ON THE COHOMOLOGY GROUP OF THE UNIT GROUP OF AN ALGEBRAIC NUMBER FIELD

By

Noriyuki MATSUMURA

1. Let K be a finite Galois extension of a finite algebraic number field k and G the Galois group of K/k . We shall denote by $H^n(G, E)$ the n -dimensional cohomology groups of G acting on the group of units E of the field K for all non-negative integers n . Iwasawa [5] gave the result that when K/k is an unramified extension, $H^2(G, E)$ is isomorphic with the factor group of the group of ambiguous ideal classes of K modulo the group of ideal classes represented by ideals of k . In this note we shall extend it to the case where K/k is a tamely ramified extension. For the sake of simplicity we assume that every infinite prime divisor of k is unramified in K .

2. We denote by $\mathfrak{P}$ a prime divisor of K and by $\mathfrak{p}$ a prime divisor of k generally. And we consider the integral divisor $\mathfrak{m}$ of K ;

$$\mathfrak{m} = \prod_{\mathfrak{p} \mid \mathfrak{p}} \prod_{\mathfrak{P} \mid \mathfrak{p}} \mathfrak{P}^{\mu_{\mathfrak{p}}} \quad (\mu_{\mathfrak{p}} \geq 0),$$

where $\mathfrak{p}$ runs through a finite set of prime divisors of k which contains all the ramified primes in K/k . For this $\mathfrak{m}$, we set

$$U(\mathfrak{m}) = \prod_{\mathfrak{P} \mid \mathfrak{m}} U_{\mathfrak{P}}^{(\mu_{\mathfrak{p}})} \prod_{\mathfrak{P} \nmid \mathfrak{m}} U_{\mathfrak{P}}$$

where every $U_{\mathfrak{P}}$ is a $\mathfrak{P}$ -adic unit group of K and $U_{\mathfrak{P}}^{(\mu_{\mathfrak{p}})}$ is a subgroup defined by

$$U_{\mathfrak{P}}^{(\mu_{\mathfrak{p}})} = \{a \in U_{\mathfrak{P}}; a \equiv 1 \pmod{\mathfrak{P}^{\mu_{\mathfrak{p}}}}\}.$$

So, it is known that for the idele group J and the principal idele group P of K , $J/P \cdot U(\mathfrak{m})$ is the so-called ray class group. Furthermore, we set

$$E(\mathfrak{m}) = P \cap U(\mathfrak{m}).$$

Then $J, P, U(\mathfrak{m})$ and $E(\mathfrak{m})$ are considered as G -modules on which G acts in natural way and also we have the exact sequence of G -modules

$$1 \rightarrow U(\mathfrak{m})/E(\mathfrak{m}) \rightarrow J/P \rightarrow J/P \cdot U(\mathfrak{m}) \rightarrow 1.$$

Since it is well known that $H^1(G, \bar{J}) = 0$ for the idele class group $\bar{J} = J/P$ of K , we have the following exact sequence of cohomology groups from the sequence above:

$$H^0(G, \bar{J}) \rightarrow H^0(G, J/P \cdot U(\mathfrak{m})) \rightarrow H^1(G, U(\mathfrak{m})/E(\mathfrak{m})) \rightarrow 0.$$

Namely we have the following

LEMMA 1. $H^1(G, U(\mathfrak{m})/E(\mathfrak{m}))$ is isomorphic with the factor group of the group of ambiguous ray classes of K modulo the group of ray classes represented by ideals of k .

3. Next we shall calculate $H^1(G, U(\mathfrak{m}))$ and $H^2(G, U(\mathfrak{m}))$. Let $K_{\mathfrak{P}}$ be the completion of the field K at a prime $\mathfrak{P}$, $k_{\mathfrak{p}}$ the completion of the field k at a prime $\mathfrak{p}$, and $G_{\mathfrak{P}}$ the Galois group of $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ for $\mathfrak{P}|\mathfrak{p}$. So, it is sufficient for our purpose to calculate $H^1(G_{\mathfrak{P}}, U_{\mathfrak{P}}^{(\mu_{\mathfrak{p}})})$ and $H^2(G_{\mathfrak{P}}, U_{\mathfrak{P}}^{(\mu_{\mathfrak{p}})})$ at a finite tamely ramified prime.

Let us assume also that $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ be a tamely ramified extension. And we denote by $G_{\mathfrak{P}}$ the Galois group of $K_{\mathfrak{P}}/k_{\mathfrak{p}}$. Moreover, by k_T and G_T , we denote the inertia field and the inertia group of $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ at the prime $\mathfrak{P}$ and we set $\mu_{\mathfrak{p}} = \mu$. Then the group G_T is a cyclic group of order e_o and we denote by s a generator of G_T .

