):\boldsymbol{Q}_p]$ is finite. For each prime number l, there exist a hyperelementary subgroup H of G and a character ξ of H such

that the l-part of the index of $A=A(\chi, \boldsymbol{Q}_p)$ is equal to the index of the simple component $A(\xi, \boldsymbol{Q}_p(\chi))$ of $\boldsymbol{Q}_p(\chi)[H]$ corresponding to ξ (cf. § 2). But $A(\xi, \boldsymbol{Q}_p(\chi))$ is isomorphic to $A(\xi, \boldsymbol{Q}_p)\otimes_{\boldsymbol{Q}_p(\xi)}\boldsymbol{Q}_p(\xi, \chi)$, and so the Hasse invariant of $A(\xi, \boldsymbol{Q}_p(\chi))$ is equal to

$$h(\xi, \boldsymbol{Q}_p)\cdot[\boldsymbol{Q}_p(\xi, \chi): \boldsymbol{Q}_p(\xi)] \qquad (\mathrm{mod}\ \boldsymbol{Z})$$

where $h(\xi, \boldsymbol{Q}_p)$ is the Hasse invariant of $A(\xi, \boldsymbol{Q}_p)$. From Propositions 1—3, it follows that $A(\xi, \boldsymbol{Q}_p)$ is similar to a Kreisalgebra $\mathfrak{A}$ whose center is $\boldsymbol{Q}_p(\xi)$. If c is the index of tame ramification of $\boldsymbol{Q}_p(\xi)/\boldsymbol{Q}_p$, it follows from Theorem 3 that the Hasse invariant of $\mathfrak{A}$ is of the form $z'/\frac{p-1}{c}$ for some $z'\in\boldsymbol{Z}$. If b is the index of tame ramification of $\boldsymbol{Q}_p(\chi)/\boldsymbol{Q}_p$, and b_1 (resp. b_2) is that of $(\boldsymbol{Q}_p(\xi)\cap\boldsymbol{Q}_p(\chi))/\boldsymbol{Q}_p$ (resp. of $\boldsymbol{Q}_p(\chi)/(\boldsymbol{Q}_p(\xi)\cap\boldsymbol{Q}_p(\chi))$), then $b=b_1b_2$ and $b_1|c$. Consequently,

$$h(\xi, \boldsymbol{Q}_p)\equiv z_1/\frac{p-1}{b_1}\ (\mathrm{mod}\ \boldsymbol{Z}), \qquad \left(z_1=z'\frac{c}{b_1}\in\boldsymbol{Z}\right)$$

and the Hasse invariant of $A(\xi, \boldsymbol{Q}_p(\chi))$ is of the form

$$z_2/\frac{p-1}{b}\ (\mathrm{mod}\ \boldsymbol{Z}), \qquad \left(z_2=z_1\frac{[\boldsymbol{Q}_p(\xi, \chi): \boldsymbol{Q}_p(\xi)]}{b_2}\in\boldsymbol{Z}\right).$$

Hence the index of $A(\xi, \boldsymbol{Q}_p(\chi))$ divides $\frac{p-1}{b}$, and so the l-part of the index of $A=A(\chi, \boldsymbol{Q}_p)$ divides $\frac{p-1}{b}$. As l is an arbitrary prime, the index of $A=A(\chi, \boldsymbol{Q}_p)$ divides $\frac{p-1}{b}$. Therefore the Hasse invariant of A is of the form

$$z/\frac{p-1}{b}\ (\mathrm{mod}\ \boldsymbol{Z}), \qquad \text{for some } z\in\boldsymbol{Z}.$$

