TOKYO J. MATH.
VOL. 1, NO. 2, 1978

More on the Schur Index and the Order and Exponent of a Finite Group

Toshihiko YAMADA

Tokyo Metropolitan University

Let G be a finite group and K a field of characteristic 0. Let χ be an absolutely irreducible character of G and let $m_K(\chi)$ denote the Schur index of χ over K. In Fein and Yamada [1], we gave a theorem which relates $m_Q(\chi)$ to the order and exponent of G, where $\boldsymbol{Q}$ is the rational field. In this paper, we will give similar results for the case $K=\boldsymbol{Q}_l$, the l-adic numbers, where l is a prime. These results are easily derived from the formula of index of an l-adic cyclotomic algebra, which was obtained by the author [4], [5].

For the rest of the paper, k is a cyclotomic extension of $\boldsymbol{Q}_l$, i.e., k is a subfield of a cyclotomic field $\boldsymbol{Q}_l(\zeta')$, where ζ' is a root of unity. For a natural number n, ζ_n denotes a primitive n-th root of unity. A *cyclotomic algebra* over k is a crossed product

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

$$(2) \qquad u_\sigma x=\sigma(x)u_\sigma \quad (x\in k(\zeta)) , \quad u_\sigma u_\tau=\beta(\sigma, \tau)u_{\sigma\tau} , \quad (\sigma, \tau\in\mathscr{G}) ,$$

where ζ is a root of unity, $\mathscr{G}$ is the Galois group of $k(\zeta)$ over k, and β is a factor set whose values are roots of unity in $k(\zeta)$. Put $L=k(\zeta)$. Let $\varepsilon(L)$ denote the group of roots of unity contained in L. Let $\varepsilon'(L)$ (respectively, $\varepsilon_l(L)$) denote the subgroup of $\varepsilon(L)$ consisting of those roots of unity in L whose orders are relatively prime to l (respectively, powers of l). We have $\varepsilon(L)=\varepsilon'(L)\times\varepsilon_l(L)$. Let

$$(3) \qquad \beta(\sigma, \tau)=\alpha(\sigma, \tau)\gamma(\sigma, \tau) , \quad \alpha(\sigma, \tau)\in\varepsilon'(L) , \quad \gamma(\sigma, \tau)\in\varepsilon_l(L) .$$

Suppose that l is an odd prime. Let $\langle\theta\rangle$ denote the inertia group and ϕ a Frobenius automorphism of the extension $k(\zeta)/k$. The order e of θ has the form $e=l^te'$, $e'\,|\,l-1$. Let f denote the residue class degree of the extension $k/\boldsymbol{Q}_l$, so $\zeta_{l^f-1}\in k$.

Received February 11, 1978

THEOREM 1 (Yamada [4]). *Let l be an odd prime and k a cyclotomic extension of Q_l. Notation being as above, let $(\beta, k(\zeta)/k) \sim (\alpha, k(\zeta)/k) \otimes_k (\gamma, k(\zeta)/k)$ be a cyclotomic algebra over k given by (1)-(3). Then the number*

$$\delta = (\alpha(\theta, \phi)/\alpha(\phi, \theta))^{e/(l^f-1)}\alpha(\theta, \theta)\alpha(\theta^2, \theta) \cdots \alpha(\theta^{e-1}, \theta)$$

belongs to k, so that we can write $\delta = \zeta_{l^f-1}^v$ for a certain integer v. The index of the cyclotomic algebra $(\beta, k(\zeta)/k)$ is equal to $e'/(v, e')$.

PROOF. In [4, Theorem 3], this theorem is stated for the case $k(\zeta) = Q_l(\zeta')$, ζ' being some root of unity. But it is easy to see that the same proof is also valid for any extension $k(\zeta)/k$, ζ being a root of unity.

