ON THE GALOIS COHOMOLOGY GROUP OF THE RING OF INTEGERS IN A GLOBAL FIELD AND ITS ADELE RING

YOSHIOMI FURUTA and YASUAKI SAWADA

By a global field we mean a field which is either an algebraic number field, or an algebraic function field in one variable over a finite constant field. The purpose of the present note is to show that the Galois cohomology group of the ring of integers of a global field is isomorphic to that of the ring of integers of its adele ring and is reduced to asking for that of the ring of local integers.

1. Throughout this note, the following notations will be used.

F	a global field
R	the rational subfield of F, i.e. the rational number field Q or the rational function field $k(x)$ according as F is an algebraic number field or an algebraic function field in one variable over a finite constant field k.
$\mathfrak{p}$	a finite or an infinite prime of F
$M(F)$	the set of all prime divisors of F
$M_0(F)$	the set of all finite prime divisors of F
$M_\infty(F)$	the set of all infinite prime divisors of F
s	a finite subset of $M(F)$, including all of $M_\infty(F)$
$F_\mathfrak{p}$	the $\mathfrak{p}$-completion of F, where $\mathfrak{p} \in M(F)$
$O_\mathfrak{p}$	the ring of integers of $F_\mathfrak{p}$, where $\mathfrak{p} \in M_0(F)$
$\boldsymbol{F}_s = \sum_{\mathfrak{p}\in s} F_\mathfrak{p} + \sum_{\mathfrak{p}\notin s} O_\mathfrak{p}$	(direct)
$\boldsymbol{F}$	the adele ring of F, i.e., $\boldsymbol{F} = \bigcup_s \boldsymbol{F}_s$
$F_s = F \cap \boldsymbol{F}_s$	
E	a Galois extension field over a global field F

Received May 18, 1967.

$\mathfrak{P}$	a prime of E which divids $\mathfrak{p}$
p	a prime of R divided by $\mathfrak{p}$
G	the Galois group of E/F
$H^r(G, A)$	the r-dimensional Galois cohomology group of G-module A
$D_{E/F}$	the different of E/F
$S_{E\to F}$	the trace function from E to F
$[A:B]$	the index of a subgroup B in a group A or the degree of an extension field A over B

We will say $\boldsymbol{F}_s$ resp. F_s the ring of s-integers of $\boldsymbol{F}$ resp. the ring of s-integers of F. Especially when F is an algebraic number field and $s = M_\infty(F)$, then F_s is the ring of usual integers. For the sake of simplicity the all of extensions to E of the prime divisors belonging to s will be denoted again by s. From now let s satisfy the condition that $\mathfrak{P} \in s$ then $\sigma\mathfrak{P} \in s$ for every $\sigma \in G$, so that $\boldsymbol{E}_s$ and E_s are G-modules.

2. Similarly to a direct product decomposition of the Galois cohomology group of the idele group, we have the following theorem.

THEOREM 1.

$$H^r(G, \boldsymbol{E}_s) \cong \sum_{\mathfrak{p}\in s} H^r(G_{\mathfrak{P}}, E_{\mathfrak{P}}) + \sum_{\mathfrak{p}\notin s} H^r(G_{\mathfrak{P}}, O_{\mathfrak{P}}) \qquad (\textit{direct})$$

for every integer r, where $\mathfrak{P}$ is an arbitrary extension of $\mathfrak{p} \in M(F)$ to E and $G_{\mathfrak{P}}$ is the decomposition group of $\mathfrak{P}$.

