Y. Miyata
Nagoya Math. J.
Vol. 111 (1988), 165-171

ON THE ISOMORPHISM CLASS OF THE RING OF ALL INTEGERS OF A CYCLIC WILDLY RAMIFIED EXTENSION OF DEGREE p II

YOSHIMASA MIYATA

Let k be an algebraic number field with the ring of integers $\mathfrak{o}_k = \mathfrak{o}$ and let G be a cyclic group of order p, an odd prime. Let K/k be a cyclic extension of degree p with the ring of integers $\mathfrak{O}_K$. Then, $\mathfrak{O}_K$ is an $\mathfrak{o}G$-module. In the case that K/k is tamely ramified, L. McCulloh [3] proved that the subset $R(\mathfrak{o}G)$ of the classes $\mathrm{cl}(\mathfrak{O})$ of the rings $\mathfrak{O}$ in the class group $\mathrm{Cl}^0(\mathfrak{o}G)$ is equal to the subgroup $\mathrm{Cl}^0(\mathfrak{o}G)^J$ generated by all c^a, $c \in \mathrm{Cl}^0(\mathfrak{o}G)$, $a \in J$, where J denotes the Stickelberger ideal (for the definitions, see below).

Now, in the previous paper [4], we studied the case that K/k is wildly ramified. Let $\Gamma(\mathfrak{O})$ be the genus containing $\mathfrak{O}$. From H. Jacobinski's results [2], we know that there exists a one-to-one corresponding between the isomorphism classes in $\Gamma(\mathfrak{O})$ and the elements of the class group M (for the definition, see also below). The group Δ of automorphisms of G acts on M and so M^J can be defined as in the group $\mathrm{Cl}^0(\mathfrak{o}G)$. In [4], we defined the invariant $N(\mathfrak{O})$ which is an element of M, and showed that $N(\mathfrak{O}) \in M^J$ (cf. [4, Theorem 4]). The purpose of this paper is to prove that the subset $R_w(\mathfrak{o}G)$ of invariants $N(\mathfrak{O})$ of the rings $\mathfrak{O}$ in the wildly ramified extensions K/k of degree p is equal to M^J (Theorem 3).

Let g be a fixed generator of G and ζ be a primitive p-th root of unity. Throughout this paper, we assume that k contains ζ. In Section 1, we shall recall the definitions given in [4], and prove Theorem 1 which is the modification of Theorem 4 of [4]. In Section 2, we shall recall L. McCulloh's results [3] and define a Δ-homomorphism ψ from $\mathrm{Cl}^0(\mathfrak{o}G)$ onto M. This homomorphism ψ plays the important role in the proof of Theorem 3 that $R_w(\mathfrak{o}G) = M^J$, which is proved in Section 3.

Received February 16, 1987.

§ 1.

Let K/k be a cyclic wildly ramified extension of degree p and let G be a cyclic group of order p. We can view G as Galois group $G(K/k)$ of K/k. In this section, we call definitions and Theorem 4 of [4]. For a prime ideal $\mathfrak{p}$ of $\mathfrak{o}$, let $k_{\mathfrak{p}}$ be the $\mathfrak{p}$-adic completion of k with the valuation ring $\mathfrak{o}_{\mathfrak{p}}$, and let $K_{\mathfrak{p}} = k_{\mathfrak{p}} \otimes_k K$ and $\mathfrak{O}_{\mathfrak{p}} = \mathfrak{o}_{\mathfrak{p}} \otimes_{\mathfrak{o}} \mathfrak{O}$. Denote by $\pi(\mathfrak{p})\,(=\pi)$ and $e(\mathfrak{p})\,(=e)$ a prime element and the absolute ramification index of $k_{\mathfrak{p}}$, respectively. We denote by $c(\mathfrak{p})$ the ramification number of $K_{\mathfrak{p}}/k_{\mathfrak{p}}$. Then, it is well known that $-1 \leqq c(\mathfrak{p}) \leqq pe(\mathfrak{p})/(p-1)$. Let $P_1 = P_1(K)\,(P_0 = P_0(K))$ be a product $\prod \mathfrak{p}$ of $\mathfrak{p}$ such that $\mathfrak{p}|(p)$ and $0 < c(\mathfrak{p}) < pe(\mathfrak{p})/(p-1) - 1$ $(c(\mathfrak{p}) = -1)$, respectively, and let $P = P_0 P_1$. As in [4], define integers $d(\mathfrak{p})$ by

