Y. Miyata
Nagoya Math. J.
Vol. 73 (1979), 61-68

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

YOSHIMASA MIYATA

Let p be a prime. Let k be a $\mathfrak{p}$-adic number field and $\mathfrak{o}$ be the ring of all integers of k. Let K/k be a cyclic totally ramified extension of degree p^n with Galois group G. Clealy the ring $\mathfrak{O}$ of all integers of K is an $\mathfrak{o}[G]$-module, and the purpose of this paper is to give a necessary and sufficient condition for the $\mathfrak{o}[G]$-module $\mathfrak{O}$ to be indecomposable.

In §§1–2, we shall prepare some lemmas. In §§3–4, we shall obtain the necessary and sufficient condition (Theorem 3).

Throughout this paper, let π be a prime element of k and e be the absolute ramification index of k. For a positive rational integer a, we define a function $m(a)$ by

$$m(a) = \left[\frac{(p-1)(a+1)}{p}\right].$$

1.

In this section, we shall obtain some inequalities for ramification numbers. Let F/k be a cyclic ramified extension of prime degree p with the first ramification number b. Let $\mathfrak{O}_F$ be the ring of all integers of F. Let e, π and $m(a)$ be the same as in Introduction. Then it is well known that

$$m(b) \leqq e$$

and

$$\operatorname{tr}_{F/k} \mathfrak{O}_F = (\pi^{m(b)}), \tag{1}$$

where $\operatorname{tr}_{F/k}$ denotes the trace map from F to k (for example, see [2]).

Let ζ be a primitive p-th root of 1. Let F' and k' be the extensions

Received October 8, 1977.

$F(\zeta)$ and $k(\zeta)$ respectively. Then the degree d of k' over k divides $p-1$ and k'/k is tamely ramified. As F/k is a cyclic extension of degree p, so is F'/k'. As is well known, the only one ramification number b' of F'/k' is db. Then we have the following lemma.

LEMMA 1. *Let F, F', b and b' be as stated in the above. Then $m(b) < e$ if and only if $m(b') < de$.*

Proof. Since the extension F'/F is tamely ramified, $\mathrm{tr}_{F'/F}\mathfrak{O}_{F'} = \mathfrak{O}_F$. Then, from (1), we have $\mathrm{tr}_{F'/k}\mathfrak{O}_{F'} = (\pi^{m(b)})$. We can choose a prime element π' of k' such that $\pi'^d \in k$. Clearly $\mathrm{tr}_{k'/k}\pi'^i = 0$ for $1 \leqq i \leqq d-1$ and $\mathrm{tr}_{k'/k}\pi'^d = d\pi'^d$. d is a unit of k. Then we obtain easily that

$$\mathrm{tr}_{F'/k}\mathfrak{O}_{F'} = \mathrm{tr}_{k'/k}\mathrm{tr}_{F'/k'}\mathfrak{O}_{F'} = (\pi^{[m(b')/d]}) .$$

Hence $(\pi^{m(b)}) = (\pi^{[m(b')/d]})$. This proves our assertion.

Let K be a cyclic totally ramified extension of degree p^n of k with the Galois group G. Since K/k is cyclic, we see that there exist n ramification numbers $b_1, \cdots, b_n$. The b_i-th ramification group is a subgroup $\langle g^{p^{i-1}}\rangle$ generated by $g^{p^{i-1}}$, where g denotes a generator of G.

LEMMA 2. *Let $K/k, b_1, \cdots, b_n$ be as above. Then if $m(b_1) < e$, $m(b_i) < p^{i-1}e$ for each $i, 1 \leqq i \leqq n$.*

Proof. As is easily seen, it is sufficient to prove only for the case $n = 2$. From Lemma 1, we can assume that k contains a primitive p-th root of 1 without any loss of generality of this proof. From a result of B. F. Wyman ([3], Corollary 26), we have that if $b_1 \geqq \dfrac{e}{p-1}$,

$$b_2 = b_1 + pe ,$$

and if $b_1 < \dfrac{e}{p-1}$,

$$b_2 \leqq \frac{p^2e}{p-1} - (p-1)b_1 .$$

At first, we suppose $b_1 \geqq \dfrac{e}{p-1}$. Then

$$\begin{aligned} m(b_2) &= \left[\frac{(p-1)(b_1+pe+1)}{p}\right] = (p-1)e + \left[\frac{(p-1)(b_1+1)}{p}\right] \\ &= (p-1)e + m(b_1) . \end{aligned}$$

From the assumption $m(b_1) < e$, it follows that $m(b_2) < pe$.