Proof. Let $\mathfrak{P}_1, \cdots, \mathfrak{P}_g (\mathfrak{P}_1 = \mathfrak{P})$ be prime divisors over $\mathfrak{p}$ and $G = \bigcup_1^g \tau_i G_{\mathfrak{P}}$, then $G_{\mathfrak{P}} = G(E_{\mathfrak{P}}/F_{\mathfrak{p}})$ and $\sum_1^g E_{\mathfrak{P}_i} = \sum_1^g \tau_i E_{\mathfrak{P}}$, $\sum_1^g O_{\mathfrak{P}_i} = \sum_1^g \tau_i O_{\mathfrak{P}}$ therefore, by the semilocal theory of cohomology we have

$$H^r(G, \sum_1^g E_{\mathfrak{P}_i}) \cong H^r(G_{\mathfrak{P}}, E_{\mathfrak{P}})$$

$$H^r(G, \sum_1^g O_{\mathfrak{P}_i}) \cong H^r(G_{\mathfrak{P}}, O_{\mathfrak{P}}).$$

Now
$$\boldsymbol{E}_s = \sum_{\mathfrak{P}\in s} \Big(\sum_{\mathfrak{p}\subset\mathfrak{P}} E_{\mathfrak{P}} \Big) + \sum_{\mathfrak{p}\notin s} \Big(\sum_{\mathfrak{p}\subset\mathfrak{P}} O_{\mathfrak{P}} \Big)$$

then

$$H^r(G, \boldsymbol{E}_s) \cong \sum_{\mathfrak{p} \in s} H^r(G, \sum_{\mathfrak{p} \subset \mathfrak{P}} E_{\mathfrak{P}}) + \sum_{\mathfrak{p} \notin s} H^r(G, \sum_{\mathfrak{p} \subset \mathfrak{P}} O_{\mathfrak{P}})$$
$$\cong \sum_{\mathfrak{p} \in s} H^r(G_{\mathfrak{P}}, E_{\mathfrak{P}}) + \sum_{\mathfrak{p} \notin s} H^r(G_{\mathfrak{P}}, O_{\mathfrak{P}}).$$

Concerning the factors of theorem 1 we have the following proposition.

PROPOSITION 1.

$H^r(G_{\mathfrak{P}}, E_{\mathfrak{P}})$ is trivial for every integer r.

Proof. Since $E_{\mathfrak{P}}$ has the normal basis, it is G-regular, and the proposition follows from the well known theorem of cohomology.

In the same way on the algebraic number field of Yokoi [2], the following lemma and proposition are proved also on algebraic function fields in one variable over a finite constant field and their local fields.

LEMMA.

Let $E_{\mathfrak{P}}/F_{\mathfrak{p}}$ be Galoisian and e be the ramification order of $E_{\mathfrak{P}}/F_{\mathfrak{p}}$. If $D_{E_{\mathfrak{P}}/F_{\mathfrak{p}}} = \mathfrak{p}^r\mathfrak{P}^s$ $(e > s \geqq 0,\ r \geqq 0)$, then $S_{E_{\mathfrak{P}} \to F_{\mathfrak{p}}} O_{\mathfrak{P}} = \mathfrak{p}^r$.

PROPOSITION 2.

If $E_{\mathfrak{P}}/F_{\mathfrak{p}}$ is tamely ramified then $H^r(G_{\mathfrak{P}}, O_{\mathfrak{P}})$ is trivial for every integer r.

It follows from this proposition and the Dedekind's theorem on OAF[1] that the number of factors in theorem 1 is finite.

3. On the Galois cohomology group of the adele ring we have the following theorem.

THEOREM 2.

$H^r(G, \boldsymbol{E})$ is trivial for every integer r.

Proof. Let $\mathfrak{F}$ be the family which consists of all finite subsets s of $M(E)$, where s satisfies the condition $M_\infty(E) \subset s$ as stated first. We make $\mathfrak{F}$ be an ordered set by means of the ordinary inclusion relation. Then $H^r(G, \boldsymbol{E})$ is the inductive limit of $\{H^r(G, \boldsymbol{E}_s)\}_{s \in \mathfrak{F}}$:

$$H^r(G, \boldsymbol{E}) \cong \varinjlim_s \{H^r(G, \boldsymbol{E}_s)\}.$$

---

[1] cf. Weiss [1], p. 157. The term OAF (ordinary arithmetic field) means the quotient field of the Dedekind domain and its finite extension field.

On the other hand it follows from theorem 1 and proposition 2 that $H^r(G, \boldsymbol{E}_s)$ is trivial for all sufficiantly large s. Hence the theorem is proved.

