Y. Miyata
Nagoya Math. J.
Vol. 54 (1974), 53–59

ON THE MODULE STRUCTURE OF THE RING OF ALL INTEGERS OF A $\mathfrak{p}$-ADIC NUMBER FIELD

YOSHIMASA MIYATA

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 ramified extension of prime degree p with Galois group G. Then the ring $\mathfrak{O}$ of all integers of K is $\mathfrak{o}[G]$-module. The purpose of this paper is to give a necessary and sufficient condition for *$\mathfrak{o}[G]$-module $\mathfrak{O}$ to be indecomposable.*

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

1. In this section, we shall construct an arithmetical sequence of rational integers and study its properties. We begin with defining sequences $a_1^i, a_2^i, \cdots, a_{p-1}^i$ for $1 \leqq i \leqq p-1$. Sequences a_j^i are defined inductively by:

$$\begin{aligned}
&a_1^1 = 1,\ a_2^1 = 2, \cdots, a_{p-1}^1 = p-1\\
&a_1^2 = 0,\ a_2^2 = a_1^1,\ a_3^2 = a_1^1 + a_2^1, \cdots, a_{p-1}^2 = a_1^1 + a_2^1 + \cdots + a_{p-2}^1, \cdots,\\
&a_1^i = 0, \cdots, a_{i-1}^i = 0,\ a_i^i = a_{i-1}^{i-1},\ a_{i+1}^i = a_{i-1}^{i-1} + a_i^{i-1}, \cdots,\\
&a_{p-1}^i = a_{i-1}^{i-1} + a_i^{i-1} + \cdots + a_{p-2}^{i-1}, \cdots .
\end{aligned}$$

We evaluate a_j^i.

LEMMA 1.

$$a_j^i = \frac{\{j-(i-1)\}\{j-(i-2)\}\cdots j}{i!} \qquad \textit{for } 1 \leqq i \leqq j \leqq p-1 .$$

Proof. We use induction on i. The result is trivial for $i = 1$. Let $i > 1$, and suppose the result holds for $a_j^{i'}$ where $1 \leqq i' \leqq i-1$ and $i' \leqq j \leqq p-1$. Then we have

Received September 13, 1973.

$$a_j^i = a_{i-1}^{i-1} + \cdots + a_{j-1}^{i-1} = \frac{1}{(i-1)!}[\{(i-1)-(i-1-1)\}\cdots(i-1)$$
$$+ \cdots + \{(j-1)-(i-1-1)\}\cdots(j-1)]$$
$$= \frac{1}{(i-1)!}\left[\sum_{a=1}^{(j-1)-(i-2)}\left\{\prod_{b=0}^{i-2}(a+b)\right\}\right].$$

From the formula $\sum_{a=1}^{j}\{\prod_{b=0}^{i-1}(a+b)\} = 1/(i+1)\prod_{b=0}^{i}(j+b)$ ([5]), we obtain

$$a_j^i = \frac{1}{(i-1)!}\,\frac{1}{i}\prod_{b=0}^{i-1}\{j-(i-1)+b\}.$$

This proves the lemma.

We may observe that the above proof also yields the following lemma:

LEMMA 2. *$(a_i^i + a_{i+1}^i + \cdots + a_{p-1}^i)/p$ is an integer of the field of p-adic numbers for $1 \leqq i < p-1$.*

Now, let θ be a primitive p-th root of 1.

LEMMA 3. *$\theta^j - 1 = a_j^1(\theta-1) + \cdots + a_j^j(\theta-1)^j$ for $1 \leqq j \leqq p-1$.*

Proof. We use induction on j. The result is clear for $j=1$. Assume it holds $j \leqq j_0 - 1$. We shall prove that it holds for $j = j_0$ Then

$$(\theta^{j_0}-1)/(\theta-1) = a_{j_0}^1 + (\theta^{j_0-1}-1) + \cdots + (\theta-1)$$
$$= a_{j_0}^1 + (\theta-1)\left(\sum_{h=1}^{j_0-1}a_h^1\right) + \cdots + (\theta-1)^{j_0-1}a_{j_0-1}^{j_0-1}.$$

