Y. Miyata
Nagoya Math. J.
Vol. 77 (1980), 13-23

ON THE MODULE STRUCTURE OF A p-EXTENSION OVER A $\mathfrak{p}$-ADIC NUMBER FIELD

YOSHIMASA MIYATA

Throughout this paper, let p be an odd prime. Let k be a $\mathfrak{p}$-adic number field and $\mathfrak{o}$ be the ring of all integers in k. Let K/k be a finite totally ramified Galois p-extension of degree p^n with the Galois group G. Clearly the ring $\mathfrak{O}$ of all integers in K is an $\mathfrak{o}[G]$-module. In the previous paper [4], we studied $\mathfrak{o}[G]$-module structure of $\mathfrak{O}$ in a cyclic totally ramified p-extension, and we have obtained the condition for $\mathfrak{O}$ to be an indecomposable $\mathfrak{o}[G]$-module. In the present paper, we shall prove the following theorem.

THEOREM 1. *Suppose that k contains a primitive p-th root of unity. Let K/k be a totally ramified Galois p-extension of degree p^n such that the extension K/k is not cyclic. Let E be a central idempotent of the group ring $k[G]$ such that $E\mathfrak{O} \subseteq \mathfrak{O}$. Then we have $E = 1$.*

As an immediate consequence of Theorem 1, we have the next theorem.

THEOREM 2. *Let k and K/k be as stated in Theorem 1. In addition, we assume that the extension K/k is abelian. Then the $\mathfrak{o}[G]$-module $\mathfrak{O}$ is indecomposable.*

In § 1, we shall study properties of central idempotent. In § 2, recalling properties of ramification numbers, we shall obtain some inequalities. In § 3, we shall study the special case where the Galois group G is an elementary abelian group of order p^2. In § 4, we shall study the case where the Galois group G is a direct product of two cyclic groups whose orders are p and p^n respectively. In § 5, we shall prove Theorem 1 and Theorem 2.

Received July 25, 1978.

1.

In this section, we shall study some properties of central idempotents. Let G be a non-cyclic p-groups and H be a normal subgroup of order p. The natural map from G onto the factor group G/H induces the ring homomorphism f_H from the group ring $k[G]$ onto $k[G/H]$. Let $C(G)$ denote the center of G. First, we assume that $C(G)$ is not cyclic. Then $C(G)$ contains an elementary abelian p-group C of order p^2.

Lemma 1. *Let G be a non-cyclic p-group and C be as stated in the above. Suppose that the center $C(G)$ of G is not cyclic. Let E be a central idempotent of $k[G]$ such that $f_H(E) = 1$ for any normal subgroup H of order p in C. Then $E = 1$.*

Proof. Without any loss of generality of proof, we can assume that k is the splitting field for G. Let χ be an absolutely irreducible character and E_χ be the central idempotent corresponding to χ. Then there is some subgroup H of C such that $E_\chi \cdot \frac{1}{p}\left(\sum_{h \in H} h\right) = E_\chi$. Since $f_H(E) = 1$ from the assumption, we have $E = \frac{1}{p}\left(\sum_{h \in H} h\right) + E'$, where E' is a central idempotent such that $E' \cdot \frac{1}{p}\left(\sum_{h \in H} h\right) = 0$. Therefore, for any absolutely irreducible character χ, $E_\chi \cdot E = E_\chi$, which implies that $E = 1$.

Next, we assume that $C(G)$ is cyclic. Clearly G has the unique normal subgroup Z of order p, and G is not abelian because G is not cyclic. Then, since p is odd, it is well known that G contains a normal elementary abelian subgroup B of order p^2(for example, see [2] III 7.5, p. 303). From the uniqueness of Z, it follows easily that Z is contained in $B \cap C(G)$. Let b and z be fixed generators of B such that $b \notin C(G)$ and $z \in C(G)$. Let $C_G(b)$ be the centralizer of b in G and Φ be the Frattini subgroup of G. As B is normal in G and Z is a characteristic subgroup of B, for any $g \in G$, we have

$$b^{-1}gb = gz^i \tag{1}$$

for some rational integer i $(0 \leqq i < p)$ which depends on g. Since $b \notin C(G)$, from (1), we see easily that $C_G(b)$ is a proper normal subgroup of G and hence we have

$$C_G(b)\Phi \neq G\,. \tag{2}$$

Now we obtain the following lemma.