Next, we suppose $b_1 < \dfrac{e}{p-1}$. Put

$$\frac{(p-1)(b_1+1)}{p} = m(b_1) + \frac{r}{p} .$$

Then

$$\begin{aligned} m(b_2) &\leqq \left[\frac{(p-1)\left\{\dfrac{p^2 e}{p-1} - (p-1)b_1 + 1\right\}}{p}\right] \\ &= pe + (p-1) - (p-1)m - r . \end{aligned}$$

From $r \leqq p-1$ and $m < e$, it follows $m(b_2) < pe$. Clearly this completes the proof.

2.

In this section, we study the properties of idempotents of the group ring $k[G]$. Let G be a cyclic group of order p^n and let g denote a generator of G. Let θ be a primitive p^n-th root of 1 and let k' be $k' = k(\theta)$. Setting

$$\varepsilon_i = \frac{1}{p^n} \sum_{j=0}^{p^n-1} (\theta^{-i})^j g^j , \qquad 0 \leqq i \leqq p^n - 1 ,$$

we see that ε_i is an idempotent and $g\varepsilon_i = \theta^i \varepsilon_i$. Let H be $H = \langle g^{p^{n-1}} \rangle$. Obviously H is a subgroup of order p. We denote by T the idempotent $\dfrac{1}{p}\Big(\sum_{h \in H} h\Big)$ in $k[G]$. The canonical map from G onto the factor group G/H induces the ring homomorphism φ from the group ring $k[G]$ onto $k[G/H]$. Then we have the following two lemmas.

LEMMA 3. *Let G be a cyclic group of order p^n. Let ε_i and φ be as stated in the above. Suppose that k contains a primitive p^n-th root θ of 1. Then $\varphi(\varepsilon_i) = 0$ for $0 \leqq i < p^n$ if and only if $(i, p) = 1$.*

Proof. From easy computations, we can obtain $\ker \varphi = k[G](1 - T)$. Then $\varepsilon_i \in \ker \varphi$ if and only if $\varepsilon_i T = 0$. From $g^{p^{n-1}} \varepsilon_i = \theta^{ip^{n-1}} \varepsilon_i$, $T\varepsilon_i = \dfrac{1}{p}\left\{\sum_{j=0}^{p-1} (\theta^{ip^{n-1}})^j\right\}\varepsilon_i$. We note that $\sum_{j=0}^{p-1} (\theta^{ip^{n-1}})^j = 0$ if and only if $(i, p) = 1$.

Clearly this completes the proof of the lemma.

LEMMA 4. *Suppose that k does not contain a primitive p^n-th root θ of 1. Let G be a cyclic group of order p^n and let S be a subgroup $\langle g^p \rangle$. Let ε be an idempotent of $k[G]$ such that $\varphi(\varepsilon) = 0$. Then, if $n \geqq 2$, $\varepsilon \in k[S]$.*

Proof. From our assumption, the extension $k(\theta)/k(\theta^p)$ is a cyclic extension of degree p with the Galois group V. It is easily seen that there exists an element σ of V such that $\sigma(\theta) = \theta^{1+p^{n-1}}$. We can consider σ as an automorphism of $k'[G]$ in the usual way. Now for $0 \leqq i < p^n$, $\varepsilon\varepsilon_i = \varepsilon_i$ or 0. If $\varepsilon\varepsilon_i = \varepsilon_i$, then $\varepsilon\varepsilon_i^\sigma = \varepsilon_i^\sigma$ because $\varepsilon^\sigma = \varepsilon$. Hence $\varepsilon\,(\sum_{j=0}^{p-1} \varepsilon_i^{\sigma^j}) = \sum_{j=0}^{p-1} \varepsilon_i^{\sigma^j}$. Put $\sum_{j=0}^{p-1} \varepsilon_i^{\sigma^j} = \sum_{\ell=0}^{p^n-1} a_\ell g^\ell$ in $k'[G]$. Then