$$d(\mathfrak{p}) = \begin{cases} pe(\mathfrak{p})/(p-1) - c(\mathfrak{p}) & \text{for } \mathfrak{p} | P_1 \\ pe(\mathfrak{p})/(p-1) & \text{for } \mathfrak{p} | P_0 \, , \end{cases}$$

Moreover, for $0 \leqq i < p$, integers $m_i(\mathfrak{p})$ are defined by

$$m_i(\mathfrak{p}) = [id(\mathfrak{p})/p] \, ,$$

where $[x]$ denotes an integer with $[x] \leqq x < [x] + 1$.

Now, we define $\mathfrak{o}_{\mathfrak{p}}G$-modules $L_{\mathfrak{p}}$ and an $\mathfrak{o}G$-module L. Let E_i be an primitive idempotent of kG with $gE_i = \zeta^i E_i$ for $0 \leqq i < p$. For $0 < i < p$ and $\mathfrak{p} | P_1$, let

$$a_i(\mathfrak{p}) = \pi(\mathfrak{p})^{-m_i} \left(\sum_{j=0}^{i} \binom{i}{j} (-1)^{i-j} E_j \right)$$

and $a_0(\mathfrak{p}) = 1$. We define $\mathfrak{o}_{\mathfrak{p}}G$-modules $L_{\mathfrak{p}}$ as follows:

(a) For $\mathfrak{p} \nmid P$, $L_{\mathfrak{p}} = \mathfrak{o}_{\mathfrak{p}} \otimes (\sum \mathfrak{o} E_i)$.

(b) For $\mathfrak{p} | P_1$, $L_{\mathfrak{p}} = \sum \mathfrak{o}_{\mathfrak{p}} a_i(\mathfrak{p})$.

(c) For $\mathfrak{p} | P_0$, $L_{\mathfrak{p}} = (1/p)\mathfrak{o}_{\mathfrak{p}} G$.

Then, it is easily known that there exists an $\mathfrak{o}G$-module L in kG such that $\mathfrak{o}_{\mathfrak{p}} \otimes_{\mathfrak{o}} L = L_{\mathfrak{p}}$ for each $\mathfrak{p}$ (for example, see [5, p. 70 (5.3) Theorem]). Denote by $\Gamma(L)$ a genus including L. By the definition of L, we have $\mathfrak{O} \in \Gamma$ (cf. [4, Lemma 7]).

Next, we define a class group M. Let χ be a character of G with $\chi(g) = \zeta$ and $X = \{\chi, \chi^2, \cdots, \chi^{p-1}\}$. Let I be the group of fractional ideals of k relatively prime to P and let $\mathrm{Map}(X, I)$ be the group of functions from X into I. As in [3], an automorphism δ in $\Delta\,(=\mathrm{Aut}\, G)$ acts on X and $\mathrm{Map}(X, I)$ as follows:

https://doi.org/10.1017/S0027763000001070 Published online by Cambridge University Press

(1) $\chi^{i\delta}(g) = \chi^i(g^{\delta^{-1}})$ and $n^\delta(\chi^i) = n(\chi^{i\delta^{-1}})$, $n \in \mathrm{Map}(X, I)$.