Conversely, let k be a subfield of Ξ of finite degree over $\boldsymbol{Q}_p$, and let the index of tame ramification of $k/\boldsymbol{Q}_p$ be equal to b, $b|(p-1)$. We must prove that for every $z\in\boldsymbol{Z}$, the central division algebra over k whose Hasse invariant is $z/\frac{p-1}{b}$ (mod $\boldsymbol{Z}$), is similar to a simple component of some group algebra $\boldsymbol{Q}_p[G]$. By virtue of Lemma, we only need to prove that a central simple algebra over k whose index is $\frac{p-1}{b}$, is similar to a simple component of some $\boldsymbol{Q}_p[G]$. When k is contained in a cyclotomic field $\boldsymbol{Q}_p(\zeta_n)$, $n=p^ht$, $(p, t)=1$, we may assume that $h\geqq 1$. Let $\mathfrak{p}$ be the prime ideal of k dividing p. Set $N_{k/\boldsymbol{Q}_p}(\mathfrak{p})=q$. Let e be the ramification index of $\boldsymbol{Q}_p(\zeta_n)/k$ and f be the residue class degree of $\boldsymbol{Q}_p(\zeta_n)/k$. Note that the index of tame ramification of $\boldsymbol{Q}_p(\zeta_n)/k$ is equal to $(p-1)/b$. Set $a=ef$. We fix a primitive (q^a-1)-th root of unity ζ_{q^a-1} and a primitive p^h-th root of unity ζ_{p^h}, and set $\zeta=\zeta_{q^a-1}\zeta_{p^h}$. Consider the field $\tilde{K}=\boldsymbol{Q}_p(\zeta)=k(\zeta_{q^a-1}, \zeta_{p^h})$. Note that ζ_t is a power of ζ_{q^f-1}

which is a power of ζ_{q^a-1}. By the same argument as in the proof of Theorem 3, we conclude that there exist subfields $\Omega=k(\zeta_{q^a-1})$ and L of $\tilde{K}/k$ such that Ω/k is unramified of degree a and L/k is totally ramified of degree e and $\tilde{K}=\Omega L$. Let $\mathfrak{G}(\tilde{K}/k)=\langle\theta\rangle\times\langle\varphi\rangle$, $\mathfrak{G}(\tilde{K}/\Omega)=\langle\theta\rangle$ and $\mathfrak{G}(\tilde{K}/L)=\langle\varphi\rangle$. Consider the following crossed product $\mathfrak{A}$:

$$\mathfrak{A}=\sum_{1\leqq\nu\leqq e,\ 1\leqq\mu\leqq a}\tilde{K}u_\theta^\nu u_\varphi^\mu \qquad \text{(direct sum)},$$

$$u_\theta x=x^\theta u_\theta\,, \qquad u_\varphi x=x^\varphi u_\varphi \qquad (x\in\tilde{K})\,,$$

$$u_\theta u_\varphi=u_\varphi u_\theta\,, \qquad u_\theta^e=\zeta_{q-1}=\zeta^{p^h(q^a-1)/(q-1)}\,, \qquad u_\varphi^a=1\,.$$

We see easily that

$$\begin{aligned}\mathfrak{A}&=\sum_{1\leqq\nu\leqq e,\ 1\leqq\mu\leqq a}L\Omega u_\theta^\nu u_\varphi^\mu\\&=(L\cdot 1+Lu_\theta+\cdots+Lu_\theta^{e-1})\cdot(\Omega\cdot 1+\Omega u_\varphi+\cdots+\Omega u_\varphi^{a-1})\\&\cong(\zeta_{q-1},\,L/k,\,\theta)\otimes_k(1,\,\Omega/k,\,\varphi)\sim(\zeta_{q-1},\,L/k,\,\theta)\,.\end{aligned}$$

The index of $(\zeta_{q-1},\,L/k,\,\theta)$ is equal to the order of the norm residue symbol $(\zeta_{q-1},\,L/k)$. Note that the index of tame ramification of L/k is equal to $(p-1)/b$. Therefore, by the same argument as in the proof of Theorem 3, we conclude that the order of $(\zeta_{q-1},\,L/k)$ is equal to $(p-1)/b$.