LEMMA 2.

$$H^1(G_T, U_{\mathfrak{P}}^{(\mu)}) = 0 \quad (\mu \geq 1)$$

PROOF. Since G_T is the cyclic group, it is sufficient to show that we have $E^{(\mu)} = E_o^{s-1}$ with some element E_o of $U_{\mathfrak{P}}^{(\mu)}$ for an element $E^{(\mu)}$ of $U_{\mathfrak{P}}^{(\mu)}$ such that $N_{K_{\mathfrak{P}}/k_T} E^{(\mu)} = 1$, where $N_{K_{\mathfrak{P}}/k_T}$ is the norm of $K_{\mathfrak{P}}/k_T$. By Hilbert's Theorem 90, we have $E^{(\mu)} = A^{s-1}$ with some element A of the multiplicative group $K_{\mathfrak{P}}^*$ of $K_{\mathfrak{P}}$. Let π be a prime element of $\mathfrak{P}$, then π^e , $g \in G_T$, is a prime element of $\mathfrak{P}$ too. Also we have a unit α_g of $K_{\mathfrak{P}}^*$ for

each $g \in G_T$ such that $\pi^g = \alpha_g \pi$. Then we can take the representative system ζ_g , in the integer ring O_T in k_T , of the classes of α_g modulo $\mathfrak{P}$. Since $K_{\mathfrak{P}}/k_{\mathfrak{P}}$ is a tamely ramified extension, these are only depending on $g \in G_T$. Also these representatives are generated by ζ_s and its order is e_0 .

Now, we can express the above element A such as

$$A = \pi^i E_1$$

for some E_1 of $U_{\mathfrak{P}}$ and some rational integer i . Here, we may suppose that $0 \leq i < e_0$. From $\pi^s \equiv \zeta_s \pi \pmod{\mathfrak{P}^2}$, we have

$$(1) \quad (\pi^{s-1})^i \equiv \zeta_s^i \pmod{\mathfrak{P}}.$$

Furthermore we can decompose:

$$E_1 = \zeta E_0,$$

where $E_0 \equiv 1 \pmod{\mathfrak{P}}$, and ζ means a root of unity, belonging to k_T . Also we have an expansion

$$E_0 = 1 + a_1 \pi + a_2 \pi^2 + \cdots, \quad a_i \in O_T$$

and

$$E_0^s = 1 + a_1 \alpha_s \pi + a_2 \alpha_s^2 \pi^2 + \cdots.$$

Therefore we see

$$(2) \quad E_0^{s-1} \equiv 1 + a_1 (\zeta_s - 1) \pi \pmod{\mathfrak{P}^2}.$$

From (1), (2), we have

$$E^{(\mu)} = A^{s-1} \equiv \zeta_s^i \equiv 1 \pmod{\mathfrak{P}},$$

hence

$$i = 0.$$

Namely $A = E_1$. In this, we can set $E_1 \equiv 1 \pmod{\mathfrak{P}}$. The remain is to show that $E_1 \equiv 1 \pmod{\mathfrak{P}^\mu}$. For $\mu = 2$, we substitute (2). Since the order of ζ_s is e_0 , for $\mu < e_0$ we can easily obtain the congruence by induction on μ . For $\mu = e_0$, π^{e_0} can be considered as a prime element of $\mathfrak{p}$ and

$1 + a_{e_0} \pi^{e_0}$ as a unit of k_T , hence setting again E_1 instead of $E_1/1 + a_{e_0} \pi^{e_0}$, it is sufficient. For $\mu = ne_0$, it is the same as in the above. This completes the proof of our lemma.

Now, $H^1(G_{\mathfrak{P}}/G_T, (U_{\mathfrak{P}}^{(\mu)})^{G_T}) = 0$ is easily seen, because $k_T/k_{\mathfrak{p}}$ is the unramified extension. Hence, from the following exact sequence, we have $H^1(G_{\mathfrak{P}}, U_{\mathfrak{P}}^{(\mu)}) = 0$ for $\mu \geq 1$;

$$0 \rightarrow H^1(G_{\mathfrak{P}}/G_T, (U_{\mathfrak{P}}^{(\mu)})^{G_T}) \xrightarrow{Inf.} H^1(G_{\mathfrak{P}}, U_{\mathfrak{P}}^{(\mu)}) \xrightarrow{Res.} H^1(G_T, U_{\mathfrak{P}}^{(\mu)}),$$

where we denote by *Inf.* and *Res.* the inflation and restriction homomorphism respectively.