Let $Z\Delta$ be the group ring over the ring of integers Z and an element θ of $Z\Delta$ be

$$\theta = \sum_{\delta \in \Delta} t(\delta)\delta^{-1},$$

where $g^\delta = g^{t(\delta)}$ with $1 \leqq t(\delta) < p$. Let the Stickelberger ideal J of $Z\Delta$ be

$$J = (p^{-1}\theta \cdot Z\Delta) \cap Z\Delta .$$

An element a of kG is written in the form;

$$a = a_0E_0 + a_1E_1 + \cdots + a_{p-1}E_{p-1} .$$

From [4, Lemmas 4 and 5], we have

Lemma 1. *Let* $\mathrm{Aut}\, L_\mathfrak{p}$ *be the group of* $\mathfrak{o}_\mathfrak{p}G$*-automorphisms of* $L_\mathfrak{p}$. *Then, if* $a \in \mathrm{Aut}\, L_\mathfrak{p}$ *for each* $\mathfrak{p} | P$, $a_0, \cdots, a_{p-1}$ *are* P*-units.*

Let H be defined by

$$H = \{a \in kG | a \in \mathrm{Aut}\, L_\mathfrak{p} \text{ for } \mathfrak{p} | P \text{ and } a_0 = 1\},$$

and so by [4, Corollary 2], H is Δ-invariant. Then, we can define a Δ-homomorphism f from H into $\mathrm{Map}(X, I)$ such that

$$f(a)(\chi^i) = a_i\mathfrak{o} .$$

The class group M is defined by

$$M = \mathrm{Map}(X, I)/f(H) .$$

Lemma 2. *For* $n \in \mathrm{Map}(X, I)$, *let* $\mathrm{cl}\, n$ *denote a natural image of* n *in* M. *Then, there exists an element* m *of* $\mathrm{Map}(X, I)$ *such that* $(m(\chi^i), (p)) = 1$ *and* $\mathrm{cl}\, m = \mathrm{cl}\, n$.

Proof. Let Λ be a left order of L:

$$\Lambda = \{a \in kG | aL \subseteq L\} .$$

Let an ideal $\mathfrak{f}$ of $\mathfrak{o}$ be the order ideal of the factor module $(\sum \mathfrak{o}E_i)/\Lambda$ (for the definition, see [5, p. 49]). By the definition of L, the set of prime divisors of $\mathfrak{f}$ is the set of prime divisors of P. Let S be

$$S = \{a \in kG | aE_i \equiv 1(\mathfrak{f}) \text{ for } 0 < i < p\} .$$

Then, by H. Jacobinski's results [2, p. 8], we have $H \supseteq S$. Every coset of the ray $R(\mathfrak{f})$ mod $\mathfrak{f}$ in I contains infinite many primes (for example, see [4, p. 215]). Thus, we can choose ideals $m(\chi^i)$ such that $m(\chi^i)$ and $n(\chi^i)$ be in the same coset of $R(\mathfrak{f})$ in I and $(m(\chi^i),(p)) = 1$. Since $H \supseteq S$, cl $n =$ cl m, which completes the proof of Lemma 2.

Finally, we remember the definition of $N(\mathfrak{O})$. From [4, Lemma 1], there exists an element α of $\mathfrak{O}$ such that $\alpha^p \in \mathfrak{o}$ and for $\mathfrak{p} | P$,

$$(2) \qquad \alpha^p \equiv 1\, (\pi(\mathfrak{p})^{d(\mathfrak{p})})\,.$$

Then, for $1 \leqq i < p$,

$$(3) \qquad (\alpha^{ip}) = \mathfrak{b}_i \mathfrak{c}_i^{-p}\,,$$

where $\mathfrak{b}_i$ is a p-power free integral ideal and $\mathfrak{c}_i$ is a fractional ideal. By (2), $(\mathfrak{c}_i, P) = 1$ and so an element $n(\mathfrak{O})$ of Map(X, I) is defined by $n(\mathfrak{O})(\chi^i) = \mathfrak{c}_i$. Let $N(\mathfrak{O})$ be the natural image cl$(n(\mathfrak{O}))$ of $n(\mathfrak{O})$ in M.

From [4, Theorem 4], we have the following theorem.