Hence by the definition of $a_{j_0}^i$ we have

$$\theta^{j_0} - 1 = a_{j_0}^1(\theta-1) + a_{j_0}^2(\theta-1)^2 + \cdots + a_{j_0}^{j_0}(\theta-1)^{j_0}.$$

2. Let K/k be a cyclic ramified extension of prime degree p. In this section, we shall evaluate valuations of some elements of K. Let Π and $\mathfrak{D}$ be a prime element of K and the different of K/k. Let e denote the absolute ramification index of k. Let $\mathfrak{D} = \mathfrak{O}\Pi^n$. We can write n in the form $n = pm + l$ with $0 \leqq l < p$. Let g be a generator of the Galois group G of K/k and c be the first ramification number of K/k. By the definition of c, we have $g(\Pi) = \Pi + u\Pi^{c+1}$, where u is a unit of K. As is well known,

$$(1) \qquad m \leqq e\,, \quad \text{and} \quad pm + l = (p-1)(c+1)\,.$$

Now, take any integer α of K. For α we define a sequence of $p-1$ integers $\alpha_0, \alpha_1, \cdots, \alpha_{p-2}$ inductively by:

$$\alpha_0 = \alpha,\ \alpha_1 = g(\alpha_0) - \alpha_0, \cdots, \quad \text{and} \quad \alpha_{p-2} = g(\alpha_{p-3}) - \alpha_{p-3} .$$

We shall evaluate the valuation of α_j. Let ν_k denote the valuation of $K(\nu_k(\Pi) = 1)$.

LEMMA 4. *Let* $a = \nu_k(\alpha)$. *Then* $\nu_k(\alpha_j) \geqq \min(a + jc, pm + 1, pe)$.

Proof. a can be written in the form $a = pq + r$ with $0 \leqq r < p$. Let (Π^{pm+1}, Π^{pe}) be the ideal generated by Π^{pm+1} and Π^{pe}. Since $e \geqq m$ and $pm + 1 < p(c + 1)$, we have

$$\begin{aligned} g(\Pi^a) &= g(\Pi^{pq+r}) = (\Pi + u\Pi^{c+1})^{pq+r} \\ &\equiv \Pi^{pq+r}(1 + u\Pi^c)^r \qquad \text{mod.}\ (\Pi^{pm+1}, \Pi^{pe}) . \end{aligned}$$

Put $(1 + u\Pi^c)^r = 1 + ru'\Pi^c$. Hence

$$(2) \qquad g(\Pi^a) \equiv \Pi^a(1 + ru'\Pi^c) \qquad \text{mod.}\ (\Pi^{pm+1}, \Pi^{pe}) .$$

Now let $j = 1$. We can write $\alpha = U\Pi^a$, where U is a unit of $\mathfrak{O}$. Then, by (2), we have

$$\begin{aligned} \alpha_1 &= g(\alpha) - \alpha = g(U)g(\Pi^a) - U\Pi^a \\ &\equiv \Pi^a\{g(U)(1 + ru'\Pi^c) - U\} \qquad \text{mod.}\ (\Pi^{pm+1}, \Pi^{pe}) . \end{aligned}$$

We have $g(U) = U + v\Pi^{c+1}$, where v is an integer of K. Hence

$$\alpha_1 \equiv \Pi^{a+c}\{ru'U + v\Pi + ru'\Pi^{c+1}) \qquad \text{mod.}\ (\Pi^{pm+1}, \Pi^{pe}) .$$

Therefore, we obtain the inequality for $j = 1$, and simulately, we obtain it also for $j > 1$.

Now, let k_0 be the field $k(\theta)$ and K_0 the field $K(\theta)$. Let e_0 denote the degree of k_0/k. Since the extension k_0/k is tamely ramified, we have $k_0 \cap K = k$. Therefore there exists a unique element g_0 of the Galois group G_0 of K_0/k_0 such that for any element α of K

$$(3) \qquad g_0(\alpha) = g(\alpha) \ \ ([3]) .$$

Let $\mathfrak{O}_0$ be the ring of all integers of K_0 and define the element E of the group ring $k_0[G]$ by

$$E = \sum_{j=1}^{p} \theta^{j-1} g_0^{p-j} .$$

https://doi.org/10.1017/S0027763000024582 Published online by Cambridge University Press

In the following we shall obtain a congruence for $E\alpha$ (where α is an integer of K as before). Keeping the same notations as in preceding Lemma 4, define α_j^i by $\alpha_j^i = g_0^{i-1}(\alpha_j)$. We obtain the following lemma.