Now we have the following main theorem.

THEOREM 3.

$H^r(G, E_s) \cong H^r(G, \boldsymbol{E}_s)$ for every integer r.

Proof. From the exact sequence

$$0 \longrightarrow E \longrightarrow \boldsymbol{E} \longrightarrow \boldsymbol{E}/E \longrightarrow 0$$

we obtain the exact sequence

$$\cdots \longrightarrow H^r(E) \longrightarrow H^r(\boldsymbol{E}) \longrightarrow H^r(\boldsymbol{E}/E) \longrightarrow H^{r+1}(E) \longrightarrow \cdots .$$

By the same way as proposition 1 and by theorem 2 we have $H^r(E) = 0$ and $H^r(\boldsymbol{E}) = 0$ for every integer r. Hence $H^r(\boldsymbol{E}/E) = 0$ for every integer r. On the other hand, from the exact sequence

$$0 \longrightarrow E_s \longrightarrow \boldsymbol{E}_s \longrightarrow \boldsymbol{E}_s/E_s \longrightarrow 0$$

we obtain the exact sequence

$$\cdots \longrightarrow H^r(E_s) \longrightarrow H^r(\boldsymbol{E}_s) \longrightarrow H^r(\boldsymbol{E}_s/E_s) \longrightarrow H^{r+1}(E_s) \longrightarrow \cdots .$$

We have easily that $\boldsymbol{E} = E + \boldsymbol{E}_s$[2]. Hence

$$\boldsymbol{E}_s/E_s = \boldsymbol{E}_s/(\boldsymbol{E}_s \cap E) \cong (\boldsymbol{E}_s + E)/E = \boldsymbol{E}/E$$

and $H^r(\boldsymbol{E}_s/E_s) \cong H^r(\boldsymbol{E}/E) = 0$. Now the above exact sequence implies $H^r(E_s) \cong H^r(\boldsymbol{E}_s)$ for every integer r.

4. By this theorem we know that the structure of the Galois cohomology group of $\boldsymbol{E}_s$ or E_s with respect to a global field is determined by the local Galois cohomology groups appeared in the decomposition in theorem 1. On the local parts using the procedure in Yokoi [3] and [4], we have the following theorems according to the above way.

THEOREM 4.

If G is a cyclic group, then $H^r(G, \boldsymbol{E}_s)$ and hence $H^r(G, E_s)$ have the same order for every integer r.

---

[2] cf. Weiss [1], p. 197.

Proof. By theorem 1 and 3 it is sufficient to consider $H^r(G_{\mathfrak{P}}, O_{\mathfrak{P}})$. Let $\gamma_1, \cdots, \gamma_n$ be a normal basis for $E_{\mathfrak{P}}/F_{\mathfrak{p}}$. Put $O^* = F_{\mathfrak{p}}\gamma_1 + \cdots + F_{\mathfrak{p}}\gamma_n$ and $\tilde{O} = O_{\mathfrak{P}}/O^*$. Then $H^r(O^*) = 0$ and the order of $\tilde{O}$ is finite. This implies that the Herbrand quotient $h_{0/1}(\tilde{O}) = 1$. Moreover it follows from the exact sequence:

$$0 \longrightarrow O^* \longrightarrow O_{\mathfrak{P}} \longrightarrow \tilde{O} \longrightarrow 0$$

that $h_{0/1}(O_{\mathfrak{P}}) = 1$. Since G is cyclic, the theorem is obtained from the well known theorem of cohomology.

Remark. When E is an algebraic number field and $s = M_\infty(F)$, the assertion on $H^r(G, E_s)$ of the theorem was given by Yokoi [4].

Now, there is an integer r for which the r-th ramification group:

$$V_r = \{\sigma \in G_{\mathfrak{P}} \mid (\sigma - 1)O_{\mathfrak{P}} \subset \mathfrak{P}^{r+1}\}$$

is trivial, and in this note the *ramification number* of $\mathfrak{P}$ with respect to E/F means the integer v smaller than the minimum of r by 1.

THEOREM 5.