THEOREM 1. *Let K/k be a wildly ramified extension of degree p with the discriminant* dis(K/k). *Let L and M be as above, and let J be the Stickelberger ideal in $Z\Delta$. Then,*

(i) *$N(\mathfrak{O}) \in M^J$ and*

(ii) *for given ideal $\mathfrak{a}$ of $\mathfrak{o}$ with $(\mathfrak{a}, (p)) = 1$, there exists a wildly ramified extension K'/k of degree p such that $\mathfrak{O}' \in \Gamma(L) = \Gamma(\mathfrak{O})$ and* $(\text{dis}(K'/k), \mathfrak{a}) = 1$.

Proof. (i) of Theorem 1 is Theorem 4 of [4] and hence its proof is done. Next, we prove (ii). Taking sufficiently large integers $n(\mathfrak{p})$ for $\mathfrak{p} | \mathfrak{a}(p)$, we choose an element b of $\mathfrak{o}$ such that for $\mathfrak{p} | (p)$, $b \equiv \alpha^p(\pi(\mathfrak{p})^{n(\mathfrak{p})})$ and for $\mathfrak{p} | \mathfrak{a}$,

$$(4) \qquad b \equiv 1(\pi(\mathfrak{p})^{n(\mathfrak{p})})\,.$$

Let $\beta = \sqrt[p]{b}$ and $K' = k(\beta)$. Then, we see that for $\mathfrak{p} | (p)$, the ramification number of K'/k is equal to the ramification number of K/k. Thus, by [4, Corollary 1], $\mathfrak{O}' \in \Gamma(L)$. As in (3), let $(\beta^p) = \mathfrak{b}\mathfrak{c}^{-p}$. Then, if $\mathfrak{p} | \text{dis}(K'/k)$ and $(\mathfrak{p}, (p)) = 1$, $\mathfrak{p}$ is a prime divisor of $\mathfrak{b}$ (for example, see [1, p. 91 Lemma 5]). By (4), $(\mathfrak{b}, \mathfrak{a}) = 1$ and so $(\text{dis}(K'/k), \mathfrak{a}) = 1$, which completes the proof of Theorem 1.

§ 2.

In this section, we recall L. McCulloh's results [3], Let $X' = \{\chi^0\} \cup X$,

https://doi.org/10.1017/S0027763000001070 Published online by Cambridge University Press

and I' be the group of fractional ideals of $\mathfrak{o}$ relatively prime to (p). Let $\mathfrak{o}_P$ be the semilocalisation of $\mathfrak{o}$ at p, and denote by $u(\mathfrak{o}_P G)$ the group of units of the ring $\mathfrak{o}_p G$. We define a homomorphism f from $u(\mathfrak{o}_p G)$ into Map (X', I') by

$$f(a)(\chi^i) = \chi^i(a)\mathfrak{o}\,.$$

Then, the class group Cl $(\mathfrak{o}G)$ of $\mathfrak{o}G$ is isomorphic to the factor group Map $(X', I')/f(u(\mathfrak{o}_p G))$. We extend an element n of Map (X, I') to an element of Map (X', I') by setting $n(\chi^0) = \mathfrak{o}$, and hence we can view Map (X, I') as a subgroup of Map (X', I'). Let ϕ be the natural homomorphism from Map (X, I') into Map $(X', I')/f(u(\mathfrak{o}_p G))$. Then,

$$\operatorname{Ker}\phi = \{f(a)\,|\,a \in u(\mathfrak{o}_p G) \text{ and } aE_0 \text{ is a unit of } \mathfrak{o}\}\,.$$

By [3, (2.3.2) Proposition], we have $\phi(\text{Map}\,(X, I')) = \text{Cl}^0(\mathfrak{o}G)$. Let T be a subgroup of $u(\mathfrak{o}_p G)$ consisting of elements a in $u(\mathfrak{o}_p G)$ with $aE_0 = 1$. Then, clearly, $f(T) = \operatorname{Ker}\phi$.

Lemma 3. *Let T be as above and H be as in Section* 1. *Then, $T \subseteq H$.*

Proof. An element of T is clearly an automorphism of L_p for each $\mathfrak{p}|P$, and so $T \subseteq H$ by the definition of H.