We easily check that ζ, u_θ and u_φ generate a finite group G in the simple algebra $\mathfrak{A}$. Defining relations are:

$$\zeta^{(q^a-1)p^h}=1\,, \qquad \zeta=\zeta_{q^a-1}\zeta_{p^h}\,, \qquad u_\theta^e=\zeta^{p^h(q^a-1)/(q-1)}\,,$$

$$u_\varphi^a=1\,, \qquad u_\theta\zeta_{q^a-1}=\zeta_{q^a-1}u_\theta\,, \qquad u_\theta\zeta_{p^h}=\zeta_{p^h}^r u_\theta\,, \qquad u_\varphi\zeta_{q^a-1}=\zeta_{q^a-1}^q u_\varphi\,,$$

$$u_\varphi\zeta_{p^h}=\zeta_{p^h}^s u_\varphi\,, \qquad u_\theta u_\varphi=u_\varphi u_\theta\,,$$

where $r^e\equiv 1 \bmod p^h$, $r^\kappa\not\equiv 1 \bmod p^h$, $1\leqq\kappa\leqq e-1$ and $s^a\equiv 1 \bmod p^h$. In fact, $G=\langle\zeta,\,u_\theta,\,u_\varphi\rangle$ is an extension of the cyclic normal subgroup $\langle\zeta\rangle=\langle\zeta_{q^a-1}\rangle\times\langle\zeta_{p^h}\rangle$ by an abelian group which is a direct product of a cyclic group of order e and a cyclic group of order a (cf. Zassenhaus [14, III, § 8]). It is clear that the finite group G spans $\mathfrak{A}$ over $\boldsymbol{Q}_p$, i. e.,

$$\mathfrak{A}=\{\sum\alpha_{\nu\mu\lambda}\zeta^\nu u_\theta^\mu u_\varphi^\lambda\ ;\ \alpha_{\nu\mu\lambda}\in\boldsymbol{Q}_p,\ 1\leqq\nu\leqq(q^a-1)p^h,\ 1\leqq\mu\leqq e,\ 1\leqq\lambda\leqq a\}\,.$$

The absolutely irreducible representation in the algebraic closure $\bar{\boldsymbol{Q}}_p$ of $\boldsymbol{Q}_p$ (unique up to equivalence) of the central simple algebra $\mathfrak{A}$ over k gives an absolutely irreducible representation U of the finite group $G=\langle\zeta,\,u_\theta,\,u_\varphi\rangle$. And it is clear that the simple component of $\boldsymbol{Q}_p[G]$ which corresponds to U is isomorphic to $\mathfrak{A}$. As was already shown, the index of $\mathfrak{A}$ is equal to $(p-1)/b$. This completes the proof of Theorem 1.

Theorem 2 is clearly equivalent to the following

THEOREM 2′. *A given central simple algebra A over K is similar to a simple component of the group algebra $K[G]$ over K of a finite group G if and only if the Hasse invariant of A is of the form*

$$\frac{\kappa}{(p-1)/bs} \pmod{\boldsymbol{Z}}, \qquad \kappa \in \boldsymbol{Z}.$$

PROOF OF THEOREM 2′. From Theorem 1 it follows that for every $z \in \boldsymbol{Z}$, the central division algebra A over k whose Hasse invariant is $z/\frac{p-1}{b} \pmod{\boldsymbol{Z}}$, is similar to a simple component of the group algebra $\boldsymbol{Q}_p[G]$ of a certain group G. Hence A is similar to a simple component of the group algebra $k[G] \cong \boldsymbol{Q}_p[G] \otimes_{\boldsymbol{Q}_p} k$ over k of the same group G. And the central simple algebra $A \otimes_k K$ over K is similar to a simple component of $K[G] \cong k[G] \otimes_k K$. The Hasse invariant of $A \otimes_k K$ is equal to

$$\frac{z}{(p-1)/b}[K:k] = \frac{z}{(p-1)/bs}\frac{[K:k]}{s}, \qquad \left(\frac{p-1}{bs}, \frac{[K:k]}{s}\right) = 1.$$

Hence for every $\kappa \in \boldsymbol{Z}$, the central division algebra over K whose Hasse invariant is equal to $\kappa/\frac{p-1}{bs} \pmod{\boldsymbol{Z}}$, is similar to a simple component of a group algebra $K[G]$ over K.

