

On Indices of Unit Groups Related to the Genus Number of Galois Extensions

Norikata NAKAGOSHI*

Department of Mathematics, Faculty of Science, Kanazawa University

(Received March 26, 1975)

1. Let K/k be a Galois extension of finite degree, over a finite algebraic number field k and denote by K^* the genus field of K over k . A formula of the genus number $g_{K/k} = (K^* : K)$ is given by Y. Furuta [2] :

$$g_{K/k} = \frac{h_k \prod_p e_p'}{(K_0 : k)(\varepsilon : \eta)},$$

where (ε) is the unit group of k , (η) is the subgroup of (ε) generated by the units η which are everywhere locally norm, h_k is the class number of k and the other notations are as in [2]. If K/k is cyclic, then $g_{K/k}$ is equal to the ambiguous ideal class number of K over k and we have some results on the relation between class numbers and $(\varepsilon : \eta)$ in [3], [6] and [7].

In the present paper, we treat of the divisors of the index $(\varepsilon : \eta)$ for Abelian extensions and decide the index for Kummer extensions $K = k(\sqrt[l]{\Delta})$, where l is an odd prime, Δ is an l -th power free rational integer and k is the l -th cyclotomic field over the rational number field \mathbb{Q} .

2. For each prime divisor p of k , we denote by U_p the unit group of the p -completion k_p of k and by H_p the subgroup of U_p , consisting of all units $\bar{\varepsilon}$ of U_p such that $\bar{\varepsilon} \equiv 1 \pmod{p}$ ("Einseinheitengruppe von k_p "). We put

$$(\eta_p) = (\varepsilon) \cap NU_{\mathfrak{P}}, \quad (\eta'_p) = (\varepsilon) \cap H_p,$$

where $U_{\mathfrak{P}}$ is the unit group of $K_{\mathfrak{P}}$ for an extension \mathfrak{P} of p in K and N is the norm with respect to $K_{\mathfrak{P}}/k_p$.

*Present address : Department of Mathematics, College of Liberal Arts, Toyama University

Let $\mathfrak{R}_p^\times, \mathfrak{R}_p^\times$ be the cyclic groups, generated by a primitive $(\mathfrak{N}(p) - 1)$ -th root of unity and a primitive $(\mathfrak{N}(p) - 1)$ -th root of unity, respectively, where $\mathfrak{N}(p)$ is the absolute norm of p .

LEMMA. *Let K/k be an Abelian extension of finite degree. Then we have*

- (i) $e(p) \equiv 0 \pmod{(\varepsilon : \eta_p)}$ for a prime divisor p of k ,
- (ii) for a tamely ramified prime divisor p of k ,

$$(\varepsilon : \eta_p) \equiv 0 \pmod{\frac{(w, \mathfrak{N}(p)-1)}{(w, \frac{\mathfrak{N}(p)-1}{e(p)})}} \text{ and } (\varepsilon : \eta_{p'}) \equiv 0 \pmod{(w, \mathfrak{N}(p)-1)},$$

where $e(p)$ is the ramification index of p in K/k , w is the number of roots of unity in k and (a, b) is the greatest common divisor for integers a and b .

Proof. If K/k is an Abelian extension of finite degree, then $(U_p : NU_p) = e(p)$, hence we have (i).

It is well-known the direct decompositions

$$U_p = \mathfrak{R}_p^\times \times H_p, \quad U_p = \mathfrak{R}_p^\times \times H_p,$$

and

$$NU_p = N\mathfrak{R}_p^\times \times NH_p, \quad NH_p \cap H_p = NH_p. \quad (1)$$

On the other hand, $(U_p : NU_p) = e(p)$, $(U_p : H_p) = \mathfrak{N}(p) - 1$ and $(H_p : H_p^{\mathfrak{N}(p)})$ is the power of p , where $\mathfrak{N}(p) = (K_p : k_p)$ and p is the prime number divisible by p (cf. [4], s. 222-223). Then it follows by the assumption that

$$NH_p = H_p \quad (2)$$

and

$$U_p / NU_p \cong \mathfrak{R}_p^\times / N\mathfrak{R}_p^\times. \quad (3)$$

Here $N\mathfrak{R}_p^\times$ is generated by a primitive $(\mathfrak{N}(p) - 1)/e(p)$ -th root of unity.

Let ξ_0 be a primitive w -th root of unity in (ε) . Then $(\varepsilon : \eta_p) \equiv 0 \pmod{(\xi_0 : (\xi_0 \cap (\eta_p)))}$, and by (1), (2) we have $(\xi_0 : (\xi_0 \cap (\eta_p))) \equiv 0 \pmod{((\xi_0) \cap \mathfrak{R}_p^\times : (\xi_0) \cap N\mathfrak{R}_p^\times)}$.

Finally, $(\varepsilon : \eta_{p'}) \equiv 0 \pmod{((\xi_0) \cap \mathfrak{R}_p^\times : 1)}$. Thus (ii) is proved.