Now, noting $I' \subseteq I$, we have a Δ-homomorphism ψ' from Map (X, I') into Map (X, I). Then, it follows that ψ' induces a Δ-homomorphism ψ from $\text{Cl}^0(\mathfrak{o}G)$ into M since T and H are Δ-groups. Then, we have

Lemma 4. $\psi(\text{Cl}^0(\mathfrak{o}G)) = M$.

Proof. By Lemma 2, for $\text{cl}\,n \in M$, there exists an element m of Map (X, I) such that $(m(\chi^i), (p)) = 1$ and $\text{cl}\,n = \text{cl}\,m$ in M. Then, $m \in$ Map (X, I') and so $\text{cl}\,n = \psi(\text{cl}\,m) \in \psi(\text{Cl}^0(\mathfrak{o}G))$.

Since ψ is a Δ-homomorphism, we have

Corollary 1. $\psi(\text{Cl}^0(\mathfrak{o}G)^J) = M^J$.

We conclude this section with stating L. McCulloh's Theorem [3, (1.3.1) Theorem].

Theorem 2. *Let G be a cyclic group of order p, and J be the Stickelberger ideal. Define a subset $R(\mathfrak{o}G)$ of $\text{Cl}^0(\mathfrak{o}G)$ by*

$$R(\mathfrak{o}G) = \{\text{cl}\,(\mathfrak{O}_K)\,|\,K \text{ runs over the set of tame extensions of degree } p\}\,.$$

Then, $R(\mathfrak{o}G) = \mathrm{Cl}^0(\mathfrak{o}G)^J$. *Moreover, given* $m \in \mathrm{Cl}^0(\mathfrak{o}G)^J$ *and an ideal* $\mathfrak{a}$ *of* $\mathfrak{o}$, *there exists a tame extension* K/k *such that* $(\mathrm{dis}\,(K/k), \mathfrak{a}) = 1$ *and* $\mathrm{cl}\,(\mathfrak{O}) = m$.

§ 3.

In this section, we prove Theorem 3, which is the aim of this paper.

THEOREM 3. *Let* G *be a cyclic group of order* p *and* K *be a wildly ramified extension of degree* p. *Let* L *and* $\Gamma(L)(=\Gamma(\mathfrak{O}))$ *be as in Section* 1. *Define a subset* $R_w(\mathfrak{o}G)$ *of* M *by*

$$R_w(\mathfrak{o}G) = \{N(\mathfrak{O}') \mid \mathfrak{O}' \text{ is the ring of a wildly ramified extension } K'/k \text{ of degree } p \text{ with } \mathfrak{O}' \in \Gamma(L)\}.$$

Then, $R_w(\mathfrak{o}G) = M^J$. *Moreover, given* $m \in M^J$ *and an ideal* $\mathfrak{a}$ *of* $\mathfrak{o}$ *with* $(\mathfrak{a}, (p)) = 1$, *there exists a wildly ramified extension* K/k *such that* $(\mathrm{dis}\,(K/k), \mathfrak{a}) = 1$ *and* $N(\mathfrak{O}) = m$.

Proof. By Theorem 1, we have $R_w(\mathfrak{o}G) \subseteq M^J$. In the following, we have the existence of such a extension K/k as above. By (ii) of Theorem 1, there exists a wildly ramified extension K'/k such that $(\mathrm{dis}\,(K'/k), \mathfrak{a}) = 1$ and $\mathfrak{O}' \in \Gamma(L)$. Let α' be an element of $\mathfrak{O}'$ satisfying the congruences (2). Then, as in (3), we have

$$(\alpha'^{ip}) = \mathfrak{b}_i' \mathfrak{c}_i'^{-p} \qquad \text{for } 1 \leqq i < p\,.$$