LEMMA 2. *Let G be a non-cyclic p-group. Suppose that the center $C(G)$ of G is cyclic. Let Z, B, z and b be as above. Let E be a central idempotent of $k[G]$ such that $E\cdot\frac{1}{p}\left(\sum_{i=0}^{p-1} z^i\right) = 0$. Then E belongs to the group ring $k[C_G(b)\Phi]$.*

Proof. We can also assume that k is a splitting field for G without loss of generality of proof. Let χ be an absolutely irreducible character and E_χ be the central idempotent of $k[G]$ corresponding to χ such that $E_\chi E = E_\chi$. Since $E\cdot\frac{1}{p}\left(\sum_{i=0}^{p-1} z^i\right) = 0$, we have $E_\chi\cdot\frac{1}{p}\left(\sum z^i\right) = 0$. Let $E_\chi = \sum_{g\in G}\alpha_g g$, where α_g is in k. In order to prove the lemma, it is sufficient to show that if $\alpha_g \neq 0$, then $g \in C_G(b)\Phi$. As is well known, G is an M-group and so χ is induced by a linear character α of some subgroup A in G. Denote by $|A|$ the order of A. Using α, we define a mapping $\dot{\alpha}$ by

$$\begin{aligned} \dot{\alpha}(g) &= \alpha(g) && \text{if } g \in A \\ \dot{\alpha}(g) &= 0 && \text{if } g \notin A\,. \end{aligned}$$

Then we have the formula

$$\chi(g) = \frac{1}{|A|}\sum_{h\in G}\dot{\alpha}(h^{-1}gh) \qquad \text{(for example, see [2] p. 553).}$$

Now, as $\alpha_g \neq 0$, $\chi(g^{-1}) = 0$ and for some $h_0 \in G$, $h_0^{-1}g^{-1}h_0 \in A$. Let $a = h_0^{-1}g^{-1}h_0$. Immediately, $\chi(a) = \chi(g^{-1})$ and so $\chi(a) \neq 0$. Here suppose that $a \notin C_G(b)$. Clearly $b \notin C_G(a)$. Since B is normal, it follows easily that $C_G(a)B$ is a subgroup of G and $C_G(a)$ is a normal subgroup of $C_G(a)B$. Hence the set $\{1, b, \cdots, b^{p-1}\}$ is a set of right coset representatives of $C_G(a)$ in $C_G(a)B$. Let a set $\{h_1, \cdots, h_l\}$ be a set of right representatives of $C_G(a)B$ in G, so the set $\{b^i h_j \mid 0 \leqq i < p, 1 \leqq j \leqq l\}$ are right representatives of $C_G(a)B$ in G. As $a \notin C_G(b)$, $b^{-1}ab = az^{i_0}$ for some i_0 such that $i_0 \neq 0$. For the sake of simplicity, we denote by z the element z^i again. Then $b^{-i}ab^i = az^i$ for $0 \leqq i < p$. Hence we have

$$\begin{aligned} \chi(a) &= \frac{|C_G(a)|}{|A|}\sum_{i,j}\dot{\alpha}(h_j^{-1}b^{-i}ab^i h_j) \\ &= \frac{|C_G(a)|}{|A|}\sum_j\sum_i\dot{\alpha}(h_j^{-1}ah_j z^i)\,. \end{aligned}$$

As $E_\chi \cdot \frac{1}{p}(\sum z^i) = 0$, $zE_\chi = \theta E_\chi$, where θ is a primitive p-th root of unity. Therefore Z is contained in A, and so $h_j^{-1}ah_jz^i \in A$ if and only if $h_j^{-1}ah_j \in A$. Hence we obtain for any j

$$\sum_i \dot{\alpha}(h_j^{-1}b^{-i}ab^ih_j) = \dot{\alpha}(h_j^{-1}ah_j)\Bigl(\sum_{i=0}^{p-1}\theta^i\Bigr) = 0 \,.$$

Then, if $a \notin C_G(b)$, $\chi(g^{-1}) = \chi(a) = 0$, which is a contradiction. Hence we conclude that if $\alpha_g \neq 0$, then $a \in C_G(b)$. As G/Φ is abelian, then $g \in a^{-1}\Phi$. Therefore we have $g \in C_G(b)\Phi$, which completes the proof.

2.