Let E be a cyclic extension field of prime degree l over a global field F, and R be its rational subfield. Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_m$ be prime divisors of F, which are ramified in E but do not belong to s, and $\mathfrak{P}_i$ resp. P_i be one of the extensions to E resp. one of the restrictions to R of $\mathfrak{p}_i$ $(i = 1, \cdots, m)$. Let $v_{\mathfrak{P}_i}$ be the ramification order of $\mathfrak{p}_i$ for F/R. Put $n_{\mathfrak{P}_i} = [F_{\mathfrak{p}_i} : R_{p_i}]$, $u_{\mathfrak{P}_i} = v_{\mathfrak{P}_i} - [v_{\mathfrak{P}_i}/l]$, where $[x]$ stand for the Gaussian symbol, $l^{\alpha_{\mathfrak{P}_i}} = [O_{p_i} : p_i]$[3] and $\nu = \sum_{i=1}^{m} \alpha_{\mathfrak{P}_i} n_{\mathfrak{P}_i} u_{\mathfrak{P}_i}/e_{\mathfrak{P}_i}$. Then $H^r(G, \boldsymbol{E}_s)$ and hence $H^r(G, E_s)$ are isomorphic to the ν-ple direct sum of the cyclic group of order l for every integer r.

Proof. In order to prove the theorem it is sufficient to count the order of $H^r(G, \boldsymbol{E}_s)$ because the order of each element of the cohomology group of a finite group G is divided by the order of G. Since G is cyclic, it follows from theorem 4 that $H^r(G, \boldsymbol{E}_s)$ and $H^0(G, \boldsymbol{E}_s)$ have the same order and they are equal to $\prod_{\mathfrak{p} \in s} [O_{\mathfrak{p}} : S_{E_{\mathfrak{P}} \to F_{\mathfrak{p}}} O_{\mathfrak{P}}]$ by theorem 1. Now we fix one

3) When $E_{\mathfrak{P}}/F_{\mathfrak{p}}$ is wildly ramified, the characteristic of the residue class field of R_p must be the prime l, hence the order of the residue class field of R_p is a power of l. Especially E is an algebraic number field then $\alpha_{\mathfrak{P}_i} = 1$.

of divisor $\mathfrak{P}_i$ and denote it by $\mathfrak{P}$. Let $D_{E_{\mathfrak{P}}/F_{\mathfrak{p}}} = \mathfrak{p}^r\mathfrak{P}^s$ $(0 \leqq s < e_{\mathfrak{P}})$, then $S_{E_{\mathfrak{P}} \to F_{\mathfrak{p}}} O_{\mathfrak{P}} = \mathfrak{p}^r$ by lemma. We have $[O_{\mathfrak{p}} : \mathfrak{p}] = l^{\alpha_{\mathfrak{P}} f_{\mathfrak{P}}}$ where $f_{\mathfrak{P}}$ is the residue class degree of $F_{\mathfrak{p}}/R_p$. Therefore the order of $H^r(G, \boldsymbol{E}_s)$ is equal to $\prod_{\mathfrak{p} \in S} l^{\alpha_{\mathfrak{P}} r n_{\mathfrak{P}}/e_{\mathfrak{P}}}$. It is easy that $r = u_{\mathfrak{P}}$ by Hilbert's formula.

Remark. When E is an algebraic number field and $s = M_\infty(F)$, the assertion on $H^r(G, E_s)$ of the theorem was given by Yokoi [3], but the consequence was simple for the reason of assuming that E and F are Galoisian over $R = Q$.

References

[1] E. Weiss: Algebraic Number Theory, McGraw-Hill (1963).
[2] H. Yokoi: On the ring of integers in an algebraic number field as a representation module of Galois group, Nagoya Math. J., **16** (1960).
[3] ————: On the Galois cohomology group of the ring of integers in an algebraic number field, Acta Arithmetica **VIII** (1963).
[4] ————: A note on the Galois cohomology group of the ring of integers in an algebraic number field, Proc. Japan Acad., **40** (1964).

Kanazawa University
Kanazawa Institute of Technology