PROPOSITION. *Let K/k be an Abelian extension of finite degree and p_1, \dots, p_t be all the finite prime divisors of k tamely ramified in K . Then*

$$(\varepsilon : \eta) \equiv 0 \pmod{2^{\delta} \prod_{i=1}^t \frac{(w_{i-1}, \mathfrak{N}(p_i)-1)}{(w_{i-1}, \frac{\mathfrak{N}(p_i)-1}{e(p_i)})}},$$

where

$$w_0 = w, \quad w_i = (w_{i-1}, (w, \frac{\mathfrak{R}(p_i) - 1}{e(p_i)}) p_i^{u_i});$$

p_i is the prime number divisible by p , $p_i^{u_i}$ is the p_i -component of w for each i ($1 \leq i \leq t$), and

$$\delta = \begin{cases} 1, & \text{if at least one of the infinite prime divisors of } k \text{ is ramified in } K \\ & \text{and } w_t = 2, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. We put

$$(\eta_{p_i}) = (\varepsilon) \cap NU_{\mathfrak{p}_i}, \quad (\eta_s) = \bigcap_{i=1}^s (\eta_{p_i}), \quad 1 \leq i \leq s \leq t,$$

and let ξ_0 be a primitive w -th root of unity in (ε) .

From the direct decomposition of H_{p_i} and (2), we have

$$NH_{\mathfrak{p}_i} = H_{p_i} = Z_{p_i} \times H_{0,p_i},$$

where Z_{p_i} is the cyclic subgroup of H_{p_i} of p_i -th power order and H_{0,p_i} is the free part of H_{p_i} of rank $(k_{p_i} : \mathbf{Q}_{p_i})$.

For $i=1$,

$$(\eta_1) = (\varepsilon) \cap NU_{\mathfrak{p}_1} \supset ((\xi_0) \cap N\mathfrak{R}_{\mathfrak{p}_1}^{\times}) \times ((\xi_0) \cap Z_{p_1})$$

and by (3)

$$(((\xi_0) \cap N\mathfrak{R}_{\mathfrak{p}_1}^{\times}) \times ((\xi_0) \cap Z_{p_1}) : 1) = (w, \frac{\mathfrak{R}(p_1) - 1}{e(p_1)}) p_1^{u_1} = w_1.$$

Thus (η_1) contains a primitive w_1 -th root of unity.

Moreover we have

$$(\eta_2) = (\eta_{p_1}) \cap (\eta_{p_2}) \supset \bigcap_{i=1}^2 \left\{ ((\xi_0) \cap N\mathfrak{R}_{\mathfrak{p}_i}^{\times}) \times ((\xi_0) \cap Z_{p_i}) \right\},$$

hence (η_2) contains a primitive w_2 -th root of unity and similarly as above, (η_s) contains a primitive w_s -th root of unity ($s=1, \dots, t$).

Let ξ_s be a primitive w_s -th root of unity for each s ($1 \leq s \leq t$). Then

$$(\eta_{s-1} : \eta_s) \equiv 0 \pmod{(\xi_{s-1} : (\xi_{s-1}) \cap (\eta_s))},$$

and

$$(\xi_{s-1} : (\xi_{s-1}) \cap (\eta_s)) \equiv 0 \pmod{((\xi_{s-1}) \cap \mathfrak{R}_{\mathfrak{p}_s}^{\times} : (\xi_{s-1}) \cap N\mathfrak{R}_{\mathfrak{p}_s}^{\times})},$$

where $(\eta_0) = (\varepsilon)$.

Suppose that the infinite real prime divisors of k are all unramified in K . Then

$(\varepsilon : \eta) \equiv 0 \pmod{\prod_{i=1}^t (\eta_{s-1} : \eta_s)}$ and the proposition is proved.

Next, let $p_{1,\infty}, \dots, p_{\lambda,\infty}$ be the infinite prime divisors of k ramified in K and put

$$(\eta_{p_{j,\infty}}) = (\varepsilon) \cap NU_{\mathfrak{p}_{j,\infty}}, \quad (\eta_{t,\nu}) = (\eta_t) \cap \prod_{j=1}^{\nu} (\eta_{p_{j,\infty}}), \quad 1 \leq j \leq \nu \leq \lambda.$$

Then

$$(\varepsilon : \eta) \equiv 0 \pmod{\prod_{s=1}^t (\eta_{s-1} : \eta_s) \cdot (\eta_t : \eta_{t,1}) \cdots (\eta_{t,\lambda-1} : \eta_{t,\lambda})}, \quad (\eta_{p_{j,\infty}}) = \{\varepsilon_0 \in (\varepsilon) \mid \varepsilon_0 > 0\},$$

$$j = 1, \dots, \lambda, \quad w = 2, \quad (\eta_t : \eta_{t,1}) = \begin{cases} 1, & \text{if } w_t = 1, \\ 2, & \text{if } w_t = 2, \end{cases}$$

and $(\eta_{t,1} : \eta_{t,2}) = \cdots = (\eta_{t,\lambda-1} : \eta_{t,\lambda}) = 1$. Thus we have the proposition.