COROLLARY 2. *Notation being as in Theorem 1, suppose that the factor set β has all its values equal to roots of unity of order prime to l, i.e., $\beta(\sigma, \tau) \in \varepsilon'(k(\zeta))$, for all $\sigma, \tau \in \mathscr{G}$. Furthermore, suppose that $e = e'$, i.e., the ramification index e of the extension $k(\zeta)/k$ is not divisible by l. Then the index of the l-adic cyclotomic algebra $(\beta, k(\zeta)/k) = \sum_\sigma k(\zeta)u_\sigma$ divides the least common multiple of the orders of the elements $[u_\theta, u_\phi]$ and $u_\theta^{l^f-1}$, where $[u_\theta, u_\phi] = u_\theta u_\phi u_\theta^{-1} u_\phi^{-1}$.*

PROOF. We have $\beta(\sigma, \tau) = \alpha(\sigma, \tau)$, $\gamma(\sigma, \tau) = 1$ for any $\sigma, \tau \in \mathscr{G}$. Since $[u_\theta, u_\phi] = \beta(\theta, \phi)/\beta(\phi, \theta)$ and $u_\theta^e = \beta(\theta, \theta)\beta(\theta^2, \theta) \cdots \beta(\theta^{e-1}, \theta)$, it follows that $[u_\theta, u_\phi]$ and u_θ^e commute. Since $e = e'$ and $e' \mid l-1$, then

$$\begin{aligned}\delta^{(l^f-1)/e} &= (\beta(\theta, \phi)/\beta(\phi, \theta)) \cdot \{\beta(\theta, \theta)\beta(\theta^2, \theta) \cdots \beta(\theta^{e-1}, \theta)\}^{(l^f-1)/e} \\ &= [u_\theta, u_\phi] \cdot (u_\theta^e)^{(l^f-1)/e} = [u_\theta, u_\phi] \cdot u_\theta^{l^f-1}.\end{aligned}$$

Moreover, $[u_\theta, u_\phi]$ and $u_\theta^{l^f-1}$ commute. On the other hand,

$$\delta^{(l^f-1)/e} = \zeta_{l^f-1}^{v(l^f-1)/e} = \zeta_e^v,$$

whose order is equal to $e/(v, e) = e'/(v, e')$, the index of $(\beta, k(\zeta)/k)$. The corollary now follows at once.

THEOREM 3. *Let G be a finite group and χ an absolutely irreducible character of G. Suppose that l is an odd prime and p is a prime such that $p^n \neq 1$ divides the Schur index $m_{Q_l}(\chi)$ but p^{n+1} does not divide $m_{Q_l}(\chi)$. Then either p^{2n} divides the exponent of G or p^n divides the exponent of G', the commutator subgroup of G, and if p^{2n} does not divide the exponent of G then p^{2n+1} divides the order of G. If a Sylow p-subgroup of G is abelian, then p^{2n} divides the exponent of G.*

PROOF. By Theorem 1, $p^n \mid l-1$. Let s be the exponent of G and let k be the subfield of $Q_l(\zeta_s)$ such that $Q_l(\zeta_s) \supset k \supset Q_l(\chi)$, $[Q_l(\zeta_s): k]$ is a power of p and $p \nmid [k: Q_l(\chi)]$. By the Brauer-Witt theorem (see [6, p. 31]) there is a hyperelementary subgroup H (at p) of G and an irreducible character ξ of H with the following properties: (1) there is a normal subgroup N of H and a linear character ψ of N such that $\xi = \psi^H$; (2) $H/N \cong \mathscr{G} = \mathrm{Gal}(k(\psi)/k)$; (3) $k(\xi) = k$; (4) $m_k(\xi) = p^n$; (5) for every $h \in H$ there is a $\tau(h) \in \mathscr{G}$ such that $\psi(hnh^{-1}) = \tau(h)(\psi(n))$ for all $n \in N$; and (6) the simple component $A(\xi, k)$ of the group algebra $k[H]$ corresponding to ξ is isomorphic to the cyclotomic algebra $(\beta, k(\psi)/k) = \sum_{\tau \in \mathscr{G}} k(\psi) u_\tau$ where, if D is a complete set of coset representatives of N in $H (1 \in D)$ with $hh' = n(h, h')h''$ for $h, h', h'' \in D$, $n(h, h') \in N$, then $\beta(\tau(h), \tau(h')) = \psi(n(h, h'))$. Since $Q_l(\zeta_s) \supset k(\psi) \supset k$ and $[H: N] = [k(\psi): k]$ is a power of p, we may assume that D is contained in a Sylow p-subgroup of H, and so for any $\tau, \tau' \in \mathscr{G}$, $\beta(\tau, \tau')$ is a root of unity whose order is a power of p. In particular, the factor set β has all its values equal to roots of unity of order prime to l.