$$a_\ell = \sum_{j=0}^{p-1} (\theta^{-i\ell})^{\sigma^j} = \theta^{-i\ell}\left(\sum_{j=0}^{p-1} (\theta^{-i\ell})^{p^{n-1}j}\right).$$

Therefore, if $(i,p) = 1 = (\ell,p)$, we have $a_\ell = 0$. Since $\varphi(\varepsilon) = 0$, it follows from Lemma 3 that if $\varepsilon\varepsilon_i = \varepsilon_i$, then $(i,p) = 1$. Let $\varepsilon = \sum_{\ell=0}^{p^n-1} b_\ell g^\ell$ in $k[G]$. The fact which we have just shown implies $b_\ell = 0$ for $0 \leqq \ell < p^n$ with $(\ell,p) = 1$. This completes the proof.

3.

In this section, we treat the case that the extension K/k is a Kummer extension. We use the same notations as in previous two sections. Let K/k be a cyclic totally ramified extension of degree p^n. Throughout this section, we suppose k contains a primitive p^n-th root θ of 1. Then we see that there exists an element A of K such that

$$K = k(A) \quad \text{and} \quad A^{p^n} = \pi^{p^m} u\,,$$

where $0 \leqq m \leqq n$ and u is a unit of k. Furthermore, we may take the unit u such that $u - 1 \in (\pi)$ since the degree of the extension is a power of p. Let $b_1, \cdots, b_n$ be the sequence of the ramification numbers of K/k as in §1. Let $K_i = k(A^{p^{n-i}})$ for $0 \leqq i \leqq n$. Then the degree of the extension K_i/k is p^i.

LEMMA 5. *Let A, m and u be as stated in the above. Then, if $m = 0$, or $m > 0$ and $u - 1 \notin (\pi^2)$, we have $m(b_1) = e$.*

Proof. By the hypothesis, $K_1 = k(\sqrt[p]{\pi u})$ or $K_1 = k(\sqrt[p]{u})$. From a result of B. F. Wyman ([3], Corollary 13), we have $b_1 = \frac{pe}{p-1}$ or $\frac{pe}{p-1} - 1$. Then $m(b_1) = e$.

Now we consider the case that $m > 0$ and $u - 1 \in (\pi^2)$. Write u in the form $u = 1 + \pi^2 u_0$, where u_0 is an integer of k. For $1 \leqq i < p^{n-1}$ with $(i, p) = 1$, we define an element B_i of K by

$$B_i = \frac{A^i}{\pi^j}\left\{1 + \frac{A^{p^{n-1}}}{\pi^{p^{m-1}}} + \cdots + \left(\frac{A^{p^{n-1}}}{\pi^{p^{m-1}}}\right)^{p-1}\right\},$$

where $j = \left[\frac{ip^m}{p^n}\right] + 1$.

LEMMA 6. *Suppose that $m > 0$ and $u - 1 \in (\pi^2)$. Let B_i be as stated in the above. Then B_i is an element of $\mathfrak{O}$.*

Proof. We denote the valuation of K by val. Clearly $\mathrm{val}\,\pi = p^n$. From $m > 0$, $K_1 = k(\sqrt[p]{u})$. Put $\sqrt[p]{u} = 1 + U$. $(1 + U)^p = 1 + \pi^2 u_0$. Therefore we have $\mathrm{val}\,U \geqq 2p^{n-1}$.