LEMMA 5. *Let $E, g_0, \alpha, \alpha_j^i$ be as above. Let p' be $p' = \max(p-2, 1)$. Then*

$$E\alpha \equiv \left(\sum_{j=1}^{p} g_0^{j-1}\right)\alpha + \sum_{i=1}^{p'} (\theta-1)^i \alpha_{p-i-1} \quad \text{mod. } \mathfrak{O}_0 p .$$

Proof. We immediately obtain the result for $p=2$, and so suppose hereafter $p \geqq 3$. Then we have $p' = p-2$ and

$$(E - \sum g_0^{j-1})\alpha \equiv \sum_{j=1}^{p-2} (\theta^j - 1)\left(\sum_{h=1}^{p-j-1} \alpha_1^h\right) \quad \text{mod. } \mathfrak{O}_0 p .$$

Then, by Lemma 3, we have

$$(E - \sum g_0^{j-1})\alpha \equiv \sum (\theta-1)^i \left\{\sum_{j=i}^{p-2} a_j^i \left(\sum_{h=1}^{p-j-1} \alpha_1^h\right)\right\} \quad \text{mod. } \mathfrak{O}_0 p .$$

First we investigate the case $i=1$. By the definition of α_j^2,

$$\sum_{j=1}^{p-2} a_j^1 \left(\sum_{h=1}^{p-j-1} \alpha_1^h\right) = \sum_{h=1}^{p-2} \left(\sum_{j=1}^{p-h-1} a_j^1\right)\alpha_1^h = \sum_{h=1}^{p-2} a_{p-h}^2 \alpha_1^h .$$

Put $p-h=j$. Then

$$\begin{aligned} &= \sum_{j=2}^{p-1} a_j^2 \alpha_1^{p-j} \\ &= \sum_{j=2}^{p-2} a_j^2 (\alpha_1^{p-j} - \alpha_1^1) + \left(\sum_{j=2}^{p-1} a_j^2\right)\alpha_1^1 \\ &= \sum_{j=2}^{p-2} a_j^2 \left(\sum_{h=1}^{p-j-1} \alpha_2^h\right) + \left(\sum_{j=2}^{p-1} a_j^2\right)\alpha_1^1 \end{aligned}$$

By Lemma 2, $(\sum a_j^2)\alpha_1^1 \in \mathfrak{O}_0 p$. Therefore

$$\sum_{j=1}^{p-2} a_j^1 \left(\sum_{h=1}^{p-j-1} \alpha_1^h\right) \equiv \sum_{j=2}^{p-2} a_j^2 \left(\sum_{h=1}^{p-j-1} \alpha_2^h\right) \quad \text{mod. } \mathfrak{O}_0 p .$$

Repeating this process, we obtain

$$\sum_{j=1}^{p-2} a_j^1 \left(\sum_{h=1}^{p-j-1} \alpha_1^h\right) \equiv \sum_{j=i}^{p-2} a_j^i \left(\sum_{h=1}^{p-j-1} \alpha_i^h\right) \quad \text{mod. } \mathfrak{O}_0 p .$$

Then,

https://doi.org/10.1017/S0027763000024582 Published online by Cambridge University Press

$$\begin{aligned}\sum a_j^1\left(\sum \alpha_1^h\right) &\equiv \sum a_j^i\left(\sum \alpha_i^h\right)\\ &\equiv \sum_{h=1}^{p-i-1}\left(\sum_{j=i}^{p-h-1} a_j^i\right)\alpha_i^h\\ &\equiv \sum_{h=1}^{p-i-1} a_{p-h}^{i+1}\alpha_i^h\end{aligned}$$

Put $p - h = j$.

$$\equiv \sum_{j=i+1}^{p-1} a_j^{i+1}\alpha_i^{p-j}$$

$$\equiv \sum_{j=i+1}^{p-2} a_j^{i+1}(\alpha_i^{p-j} - \alpha_i^1) + \left(\sum_{j=i+1}^{p-1} a_j^{i+1}\right)\alpha_i^1 \qquad \operatorname{mod} \mathfrak{O}_0 p\ .$$