Now denote by e the absolute ramification index of k. Let F/k be a cyclic ramified extension of degree p with the first ramification number b. Define a function m by $m(b) = \left[\frac{(p-1)(b+1)}{p}\right]$. We write b in the form $b = p\left[\frac{b}{p}\right] + p - \lambda$. From [1] Theorem 3, we have that for $(b, p) = 1$,

$$(3) \qquad m(b) + \lambda - 1 \equiv 0 \qquad (p-1)\,.$$

Next let K_1 and K_2 be cyclic ramified extensions of degree p with ramification numbers b_1 and b_2 respectively. Let K be the composition field of K_1 and K_2. According to the result of E. Maus ([3]), we can obtain the first ramification number $b(K/K_1)$ for the extension K/K_1 as follows:

i) if $b_2 > b_1$, $b(K/K_1) = b_1 + p(b_2 - b_1)$

ii) if $b_2 < b_1$, $b(K/K_1) = b_2$

iii) if $b_2 = b_1$, either $b(K/K_1) = b_1$, or for some c such that $c < b_1$, $b(K/K_1) = c$.

Using these equalities, we shall have the following lemma.

LEMMA 3. *Let K/k be a totally ramified extension such that the Galois group of K/k is an elementary abelian p-group of order p^2. Let F be a subfield of degree p in K. Then $m(b(K/F)) < pe$.*

Proof. There is a subfield F_1 of degree p such that K is the composition field of F and F_1. Denote by b and b_1 the first ramification numbers of F and F_1 respectively. First, we consider the case $b < b_1$. From the above equality i), we have $m(b(K/F)) = m(b) + (p-1)(b_1 - b)$.

Since $b_1 \leqq \frac{pe}{p-1}$, $(p-1)b - m(b) \leqq pe - m(b(K/F))$. As is easily seen, $b < b_1$ means $(b, p) = 1$. Put $b = p\left[\frac{b}{p}\right] + p - \lambda$, so that $(p-1)b - m(b)$ $= (p-1)^2\left[\frac{b}{p}\right] + (p-2)(p-\lambda)$. Since p is odd, then $(p-1)b - m(b) > 0$, so $pe - m(b(K/F)) > 0$.

Next, we shall consider remaining cases. From the above equalities ii) and iii), we have $m(b(K/F)) \leqq m(b)$. Then, by the well known fact that $m(b) \leqq e$, we have $m(b(K/F)) < pe$. Thus the proof is completed.

Now, let L/k be a cyclic totally ramified extension of degree p^n with n ramification numbers $b_1, b_2, \cdots, b_n$.

LEMMA 4. *Let L/k, b_1 and b_n be as above. Then $m(b_1) < e$ if and only if $m(b_n) < p^{n-1}e$.*

Proof. From [4] Lemma 2, we have that if $m(b_1) < e$, then $m(b_n) < p^{n-1}e$. Then, to complete the proof, we need to show that if $m(b_n) < p^{n-1}e$, $m(b_1) < e$. For it, as is easily seen, it suffices to prove only for the case of $n = 2$. From [4] Lemma 1, we can assume that k contains a primitive p-th root of unity without loss of generality of proof. Then we observe that $m(b_1) = e$ if and only if $b_1 = \frac{pe}{p-1}$ or $\frac{pe}{p-1} - 1$. Hence $b_2 \geqq \frac{p^2e}{p-1} - 1$. From [5] Corollary 26, we have that if $b_1 < \frac{e}{p-1}$, $\frac{p^2e}{p-1} - (p-1)b_1 \geqq b_2$ and if $b_1 \geqq \frac{e}{p-1}$, $b_2 = b_1 + pe$. First, suppose $b_1 < \frac{e}{p-1}$. Then we have that $\frac{p^2e}{p-1} - (p-1)b_1 \geqq \frac{p^2e}{p-1} - 1$ and hence $(p-1)b_1 \leqq 1$, which is a contradiction. Thus we have that $b_1 \geqq \frac{e}{p-1}$ and $b_1 \geqq \frac{pe}{p-1} - 1$ because $b_1 = b_2 - pe$ and $b_2 \geqq \frac{p^2e}{p-1} - 1$. From this result, it clearly follows that $m(b_1) = e$.

4.