Conversely, let A be a simple component of the group algebra $K[G]$ over K of a group G such that the center of A is K. If χ is an absolutely irreducible character of G which corresponds to A, then $K(\chi) = K$ and A is isomorphic to $A(\chi, \boldsymbol{Q}_p) \otimes_{\boldsymbol{Q}_p(\chi)} K$ where $A(\chi, \boldsymbol{Q}_p)$ is the simple component of $\boldsymbol{Q}_p[G]$ which corresponds to χ. The field $\boldsymbol{Q}_p(\chi)$ is contained in $\Xi \cap K = k$. If the index of tame ramification of $\boldsymbol{Q}_p(\chi)/\boldsymbol{Q}_p$ (resp. of $k/\boldsymbol{Q}_p(\chi)$) is equal to b_1 (resp. b_2), then $b = b_1 b_2$ and the Hasse invariant of the central simple algebra $A(\chi, \boldsymbol{Q}_p)$ over $\boldsymbol{Q}_p(\chi)$ is equal to $z/\frac{p-1}{b_1}$ for a certain $z \in \boldsymbol{Z}$. So the Hasse invariant of the central simple algebra A over K is equal to

$$\begin{aligned}\frac{z}{(p-1)/b_1}[K:\boldsymbol{Q}_p(\chi)] &= \frac{z}{(p-1)/b}\frac{[k:\boldsymbol{Q}_p(\chi)]}{b_2}[K:k] \\ &= \frac{z}{(p-1)/bs}\frac{[k:\boldsymbol{Q}_p(\chi)]}{b_2}\frac{[K:k]}{s} \pmod{\boldsymbol{Z}}.\end{aligned}$$

Thus the Hasse invariant of A is of the form $\kappa/\frac{p-1}{bs} \pmod{\boldsymbol{Z}}$, $\kappa \in \boldsymbol{Z}$. This completes the proof of Theorem 2′.

Tokyo Metropolitan University

References

[1] R. Brauer, On the representations of groups of finite order, Proc. Internat. Congress, Cambridge, 1950, vol. 2, 33-36.
[2] R. Brauer, On the algebraic structure of group rings, J. Math. Soc. Japan, **3** (1951), 237-251.
[3] R. Brauer, Representations of finite groups, Lectures on modern mathematics, edited by T. L. Saaty, vol. I, 133-175, John Wiley & Sons, New York, 1963.
[4] C. W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras, Interscience, New York, 1962.
[5] M. Deuring, Algebren, Springer, Berlin, 1935.
[6] W. Feit, Characters of finite groups, Benjamin, New York, 1967.
[7] B. Huppert, Endliche Gruppen I, Springer, Berlin, 1967.
[8] J.-P. Serre, Corps locaux, Hermann, Paris, 1962.
[9] L. Solomon, The representation of finite groups in algebraic number fields, J. Math. Soc. Japan, **13** (1961), 144-164.
[10] E. Weiss, Cohomology of groups, Academic Press, New York, 1969.
[11] E. Witt, Die algebraische Struktur des Gruppenringes einer endlichen Gruppe über einem Zahlkörper, J. Reine Angew. Math., **190** (1952), 231-245.
[12] T. Yamada, On the group algebras of metabelian groups over algebraic number fields II, J. Fac. Sci. Univ. Tokyo, **16** (1969), 83-90.
[13] T. Yamada, On the Schur index of a monomial representation, Proc. Japan Acad., **45** (1969), 522-525.
[14] H. Zassenhaus, The theory of groups, 2nd ed., Chelsea, New York, 1958.