Using Lemma 2 again, we obtain $(\sum a_j^{i+1})\alpha_i^1 \in \mathfrak{O}_0 p$. Hence

$$\sum a_j^1\left(\sum \alpha_1^h\right) \equiv \sum_{j=i+1}^{p-2} a_j^{i+1}\left(\sum_{h=1}^{p-j-1} \alpha_{j+1}^h\right) \qquad \operatorname{mod.} \mathfrak{O}_0 p\ .$$

Therefore we have

$$(\theta - 1)\left\{\sum a_j^1\left(\sum a_1^h\right)\right\} \equiv (\theta - 1)a_{p-2}^{p-2}a_{p-2}^1 \qquad \operatorname{mod.} \mathfrak{O}_0 p\ .$$

Applying the same arguments, for $i \geqq 2$ we have

$$(\theta - 1)^i\left\{\sum_{j=i}^{p-2} a_j^i\left(\sum_{h=1}^{p-j-1} \alpha_1^h\right)\right\} \equiv (\theta - 1)^i a_{p-2}^{p-2}a_{p-i-1}^1 \qquad \operatorname{mod.} \mathfrak{O}_0 p\ .$$

From $a_{p-2}^{p-2} = 1$, for $1 \leqq i \leqq p-2$ we have

$$(\theta - 1)^i\left\{\sum a_j^i\left(\sum \alpha_1^h\right)\right\} \equiv (\theta - 1)^i\alpha_{p-i-1}^1 \qquad \operatorname{mod.} \mathfrak{O}_0 p\ .$$

The lemma is proved.

3. We shall use the same notations as in the previous section. Let π be a prime element of k, and write $\mathfrak{D} = \mathfrak{O}\Pi^{pm+l}$ as before. At first, we observe that there is a prime element Π' such that $(\sum_{j=1}^{p} g^{j-1})\Pi'^{p-l-1} \in \mathfrak{o}\pi^m$ and $\notin \mathfrak{o}\pi^{m+1}$ ([2]). Therefore we may have

$$\nu_k\left\{\left(\sum g^{j-1}\right)\Pi^{p-l-1}\right\} = pm\ . \tag{4}$$

Next, from the result of E. Maus ([4] (3.19)), we have the following lemma:

LEMMA 6. *The first ramification number c_0 of the extension K_0/k_0 is $e_0 c$.*

Finally, we obtain the next theorem which is the aim of this paper.

THEOREM 1. *Let K/k be a cyclic ramified extension of prime degree p, and e be the absolute ramification index of k. Let $\mathfrak{O}, \mathfrak{o}, G$, and m be as stated before. Then $\mathfrak{O}$ is an indecomposable $\mathfrak{o}[G]$-module if and only if $m < e$.*

This is obviously equivalent with the following theorem that we shall prove in the following:

THEOREM 2. *Let $K/k, \mathfrak{O}, \mathfrak{o}, G, e, m.$ be as in Theorem 1. Then $\mathfrak{O}$ is decomposable if and only if $m = e$.*

Proof. At first we suppose $m = e$. As is well known, $(\sum_{j=1}^{p} g^{j-1})\mathfrak{O} \subseteq \mathfrak{o}\pi^m$ (*e.g.* [1]). Since $m = e$, then $(\sum g^{j-1})\mathfrak{O} \subseteq \mathfrak{o}p$. Therefore $\mathfrak{O}$ is decomposable.

Conversely, we suppose that $\mathfrak{O}$ is decomposable. Then there are $\mathfrak{o}[G]$-submodules $\mathfrak{O}_1$ and $\mathfrak{O}_2$ of $\mathfrak{O}$ such that

$$\mathfrak{O} = \mathfrak{O}_1 \oplus \mathfrak{O}_2 .$$

As the $k[G]$-module $K(= k\mathfrak{O})$ is isomorphic to $k[G]$, we have

$$k\mathfrak{O}_1 \cong \sum_{\{\chi_j\}} \left\{ \frac{\sum_{i=1}^{p-1} \chi_j(g^{-i})g^i}{p} \right\} k\mathfrak{O} ,$$

where $\{\chi_j\}$ are irreducible k-character of G. Then we see that the element $\sum_{\{\chi_j\}} \{\sum \chi_j(g^{-i})g^i\}/p$ is an $\mathfrak{o}[G]$-endomorphism of $\mathfrak{O}$. Hence

$$(5) \qquad \sum_{\{\chi_j\}} \{\sum \chi_j(g^{-i})g^i\}\mathfrak{O} \subseteq \mathfrak{O}p .$$