Throughout the rest of this paper, we assume that k contains a primitive p-th root of unity. Then $(p-1)$ divides e and so let e_0 be

$e_0 = \dfrac{e}{p-1}$. Let π_0 be a prime element of k and denote by val_k the valuation of k ($\mathrm{val}_k(\pi_0) = 1$). Let K/k be a totally ramified extension whose Galois group is a elementary abelian p-group of order p^2 as described in the paragraph preceding Lemma 3. Now we may divide such extensions into following five types.

(i) $K = k(w_1, w_2)$, where $w_i^p \in k$ and $\mathrm{val}_k(w_i^p - 1) \geqq 2$ for $i = 1, 2$.

(ii) $K = k(z, w)$, where $w^p \in k$, $\mathrm{val}_k(w^p - 1) \geqq 2$, $z^p \in k$ and $\mathrm{val}_k(z^p - 1) = 1$.

(iii) $K = k(z_1, z_2)$, where $z_i^p \in k$ and $\mathrm{val}_k(z_i^p - 1) = 1$. Moreover, let K/k be the extension with exactly one ramification number $pe_0 - 1$.

(iv) $K = k(\pi, w)$, where $w^p \in k$, $\mathrm{val}_k(w^p - 1) \geqq 2$, $\pi^p \in k$ and $\mathrm{val}_k(\pi^p) = 1$.

(v) $K = k(\pi, z)$, where $z^p \in k$, $\mathrm{val}_k(z^p - 1) = 1$, $\pi^p \in k$ and $\mathrm{val}_k(\pi^p) = 1$.

In the following, we shall prove that the ring $\mathfrak{O}$ of all integers in K is an indecomposable $\mathfrak{o}[G]$-module. Let φ be an $\mathfrak{o}[G]$-endomorphism of $\mathfrak{O}$ such that $\varphi^2 = \varphi$. Clearly, proving that the ring $\mathfrak{O}$ is indecomposable is equivalent to showing $\varphi = 1$. We shall show the latter for the extension of each type stated in the above as (ii), (iii), (iv) and (v). Now we begin with the case of type (iii).

(I) The case of type (iii). Let Π be a prime element of K. Since $\mathrm{val}_K(z_i - 1) = p$ because of the definition of type (iii), then there exist units ω_1 and ω_2 of k such that $z_i - 1 \equiv \omega_i \Pi^p \ (\Pi^{p+1})$ for $i = 1, 2$.

Lemma 5. *Let z_i and ω_i be as above. For rational integers i_1 and i_2, let $i_1\omega_1 + i_2\omega_2 \equiv 0 \ (\Pi)$. Then $i_1 \equiv i_2 \equiv 0 \ (p)$.*

Proof. From the assumption, we have $z_1^{i_1} z_2^{i_2} \equiv 1 \, (\Pi^{p+1})$. Suppose $z_1^{i_1} z_2^{i_2} \notin k$ and let b be the ramification number for the extension $k(z_1^{i_1} z_2^{i_2})/k$. Then, from the result of B. F. Wyman ([5]), we have $b < pe_0 - 1$, which is contrary to the fact that K/k has exactly one ramification number $pe_0 - 1$. Hence $z_1^{i_1} z_2^{i_2} \in k$, which implies that $i_1 \equiv i_2 \equiv 0 \, (p)$.

Lemma 6. *Let I_0 and I_1 be subsets of $\{0, 1, \cdots, p-1\}$. Moreover, suppose that I_1 is a proper subset. Then*

$$\mathrm{val}_K \left[\left\{ \left(\sum_{i \in I_0} z_1^i \right) z_2 \right\} - \sum_{i \in I_0} z_1^i \right] - (|I_1| - |I_0|) = p \,,$$

where $|I_j|$ is the number of the set I_j.

Proof. Since $z_j^i \equiv 1 + i\omega_j \Pi^p (\Pi^{p+1})$, we have

$$\left\{\left(\sum_{i\in I_1} z_1^i\right)z_2 - \sum_{i\in I_0} z_1^i\right\} - (|I_1| - |I_0|)$$
$$\equiv |I_1|\,\omega_2\Pi^p + \left\{\left(\sum_{i\in I_1} i\right) - \left(\sum_{i\in I_0} i\right)\right\}\omega_1\Pi^p\,(\Pi^{p+1})\ .$$

By Lemma 5 and from the assumption $0 < |I_1| < p$, it follows that $|I_1|\,\omega_2 + \{(\sum_{i\in I_1} i) - (\sum_{i\in I_0} i)\}\omega_1 \notin (\pi_0)$. This completes the proof.