As shown in the proof of Theorem 1, $(\mathfrak{b}_i', \mathfrak{a}) = 1$. Let $n = N(\mathfrak{O}')$ and $m' = n^{-1}m$ in M. Since $n \in M^J$ by Theorem 1 (i), we have $m' \in M^J$. Then, by Corollary 1, for some $\mathrm{cl}\,(\mathfrak{O}'') \in \mathrm{Cl}^0(\mathfrak{o}G)^J$ $\psi(\mathrm{cl}\,(\mathfrak{O}'')) = m'$. By Theorem 2, $\mathfrak{O}''$ can be chosen so that the discriminant of $k\mathfrak{O}''$ is relatively prime to the product $\mathfrak{b}$ of $\mathfrak{a}, \mathfrak{b}_1', \cdots, \mathfrak{b}_{p-1}'$. Moreover, as shown in the proof of [3, (4.2.1) Theorem], there exists an element β of $\mathfrak{O}''$ such that $\beta^p \equiv 1\ ((\zeta-1)^p)$. Let

$$(\beta^{ip}) = \mathfrak{b}_i \mathfrak{c}_i^{-p}\,,$$

where $\mathfrak{b}_i$ is p-power free, and so $(\mathfrak{b}_i, \mathfrak{b}) = 1$ because $(\mathrm{dis}\,(k\mathfrak{O}''/k), \mathfrak{b}) = 1$. Ideals $\mathfrak{c}_i$ define an element c of $\mathrm{Map}\,(X, I')$ by $c(\chi^i) = \mathfrak{c}_i$. By [3, (3.2.2) Theorem 3], $\mathrm{cl}\,(\mathfrak{O}'') = \mathrm{cl}\, c$, and hence

$$m = \psi(\mathrm{cl}\, c) N(\mathfrak{O}')\,. \tag{5}$$

Now, let $F = k(\alpha'\beta)$, and then F is clearly the extension of degree p over k. The action of g on $\alpha'\beta$ is defined by $g(\alpha'\beta) = \zeta\alpha'\beta$. Since $k(\beta)/k$ is tamely ramified, the ramification number $c'(\mathfrak{p})$ of F/k is equal to the ramification number $c(\mathfrak{p})$ of K/k for $\mathfrak{p}|(p)$. Therefore, by [4, Corollary 1], the ring $\mathfrak{O}_F$ of all integers in F belongs to the genus $\Gamma(L)$. We have

$$(\alpha'\beta)^{pi} = \mathfrak{b}_i'\mathfrak{b}_i(\mathfrak{c}_i'\mathfrak{c}_i)^{-p}$$

and $\mathfrak{b}_i'\mathfrak{b}_i$ is p-power free because $\mathfrak{b}_i'$ and $\mathfrak{b}$ are p-power free with $(\mathfrak{b}_i', \mathfrak{b}_i) = 1$. Then, ideals $\mathfrak{c}_i'$, $\mathfrak{c}_i$ define an element $n(\mathfrak{O}_F)$ of Map(X, I) by $n(\mathfrak{O}_F)(\chi^i) = \mathfrak{c}_i'\mathfrak{c}_i$, and so $n(\mathfrak{O}_F) = c\cdot n(\mathfrak{O}')$. By the definition of $N(\mathfrak{O})$ and (5), we have $m = N(\mathfrak{O}_F)$, which accomplishes the proof of Theorem 3.

References

[1] J. W. S. Cassels and A. Fröhlich, "Algebraic Number Theory", Academic Press, London/New York, 1967.

[2] H. Jacobinski, Genera and decompositions of lattices, Acta Math., **121** (1968), 1–29.

[3] L. R. McCulloh, A Stickelberger condition on Galois module structure for Kummer extensions of prime degree, in "Algebraic number fields", Proc. Durham Symp., Academic Press, London/New York, 1977, 561–588.

[4] Y. Miyata, On the isomorphism class of the ring of all integers of a cyclic wildly ramified extension of degree p, J. Algebra, to appear.

[5] I. Reiner, "Maximal orders", Academic Press, London, 1975.

Department of Mathematics
Faculty of Education
Shizuoka University
Shizuoka, 422 Japan