Now χ_j is a direct sum of irreducible k_0-character χ_{jr}:

$$\chi_j = \chi_{j1} + \cdots + \chi_{jr_j} .$$

Then $\sum \chi_j(g^{-i})g^i/p$ is a sum of central idempotents $\sum \chi_{jr}(g^{-i})g^i/p$. Let $E_{jr} = \sum_{i=0}^{p-1} \chi_{jr}(g^{-i})g^i$. Then we have

$$(6) \qquad \sum_{\{\chi_j\}} (\sum \chi_j(g^{-i})g^i) = \sum_{j,r} E_{jr} .$$

Let s denote the number of the set E_{jr} (i.e. $s = \sum_j r_j$). By Lemma 5 and (3), we have $(\sum E_{jr})\Pi^{p-l-1} \equiv s(\sum g^{j-1})\Pi^{p-l-1} + \sum_{\{\theta_{jr}\}} \{\sum_{i=1}^{p'} (\theta_{jr} - 1)^i \alpha_{p-i-1}\}$ mod. $\mathfrak{O}_0 p$, where $\{\theta_{jr}\}$ are $\chi_{jr}(g^{-1})$. From (5) and (6),

$$(7) \qquad s(\sum g^{j-1})\Pi^{p-l-1} + \sum_{\{\theta_{jr}\}} (\sum (\theta_{jr} - 1)^i \alpha^1_{p-i-1}) \equiv 0 \qquad \text{mod. } \mathfrak{O}_0 p .$$

https://doi.org/10.1017/S0027763000024582 Published online by Cambridge University Press

Furthermore, it follows from Lemma 4 that

$$\nu_k\{\alpha^1_{p-i-1}\} \geqq \min(p-l-1+c(p-i-1), pm+1, pe)\ .$$

Let ν_{k_0} denote the valuation of K_0 (i.e. $\nu_{k_0}(\Pi)=e_0$). Then

(8) $$\nu_{k_0}\{(\theta-1)^i\alpha^1_{p-i-1}\} \geqq \min(N, pme_0+1, pee_0)\ ,$$

where

$$N=\{p-l-1+c(p-i-1)\}e_0+\frac{pee_0}{p-1}i\ .$$

As $(c+1)(p-1)=pm+l$, we have $(p-1)c+p-l-1=pm$. Here we note that

$$\begin{aligned} N &= \{(p-l-1)+(p-1)c\}e_0+\left(\frac{pee_0}{p-1}-ce_0\right)i \\ &= pme_0+\left(\frac{pee_0}{p-1}-ce_0\right)i\ . \end{aligned}$$

First, we consider the case that $pee_0/(p-1)=ce_0$. Then, from (1), we obtain $m=e$. Next, we consider the case that $pee_0/(p-1)>ce_0$. Then we have $N>pme_0$. Therefore, by (7) and (8),

(9) $$\nu_{k_0}\{s(\sum g^{j-1})\Pi^{p-l-1}\} \geqq pee_0\ .$$

As $\mathfrak{O}_2 \neq \{0\}$, $1 \leqq s < p$. Then s is a unit of $\mathfrak{O}_0$. It follows from (4) and (9) that $pme_0 \geqq pee_0$. This implies $m=e$, and the proof of the theorem is completed.

References

[1] E. Artin and J. Tate, Class Field Theory, Benjamin, New York, 1967.

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

[3] N. Bourbaki, Èléments de Mathématique Algèbre Chap. 4 et 5, Hermann, Paris, 1959.

[4] E. Maus, Arithmetisch disjunkte Körper, J. reine angew. Math. **226** (1967), 184–203.

[5] Sūgaku Jiten (Mathematical dictonary), Iwanami, Tokyo, 1968.

Faculty of Education, Shizuoka University

https://doi.org/10.1017/S0027763000024582 Published online by Cambridge University Press