Now we can assume that $\varphi(1) = 1$ (replacing φ by $1 - \varphi$ if necessary). Clearly $\varphi(z_1^{i_1}z_2^{i_2}) = z_1^{i_1}z_2^{i_2}$ or 0. Let $\alpha_j = \dfrac{1}{\pi_0}(1 + z_1 + \cdots + z_1^{p-1})(z_2^j - 1)$ for $1 \leqq j < p$. Then $\alpha_j = \dfrac{1}{\pi_0}\cdot\dfrac{z_1^p - 1}{z_1 - 1}(z_2^j - 1)$. As $\mathrm{val}_K(z_1 - 1) = \mathrm{val}_K(z_2 - 1) = p$, $\mathrm{val}_K(\alpha_j) = 0$. Set $\varphi(\alpha_1) = \dfrac{1}{\pi_0}\left\{\left(\sum_{i\in I_1} z_1^i\right)z_2 - \sum_{i\in I_0} z_1^i\right\}$ and suppose that I_1 is a proper subset of $\{0, 1, \cdots, p-1\}$. From Lemma 6, we have $\mathrm{val}_K(\varphi(\alpha_1)) \leqq p - p^2$, which is a contradiction. Hence $I_1 = \varnothing$ or $\{0, 1, \cdots, p-1\}$. Next suppose $I_1 = \varnothing$, so $\varphi(\alpha_1) < 0$, a contradiction. Thus we conclude $I_1 = \{0, 1, \cdots, p-1\}$. Now we examine the set I_0 and suppose $0 < |I_0| < p$. Then we have $\pi_0\varphi(\alpha_1) \equiv -|I_0|\,(\Pi^p)$ and so $\mathrm{val}_K(\varphi(\alpha_1)) < 0$, a contradiction. As $\varphi(1) = 1$, $|I_0| > 0$ and hence $I_0 = \{0, 1, \cdots, p-1\}$. Therefore we have $\varphi(z_1^i z_2) = z_1^i z_2$ and $\varphi(z_1^i) = z_1^i$ for $0 \leqq i < p$. Similarly, evaluating $\mathrm{val}_K(\varphi(\alpha_j))$, we have that $\varphi(z_1^i z_2^j) = z_1^i z_2^j$ for any i and any j, and that $\varphi = 1$.

(II) The case of type (ii). Let $\alpha_j = \dfrac{1}{\pi_0} z^j(1 + w + \cdots + w^{p-1})$ for $j = 0, 1, \cdots, p-1$ and let $\beta = \dfrac{1}{\pi_0}(1 + z + \cdots + z^{p-1})\pi_1$, where π_1 is a prime element of $k(w)$. Using the similar arguments as in (I), we can easily conclude $\varphi = 1$.

(III) The case of type (iv). Without loss of generality of proof, we can assume $\pi^p = \pi_0$. Let $\alpha_j = \dfrac{1}{\pi_0}\pi^j(1 + w + \cdots + w^{p-1})$ for $j = 0, 1, \cdots, p-1$. Using the result of S. Amano ([1]), we shall define an integer β. From his result, there exists a prime element π_1 of $k(w)$ such that π_1 is a root of the following equation

$$X^p - \omega\pi_0^m X - \pi_0(1 + a\pi_0) = 0\ , \tag{4}$$

where ω is a unit of $k, a \in \mathfrak{o}$ and $m = m(b(k(w)/k))$. Clearly $\pi_1^p = \pi_0(1 + \omega\pi_0^{m-1}\pi_1^\lambda + a\pi_0)$. Then chose an integer ε of $\mathfrak{o}$ as follows: if $m \leqq 2, \varepsilon = 0$ and if $m \geqq 3$, chose ε such that $\pi_1^p(1 + \varepsilon\pi_1)^p \equiv \pi_0\,(\pi_0^3)$. Let $u = \dfrac{\pi_1(1 + \varepsilon\pi_1)}{\pi}$ and $\beta = \dfrac{\pi^{p-1}}{\pi_0}(u^{p-1} + u^{p-2} + \cdots + 1)$. Then u is a unit of K such that $u \equiv 1\,(\Pi)$. Put $i = \mathrm{val}_K(u - 1)$. Then it is easy to see that if $i < \dfrac{p^2e}{p-1}$, $\mathrm{val}_K\,(u^p - 1) = pi$ and if $i \geqq \dfrac{p^2e}{p-1}$, $\mathrm{val}_K\,(u^p - 1) = i + p^2e$. From (3), we have that if $m = 1, \lambda \geqq 2$ and so $i \geqq 2$. First, assume $i < \dfrac{p^2e}{p-1}$. Then $\mathrm{val}_K\,(\beta) = pi + (p-1)p - i - p^2 = (p-1)i - p$. As $i \geqq 2$, we have $\mathrm{val}_K\,(\beta) > 0$. For the case $i \geqq \dfrac{p^2e}{p-1}$, $\mathrm{val}_K\,(\beta) = p^2e - p$. Hence β is in $\mathfrak{O}$ for the both cases. Also, we immediately get $\mathrm{val}_K\,(\alpha_j) \geqq 0$. Since $\varphi(\alpha_j)$ and $\varphi(\beta)$ are in $\mathfrak{O}$, we have that $\varphi(\pi^jw^i) = \pi^jw^i$ and $\varphi = 1$ as in (I).