Let N_0 be the kernel of ψ and ζ a primitive $|N/N_0|$-th root of unity. Then $k(\psi) = k(\zeta)$ and N_0 is also the kernel of ξ. Moreover, the cyclotomic algebra $(\beta, k(\zeta)/k) = \sum_\tau k(\zeta) u_\tau$ contains the finite group $F = \langle \zeta, u_\tau (\tau \in \mathscr{G}) \rangle$, which is canonically isomorphic to H/N_0, i.e., F is a section of G.

Let $\langle \theta \rangle$ denote the inertia group and ϕ a Frobenius automorphism of the extension $k(\zeta)/k$. Let f be the residue class degree of k/Q_l. The order of $\langle \theta \rangle$ is a power of p, so is relatively prime to l. Corollary 2 now yields that p^n, the index of $(\beta, k(\zeta)/k)$, divides the least common multiple of the orders of the elements $[u_\theta, u_\phi]$ and $u_\theta^{l^f - 1}$ of F. Hence either p^n divides the exponent of F' or p^{2n} divides the exponent of F, because $l^f - 1 \equiv l - 1 \equiv 0 (\mathrm{mod}\, p^n)$. If a Sylow p-subgroup of G is abelian, then a Sylow p-subgroup of H is also abelian, and so $hh' = h'h$ for any $h, h' \in D$. By the isomorphism $H/N_0 \cong F$, this implies $u_\tau u_{\tau'} = u_{\tau'} u_\tau$ for any $\tau, \tau' \in \mathscr{G}$. In particular, $[u_\theta, u_\phi] = 1$, and consequently, p^{2n} divides the order of F.

If p^{2n} does not divide the exponent of F, then p^n divides the order of $[u_\theta, u_\phi] \in \langle \zeta \rangle$, so $p^n \,|\, |\langle \zeta \rangle|$. Recall that $F = \langle \zeta, u_\theta, u_\phi \rangle \triangleright \langle \zeta \rangle$ and $F/\langle \zeta \rangle \cong \langle \theta, \phi \rangle = \mathscr{G}$. By Theorem 1, p^n divides the order of θ, so p^{n+1} divides $[F: \langle \zeta \rangle]$. Hence $p^{2n+1} \,|\, |F|$. Since F is a section of G, Theorem 3 is proved.

Next we will give a corresponding result for the 2-adic number field Q_2. It is known that $m_{Q_2}(\chi) = 1$ or 2 for any irreducible character χ of a finite group G.

THEOREM 4. *Let G be a finite group and χ an irreducible character* *of G. If $m_{Q_2}(\chi)=2$, then 2^2 divides the exponent of G, 2 divides the exponent of G', and 2^3 divides the order of G.*

PROOF. As in the proof of Theorem 3, the Brauer-Witt theorem implies that there is a 2-adic cyclotomic algebra $B=(\beta, k(\zeta)/k)=\sum_{\tau\in\mathcal{G}} k(\zeta)u_\tau$, $\mathcal{G}=\mathrm{Gal}(k(\zeta)/k)$, with the following properties: (1) ζ is a root of unity and k is a cyclotomic extension of $\boldsymbol{Q}_2$; (2) the index of B equals 2; (3) if ζ has order $2^t r$, $(2, r)=1$, then $\beta(\sigma, \tau)\in\langle\zeta_{2^t}\rangle$ for $\sigma, \tau\in\mathcal{G}$; (4) B contains a finite group $F=\langle\zeta, u_\tau(\tau\in\mathcal{G})\rangle$, which is isomorphic to a section of G; (5) $F\triangleright\langle\zeta\rangle$ and $F/\langle\zeta\rangle\cong\mathcal{G}$.

Since B has index 2, then $\zeta_4\notin k$ (see [3, Satz 12] or [5, Proposition 5.4]). Furthermore, $t\geqq 2$, because if $t\leqq 1$, then $k(\zeta)/k$ would be unramified and the index of B would be equal to 1. Hence 2^2 divides the exponent of F. By Theorem 3.1 of [5], we see easily that $\mathcal{G}$ contains an automorphism ι with $\iota(\zeta_{2^t})=\zeta_{2^t}^{-1}$. Then $u_\iota\zeta_{2^t}u_\iota^{-1}=\zeta_{2^t}^{-1}$ and the commutator $[u_\iota, \zeta_{2^t}]=\zeta_{2^t}^{-2}\in F'$ has order $2^{t-1}\geqq 2$, i.e., $2\,|\,|F'|$. Since $\iota\in\mathcal{G}$ has order 2, then $|F|=[F\colon\langle\zeta\rangle]\cdot|\langle\zeta\rangle|=|\mathcal{G}|\cdot|\langle\zeta\rangle|\equiv 0 \pmod 8$, as was to be shown.