$$u_0\pi^2 = (1 + U)^p - 1 = U\left(\sum_{j=0}^{p-1}(1 + U)^j\right). \tag{2}$$

Now we evaluate the valuation of the sum $\sum_{j=0}^{p-1}(1 + U)^j$. By the formula $\sum_{r=m}^{n}\binom{r}{m} = \binom{n+1}{m+1}$, we obtain

$$\sum_{j=0}^{p-1}(1 + U)^j = \sum_{j=0}^{p-1}\binom{p}{j+1}U^j.$$

Clearly from $\mathrm{val}\,U \geqq 2p^{n-1}$, it follows that $\mathrm{val}\sum_{j=0}^{p-1}(1 + U)^j \geqq p^n$. By (2), we have

$$\mathrm{val}\,U \leqq p^n + \mathrm{val}\,u_0. \tag{3}$$

Here we note that $A^{p^{n-1}} = \pi^{p^{m-1}}\sqrt[p]{u}$. Therefore

$$\begin{aligned} B_i &= \frac{A^i}{\pi^j}(1 + \sqrt[p]{u} + (\sqrt[p]{u})^2 + \cdots + (\sqrt[p]{u})^{p-1}) \\ &= \frac{A^i}{\pi^j}\frac{u-1}{\sqrt[p]{u} - 1}. \end{aligned}$$

Hence

$$\operatorname{val} B_i = ip^m + 2p^n + \operatorname{val} u_0 - jp^n - \operatorname{val} U .$$

By the definition of $j, ip^m + p^n - jp^n \geqq 0$, and we obtain

$$\operatorname{val} B_i \geqq p^n + \operatorname{val} u_0 - \operatorname{val} U .$$

From (3), $\operatorname{val} B_i \geqq 0$. Then B_i belongs to $\mathfrak{O}$.

We are now ready to prove the following theorem which is the main aim of this section.

THEOREM 1. *Suppose k contains a primitive p^n-th root of 1. Let K/k be a cyclic totally ramified extension of degree p^n. Then the ring $\mathfrak{O}$ of all integers in K is an indecomposable $\mathfrak{o}[G]$-module if and only if $m(b_1) < e$.*

Proof. First, suppose $m(b_1) = e$. Then, from Lemma 2, we have $m(b_n) = p^{n-1}e$. Let T be the idempotent $\frac{1}{p}\left(\sum_{\ell=0}^{p-1} (g^{p^{n-1}})^\ell\right)$ as in § 2. Then it follows from (1) that $T\mathfrak{O} \subseteq \mathfrak{O}$, and so $\mathfrak{O}$ posseses a direct sum decomposition

$$\mathfrak{O} = T\mathfrak{O} \oplus (1 - T)\mathfrak{O} .$$

Therefore $\mathfrak{O}$ is not indecomposable, and we have proved that if $\mathfrak{O}$ is indecomposable, then $m(b_1) < e$.

Next suppose $m(b_1) < e$. We use induction on the length n of a tower of intermediate fields

$$k = K_0 \subset K_1 \subset \cdots \subset K_n = K .$$

As a immediate consequence of Theorem 1 of [1], we obtain the result for $n = 1$. Assume the result holds for the extension whose length is fewer than n. Let E be an $\mathfrak{o}[G]$-endomorphism of $\mathfrak{O}$ such that $E^2 = E$ (i.e. a projection). Then we can consider E as an idempotent of $k[G]$. Let $\mathfrak{O}_i$ be the ring of all integers in K_i, so $\mathfrak{O}_i$ is an $\mathfrak{o}[G]$-submodule of $\mathfrak{O}$. Then $E\mathfrak{O}_{n-1} \subseteq \mathfrak{O}_{n-1}$. φ denotes the canonical map from $k[G]$ to $k[G/H]$ as in § 2, where H is the Galois group of the extension K/K_{n-1}. For any element α of K_{n-1}, we have $E\alpha = \varphi(E)\alpha$. From our inductive assumption, $\mathfrak{O}_{n-1}$ is an indecomposable $\mathfrak{o}[G/H]$-module, so that $\varphi(E) = 1$ or 0. Without loss of generality, we may assume $\varphi(E) = 1$. Since T is the identity map of $\mathfrak{O}_{n-1}$, $E - T \in \ker \varphi$. Put $E = T + E_1$. Let I be the set defined by