(VI) The case of type (v). As $\mathrm{val}_K\,(z^p - 1) = 1$, z satisfies the following congruence $z^p \equiv 1 + \varepsilon_0\pi_0\,(\pi_0^2)$, where ε_0 is a unit of k. Then there exists a unit ε of k such that $\varepsilon^p\varepsilon_0 \equiv 1\,(\pi_0)$. Now, let $\alpha_0 = \dfrac{1}{\pi_0}\Big[\{\varepsilon(-1+z)\}^{p-1} + \{\varepsilon(-1 + z)\}^{p-2}\pi + \cdots + \pi^{p-1}\Big]$ and $u = \dfrac{\varepsilon(-1 + z)}{\pi}$. Then $u^p \equiv \dfrac{\varepsilon^p(-1+z^p)}{\pi_0} \equiv 1\,(\Pi^{p^2})$. Put $i = \mathrm{val}_K\,(u - 1)$, so clearly $i \geqq p$. Then we have $\mathrm{val}_K\,(\alpha_0) > 0$ as in (III). We observe easily that $(-1 + z)^{p-1} \equiv 1 + z + \cdots + z^{p-1}(p)$. Hence $\pi_0\varphi(\alpha_0) \equiv \varepsilon^{p-1}\varphi(1 + z + \cdots + z^{p-1})(\pi)$. Set $\varphi(1 + z + \cdots + z^{p-1}) = \sum_{i \in I} z^i$ and suppose $1 \leqq |I| < p$. Then $\varphi(1 + z + \cdots + z^{p-1})$ is a unit of K and so $\mathrm{val}_K\,\varphi(\alpha_0) = -p^2$, a contradiction. Thus $\varphi(z^i) = z^i$ for $i = 0, 1, \cdots, p-1$. Using the same arguments as in (III) with this fact, we conclude $\varphi = 1$.

PROPOSITION 1. *Suppose that k contains a primitive p-th root of unity. Let K/k be a totally ramified extension whose Galois group is an elementary abelian p-group of order p^2. Then $\mathfrak{O}$ is an indecomposable* $\mathfrak{o}[G]$*-module.*

Proof. We have just proved the results for the cases where the extensions K/k are not of type (i). It remains to verify for the case of type (i). First, we note that for any subfield F of degree p in K, $m(b(F/k)) < e$. From [4] Theorem 3, the ring $\mathfrak{O}_F$ of all integers in F is indecomposable.

Hence, from Lemma 1, we obtain the desired result for the extension of type (i).

4.