Let $\boldsymbol{R}$ be the real numbers. Let G be a finite group and χ an irreducible character of G. Although $m_{\boldsymbol{R}}(\chi)=1$ or 2, Theorem 4 does not necessarily hold for the case $m_{\boldsymbol{R}}(\chi)=2$. We will give such an example.

REMARK. Let $G=\langle a, b\rangle$ be the group of order 12 with the defining relations $a^6=1$, $b^2=a^3$, $bab^{-1}=a^{-1}$. Then $|G|=$exponent of $G=2^2 3$, $|G'|=3$. It is easy to see that G has a faithful irreducible character χ which is induced from a faithful linear character ψ of $\langle a\rangle$. The simple component of the group algebra $\boldsymbol{Q}[G]$ over the rationals $\boldsymbol{Q}$ which corresponds to χ is canonically isomorphic to the cyclic algebra $(-1, \boldsymbol{Q}(\zeta_3)/\boldsymbol{Q}, \iota)=\boldsymbol{Q}(\zeta_3)+\boldsymbol{Q}(\zeta_3)u$, $u^2=-1$, $u\zeta_3 u^{-1}=\zeta_3^{-1}=\iota(\zeta_3)$. This algebra has $\boldsymbol{R}$-local index 2, and so $m_{\boldsymbol{R}}(\chi)=2$. But 2 does not divide the exponent of G' and $2^3\nmid|G|$.

THEOREM 5. *Let G be a finite group and χ a complex irreducible character of G. Let p be a prime. Suppose $p^n(>1)$ divides the Schur index $m_{\boldsymbol{Q}}(\chi)$ of χ over the rationals $\boldsymbol{Q}$ and $p^{n+1}\nmid m_{\boldsymbol{Q}}(\chi)$. Then either p^{2n} divides the exponent of G or p^n divides the exponent of G'. If p^{2n} does not divide the exponent of G, then p^{2n+1} divides the order of G. If a Sylow p-subgroup of G is abelian then p^{2n} divides the exponent of G.*

PROOF. Recall that $m_{\boldsymbol{Q}}(\chi)$ is the least common multiple of the (local) Schur indices $m_{\boldsymbol{Q}_l}(\chi)$ and $m_{\boldsymbol{R}}(\chi)$, where l ranges over all the primes. If there is an odd prime l such that $m_{\boldsymbol{Q}_l}(\chi)$ is divisible by p^n, then Theorem 5 is immediate from Theorem 3. If there is no odd prime l with $m_{\boldsymbol{Q}_l}(\chi)$ divisible by p^n, then p^n divides either $m_{\boldsymbol{Q}_2}(\chi)$ or $m_{\boldsymbol{R}}(\chi)$. It follows that

$p=2, n=1$. Then by the Fein-Yamada theorem [1], $2^2=2^{2n}$ divides the exponent of G, and Theorem 5 is proved.

REMARK. We use the notation of Theorem 5. In [1], we actually proved that either p^{n+1} divides the exponent of G or p^n divides the exponent of G' (see p. 497 of [1]). The fact that either p^{2n} divides the exponent of G or p^n divides the exponent of G' is thus a refinement of part of the Fein-Yamada theorem and was already announced by Ford [2].

References

[1] B. FEIN and T. YAMADA, The Schur index and the order and exponent of a finite group, J. Algebra, **28** (1974), 496–498.

[2] C. FORD, Theorems relating finite groups and division algebras, in Proceedings of the Conference on Finite Groups, ed. by W. Scott, Academic Press, New York, 1976.

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

[4] 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.

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

[6] T. YAMADA, The Schur Subgroup of the Brauer Group, Lecture Notes in Math., Vol. 397, Springer, 1974.

Present Address:
DEPARTMENT OF MATHEMATICS
TOKYO METROPOLITAN UNIVERSITY
FUKAZAWA, SETAGAYA-KU, TOKYO 158