Next, we shall calculate $H^2(G_{\mathfrak{P}}, U_{\mathfrak{P}}^{(\mu)})$. From Lemma 2, for $\mu \geq 1$ we have the exact sequence

$$0 \rightarrow H^2(G_{\mathfrak{P}}/G_T, (U_{\mathfrak{P}}^{(\mu)})^{G_T}) \xrightarrow{Inf.} H^2(G_{\mathfrak{P}}, U_{\mathfrak{P}}^{(\mu)}) \xrightarrow{Res.} H^2(G_T, U_{\mathfrak{P}}^{(\mu)}).$$

LEMMA 3.

$$H^2(G_T, U_{\mathfrak{P}}^{(\mu)}) = 0 \quad (\mu \geq 1)$$

PROOF. Since G_T is the cyclic group of order e_0 , it is sufficient to show that we have $E^{(\mu)} \in N_{K_{\mathfrak{P}}/k_T} U_{\mathfrak{P}}^{(\mu)}$ for an element $E^{(\mu)}$ of $U_{\mathfrak{P}}^{(\mu)}$ such that $E^{(\mu)} \in (U_{\mathfrak{P}}^{(\mu)})^{G_T}$. From $E_{\mathfrak{P}}^{(\mu)} \in (U_{\mathfrak{P}}^{(\mu)})^{G_T}$ we have

$$E^{(\mu)} \equiv 1 \pmod{\mathfrak{p}^{\left[\frac{\mu-1}{e_0}\right]+1}},$$

where we let the same symbol $\mathfrak{p}$ stand for the prime of k_T dividing $\mathfrak{p}$ and $[*]$ is the Gauss symbol. And because $K_{\mathfrak{P}}/k_T$ is a tamely ramified extension, we have

$$U_{\mathfrak{p}}^{\left(\left[\frac{\mu-1}{e_0}\right]+1\right)} = (U_{\mathfrak{p}}^{\left(\left[\frac{\mu-1}{e_0}\right]+1\right)})^{e_0} \subset N_{K_{\mathfrak{P}}/k_T} U_{\mathfrak{P}}^{(\mu)}$$

This furnishes the proof of the lemma.

Moreover we have $H^2(G_{\mathfrak{P}}/G_T, (U_{\mathfrak{P}}^{(\mu)})^{G_T}) = 0$. It is easily seen because $k_T/k_{\mathfrak{p}}$ is the unramified extension. Therefore we have

$$H^2(G_{\mathfrak{p}}, U_{\mathfrak{P}}^{(\mu)}) = 0 \quad \text{for } \mu \geq 1$$

4. Let us return to the global case. From 3, we have

$$H^1(G, U(\mathfrak{m})) = H^2(G, U(\mathfrak{m})) = 0 \quad \text{for } \mu_{\mathfrak{p}} \geq 1.$$

where every $\mathfrak{p}$ is a tamely ramified prime of K/k .

Also, from the exact sequence

$$1 \rightarrow E(\mathfrak{m}) \rightarrow U(\mathfrak{m}) \rightarrow U(\mathfrak{m})/E(\mathfrak{m}) \rightarrow 1$$

we have the isomorphism of cohomology groups;

$$H^1(G, U(\mathfrak{m})/E(\mathfrak{m})) \rightarrow H^2(G, E(\mathfrak{m})).$$

Hence, from Lemma 1 we have the following theorem:

THEOREM. $H^2(G, E(\mathfrak{m}))$ is isomorphic with the factor group of the group of ambiguous ray classes of K modulo the group of ray classes represented by ideals of k .

REMARK. When K/k is an unramified extension, we set $\mathfrak{m}=1$, so we have $U(\mathfrak{m}) = \prod_{\mathfrak{P}} U_{\mathfrak{P}}$, where $\mathfrak{P}$ runs through all prime divisors of K , $P \cap U(\mathfrak{m}) = E$ and $J/P \cdot U(\mathfrak{m})$ is considered as the ideal group of K .

References

- [1] G. W. S. CASSELS and A. FRÖHLICH, Algebraic Number Theory, Academic Press London, 1967.
- [2] C. CHEVALLEY, Class field theory, Nagoya Univ., 1953.
- [3] ———, *La théorie du corps de classes*, Ann. of Math., **41**, 1940, 394–418.
- [4] H. HASSE, Vorlesungen über Klassenkörpertheorie, Physica Verlag, Würzburg, 1967.
- [5] K. IWASAWA, *A note on the group of units of an algebraic number field*, J. Math. Pures et Appl., **35**, 1956, 180–192.
- [6] T. TAKAGI, Daisūteki Seisūron (in Japanese), Iwanami, 1971.