In this section, we shall treat the case where the Galois group G is a direct product of two cyclic groups whose orders are p and p^n respectively. Let F and L be cyclic totally ramified extensions of degrees p and p^n respectively. Let K be a composition field of F and L, and assume that K is totally ramified. Let φ be an $\mathfrak{o}[G]$-endomorphism of $\mathfrak{O}$ such that $\varphi^2 = \varphi$ as in the previous section. As G is abelian, we can consider φ as an idempotent of $k[G]$. Let L_1 is the unique subfield of degree p in L and S denote the subgroup of G corresponding to L_1. First, we assume that k contains a primitive p^n-th root of unity. Then there exists an element γ of L such that $L = k(\gamma)$ and $\gamma^{p^n} = \pi_0^{p^m} u_0$, where $0 \leqq m \leqq n$ and u_0 is a unit of k such that $u_0 \equiv 1\,(\pi_0)$. Denote by δ a primitive element of F as given in § 3, i.e. δ is one of w, z and π. Now, since $k\gamma^i\delta^j$ is a $k[G]$-module, obviously $\varphi(\gamma^i\delta^j) = \gamma^i\delta^j$ or 0 for $0 \leqq i < p^n$ and $0 \leqq j < p$. For $1 \leqq i < p^{n-1}$ with $(i, p) = 1$, put $q = [ip^m/p^n]$. Then γ^i/π_0^q is integer of K. For the case $m \geqq 1$, let $v = \gamma^{p^{n-1}}/\pi_0^{p^{m-1}}$. Immediately, we have that v^p is a unit of k such that $v^p \equiv 1(\pi_0)$ and that $\sum_{l=0}^{p-1} \mathfrak{o}\left(\dfrac{\gamma^{i+lp^{n-1}}}{\pi_0^{q+lp^{m-1}}}\right) = \dfrac{\gamma^i}{\pi_0^q} \sum_{l=0}^{p-1} \mathfrak{o}v^l$. For the case $m = 0$, we have $\sum_{l=0}^{p-1} \mathfrak{o}\gamma^{i+lp^{n-1}} = \gamma^i(\sum \mathfrak{o}\eta^l)$, where $\eta = \gamma^{p^{n-1}}(\mathrm{val}_{L_1}(\eta) = 1)$. Furthermore, we remark $\gamma^i L_1 = \sum_{l=0}^{p-1} k\gamma^{i+lp^{n-1}}$. Now, from the similar arguments as in § 3 with the above remarks, we conclude that $\varphi(\gamma^{i+lp^{n-1}}\delta^j) = \gamma^{i+lp^{n-1}}\delta^j$ for any l and any j, or all $\varphi(\gamma^{i+lp^{n-1}}\delta^j)$ are simultaneously equal to the zero element of $\mathfrak{O}$ except the case where $p = 3, e = 2$, $\mathrm{val}_L(\gamma^i/\pi_0^q) \geqq p^{n-1}$ and the extension L_1F is of type (v) such that $m(b(L_1/k)) = 2$ and $m(b(F/k)) = 3$. In the following, we consider the remaining case. Let π_1 be a prime element of L_1 which satisfies the equation (4) as given in § 3. As is easily seen, $\{1, v, v^2\}$ is an integral base. Then π_1 is written in the form $\pi_1 = a_0 + a_1 v + a_2 v^2$, where $a_i \in \mathfrak{o}$. As $\mathrm{tr}_{L_1/k}\,\pi_1 = 0$, we see that $a_0 = 0$ and $a_1 \equiv -a_2 \not\equiv 0\,(\pi_0)$. Denote γ^i/π_0^q by $\gamma'$and let i_0 be the minimal integer i' such that $3^{n-1}i' + \mathrm{val}_L(\gamma') \geqq 3^n$. As $3^{n-1} \leqq \mathrm{val}_L\,\gamma' < 3^n$, we have $0 < i_0 \leqq 2$. First, we consider the case $i_0 = 1$. Let $\alpha_0 = \dfrac{\gamma'}{\pi_0}(1 + v + v^2)$ and $\alpha_2 = \dfrac{\gamma'\pi^2}{\pi_0^2}(1 + v + v^2)$. Then, evaluating $\mathrm{val}_K(\varphi(\alpha_0))$ and $\mathrm{val}_K(\varphi(\alpha_2))$, we have $\varphi(\gamma' v^i) = \gamma' v^i$ and $\varphi(\gamma' v^i \pi^2) = \gamma' v^i \pi^2$ for $0 \leqq i < 3$. Next let $\alpha_1 = \frac{\gamma}{\pi_0}(1 + u + u^2)$, where $u = \frac{\pi_1}{\pi}$ as in § 3. As $u \equiv 1\,(\pi_1)$, we see $\mathrm{val}_K\,\alpha_1 \geqq 0$. Clearly $\frac{\pi_0}{\pi_0}\alpha_1 = \frac{\gamma}{\pi_0^2}(\pi_0 + \pi_1\pi^2 + \pi_1^2\pi)$. Let $\varphi\{\gamma(1 + v + v^2)\pi\} = \gamma\pi(\sum_{i\in I} v^i)$ and suppose $1 \leqq |I| < 3$. Then $\pi_0^2\varphi(\alpha_1) \equiv \gamma(-a_1^2)\pi(\gamma\pi_0)$, which is contrary to $\varphi(\alpha_1) \geqq 0$ since a_1 is a unit of k and $\mathrm{val}_K\,(\gamma\pi) < 2\cdot 3^{n+1}$. Thus we conclude $I = \{0, 1, 2\}$ or $\varnothing$. Similarly, for the case $i_0 = 2$, we have the desired result. This completes the proof of the above statement for this case. Now, according to the same arguments as used in [4] with the above statement, we have that the idempotent φ is an element of $k[S]$. Next, we assume that k does not contains a primitive p^n-th root of unity. Then it follows from [4] Lemma 4 that $\varphi \in k[S]$. Therefore, clearly by the inductive arguments, we obtain the following proposition.