$$I = \{i \mid 0 \leqq i < p^n, (i, p) = 1\} .$$

Then, from Lemma 3, there exists a subset I_0 of the set I such that $E_1 = \sum_{i \in I_0} \varepsilon_i$, where ε_i is the primitive idempotent of $k[G]$ defined as in § 2. For $1 \leqq i < p^{n-1}$ with $(i, p) = 1$, let I_i be $I_i = \{i, i + p^{n-1}, \cdots, i + (p-1)p^{n-1}\}$. Now suppose $I_i \cap I_0 \neq I_i$. Let r be the number of elements in $I_i \cap I_0$. From the hypothesis, $I_i \cap I_0 \neq I_i$, $(r, p) = 1$. For the integer B_i defined before, it is easy to see that

$$\mathrm{val}\,(EB_i) = \mathrm{val}\left\{\Big(\sum_{\ell \in I_0 \cap I_i} \varepsilon_\ell\Big) B_i\right\} = \mathrm{val}\left(r \frac{A^i}{\pi^j}\right) .$$

By the definition of j, $\mathrm{val}\left(\frac{A^i}{\pi^j}\right) < 0$. Since $(r, p) = 1$, $\mathrm{val}\,(r) = 0$. Therefore we have $\mathrm{val}\,(EB_i) < 0$, which is a contradiction. Thus we have obtained $I_0 \supseteq I_i$ for each i with $1 \leqq i < p^{n-1}$ and $(i, p) = 1$. This implies $I_0 = I$. Then it follows from Lemma 3 that $E_1 = 1 - T$. Hence $E = 1$, and which completes the proof.

4.

In this section, we treat the case that k does not contain any primitive p^n-th root of 1. We use the same notations as in the previous sections. Then we have

THEOREM 2. *Suppose k does not contain any primitive p^n-th root θ of 1. Let K/k be a cyclic totally ramified extension of degree p^n. Then the ring $\mathfrak{O}$ of all integers in K is an indecomposable $\mathfrak{o}[G]$-module if and only if $m(b_1) < e$.*

Proof. Precisely from the same arguments as in the proof of Theorem 1, it is sufficient to prove that if $m(b_1) < e$, then $\mathfrak{O}$ is indecomposable. Now we assume $m(b_1) < e$. We also use induction on n as in the proof of Theorem 1. From Theorem 1 of [1], we obtain at once the result for $n = 1$. Assume the result holds for the fewer length than n. Then, we can write $E = T + E_1$ and $E_1 = \sum_{i \in I_0} \varepsilon_i$ in $k(\theta)[G]$. Let S be $S = \langle g^p \rangle$ as before. Since $\theta \notin k$, it follows from Lemma 4 that $E_1 \in k[S]$. Therefore E belongs to $k[S]$. Clearly S is the Galois group of the extension K/K_1, which contains $(n-1)$ intermediate fields. We see that b_2 is the first ramification number for K/K_1 (for example, see [2]). From Lemma 2 and our assumption $m(b_1) < e$, we have $m(b_2) < pe$.

Then, by the inductive assumption and Theorem 1, we can see that $\mathfrak{O}$ is an indecomposable $\mathfrak{O}_1[S]$-module. Thus we obtain $E = 1$, and this completes the proof.

Finally, from Theorem 1 and Theorem 2, we have the following theorem which is the main aim of this short paper.

THEOREM 3. *Let K/k be a cyclic totally ramified extension of degree p^n. Let b_1 be the first ramification number for K/k. Then the ring $\mathfrak{O}$ of all integers in K is an indecomposable $\mathfrak{o}[G]$-module if and only if $m(b_1) < e$.*

REFERENCES

[1] Y. Miyata, On the module structure of the ring of all integers of a $\mathfrak{p}$-adic number field, Nagoya Math. J. **54** (1974), 53–59.
[2] J. P. Serre, Corps Locaux, Paris, 1962.
[3] B. F. Wyman, Wildly ramified gamma extension, Amer. J. Math. **91** (1969), 135–152.

Faculty of Education
Shizuoka University