PROPOSITION 2. *Let K/k be a totally ramified extension whose Galois group is a direct product of two cyclic groups of orders p and p^n respectively. Suppose that k contains a primitive p-th root of unity. Then $\mathfrak{O}$ is indecomposable.*

5.

In this section, we shall give the proofs of Theorem 1 and Theorem 2. First, we shall prove Theorem 1 and use the same notations as in the previous sections. Let G be a non-cyclic p-group of order p^n and let E be a central idempotent of $k[G]$ such that $E\mathfrak{O} \subseteq \mathfrak{O}$. We use induction on n of p-power p^n. From Proposition 1, we obtain the result for $n = 2$. Assume the result holds for $n < r$. Let G be a non-cyclic p-group of order p^r. First, we assume that the center $C(G)$ of G is not cyclic as in Lemma 1. Now, if there exists a subgroup H of order p in C such that the factor group G/H is cyclic, then G is of type (p, p^{r-1}) and so the desired result follows from Proposition 2. Thus we consider the case where for any subgroup H of order p in C, the factor group G/H is not cyclic. By our inductive assumption, $f_H(E) = 1$. Then, from Lemma 1, we obtain $E = 1$, which completes the proof of Theorem 1 for the first case. Next, we assume that $C(G)$ is cyclic. As G is not cyclic, G is not abelian and hence G/Z is not cyclic. By our inductive assumption, we have $f_Z(E) = 1$ and so we can write $E = \frac{1}{p}\sum_{i=0}^{p-1} z^i + E_0$, where E_0 is a central idempotent such that $E_0 \cdot \dfrac{1}{p}(\sum_{i=0}^{p-1} z^i) = 0$. From Lemma 2, we have $E_0 \in C_G(b)\Phi$ and $E \in C_G(b)\Phi$. Denote by K_Z the subfield corresponding to Z. Then, from Lemma 3, $m(b(K/K_Z)) < e_Z$, where e_Z is the absolute ramification index of K_Z, since K_Z contains a subfield K_B corresponding to B. Therefore, if $C_G(b)\Phi$ is cyclic, it follows from Lemma 4 and [4] Theorem 3 that $E = 1$. Thus we now consider the case where $C_G(b)\Phi$ is not cyclic. Now, by (2), we note $|C_G(b)\Phi| < |G|$. Hence we can apply our inductive assumption to this case and conclude $E = 1$. The proof of Theorem 1 is completed.

Next, we shall prove Theorem 2. Let φ be an $\mathfrak{o}[G]$-endomorphism of $\mathfrak{O}$ such that $\varphi^2 = \varphi$. To prove Theorem 2 it is sufficient to show $\varphi = 1$. As the extension K/k is abelian, we can consider φ as an idempotent of $k[G]$. Then, from Theorem 1, we have obtained $\varphi = 1$ and the proof of Theorem 2.

References

[1] S. Amano, Eisenstein equations of degree p in a 𝔭-adic field, J. Fac. Sci. Univ. Tokyo **18**, No. 1 (1971), 1–21.

[2] B. Huppert, Endlich Gruppen I, Die Grundlehren der math. Wissenshaften, Band 134, Springer-Verlag, Berlin and New York 1967.

[3] E. Maus, Arithmetish disjucte Körper, J. reine angew. Math. **226** (1967), 184–203.

[4] Y. Miyata, On the module of a cyclic extension over a 𝔭-adic number field, Nagoya Math. J. **73** (1979), 61–68.

[5] B. F. Wyman, Wildly ramified gamma extension, Amer. J. of Math. **91** (1969), 135–152.

Faculty of Education
Shizuoka University