3. We note that if K/k is a tamely ramified Abelian extension of finite degree, then $(\varepsilon : \eta)$ can be expressed as follows; let ρ_i be a primitive $(\mathfrak{R}(p_i) - 1)$ -th root of unity and $(\eta_s \bmod p_i)$ be the subgroup of $\mathfrak{R}_{p_i}^{\times}$, generated by the representatives of $\eta_s \bmod p_i$, $1 \leq i \leq s \leq t$. Then

$$(\eta_{s-1})/(\eta_s) \cong (\eta_{s-1} \bmod p_s)/(\eta_{s-1} \bmod p_s) \cap N\mathfrak{R}_{\mathfrak{p}_s}^{\times},$$

where $(\eta_0) = (\varepsilon)$. We take also the rational integers $a(p_s)$ and $b(p_s)$ such that

$$(\eta_{s-1} \bmod p_s) = \langle \rho_s^{a(p_s)} \rangle, \quad (\eta_{s-1} \bmod p_s) \cap N\mathfrak{R}_{\mathfrak{p}_s}^{\times} = \langle \rho_s^{b(p_s)} \rangle.$$

Then $b(p_s)$ is the least common multiple of $a(p_s)$ and $e(p_s)$ and we have

$$(\eta_{s-1} : \eta_s) = \frac{d_0(p_s)}{d(p_s)},$$

where $d(p_s) = (a(p_s), \mathfrak{R}(p_s) - 1)$ and $d_0(p_s) = (b(p_s), \mathfrak{R}(p_s) - 1)$. Therefore, it follows

$$(\varepsilon : \eta) = 2^{\delta} \prod_{i=1}^t \frac{d_0(p_i)}{d(p_i)},$$

where δ is defined in the proposition.

4. Examples.

(a). Put $k = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{d})$, where d is a square free positive rational integer, having prime factors $p \neq 2$. For each odd prime factor p of d we have

$$\frac{(2, p-1)}{(2, \frac{p-1}{2})} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4}, \\ 2, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Then we have by (i) of the lemma that $(\varepsilon : \eta_p) = 2$, if $p \equiv 3 \pmod{4}$.

(b). Let $K=k(\sqrt[l]{\Delta})$, where l is an odd prime number, Δ is an l -th power free rational integer having prime factors $p \neq l$ and k is the l -th cyclotomic field over \mathbb{Q} .

For a prime factor p of Δ not equal to l , we have

$$\frac{(2l, \frac{\mathfrak{R}(p)-1}{l})}{(2l, \frac{\mathfrak{R}(p)-1}{l})} = \begin{cases} 1, & \text{if } \mathfrak{R}(p) \equiv 1 \pmod{l^2}, \\ l, & \text{if } \mathfrak{R}(p) \not\equiv 1 \pmod{l^2}. \end{cases}$$

Hence we have $(\varepsilon : \eta_p) = l$, if $\mathfrak{R}(p) \not\equiv 1 \pmod{l^2}$.

(c). Let $k=\mathbb{Q}(\zeta)$, $\zeta = \exp(2\pi i/3 \cdot 5 \cdot 7 \cdot 11)$ and $K=k(\sqrt[3 \cdot 5]{7 \cdot 11})$.

Let p_1 and p_2 be the prime divisors of k , lying above 7, 11, respectively. Then

$$\frac{(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11, \frac{\mathfrak{R}(p_i)-1}{3 \cdot 5})}{(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11, \frac{\mathfrak{R}(p_i)-1}{3 \cdot 5})} = \begin{cases} 3, & \text{for } i=1, \\ 5, & \text{for } i=2, \end{cases}$$

and $(\varepsilon : \eta) \equiv 0 \pmod{3 \cdot 5}$.

5. Notations being as above, we have the following

THEOREM. Let l be an odd prime and ζ be a primitive l -th root of unity. We put $k=\mathbb{Q}(\zeta)$ and $K=k(\sqrt[l]{\Delta})$, where Δ is an l -th power free rational integer. Let \mathfrak{p} be a prime divisor of k , lying above a rational prime p and t be a number of ramified prime divisors of k in K .

(i) If $\mathfrak{R}(p) \equiv 1 \pmod{l^2}$ for each prime factor p of Δ and l is a regular prime, then

$$(\varepsilon : \eta) = 1 \text{ and } g_{K/k} = h_k \cdot l^{t-1}.$$

(ii) If $\mathfrak{R}(p) \not\equiv 1 \pmod{l^2}$ for some prime factor p of Δ and $\Delta^{l-1} \equiv 1 \pmod{l^2}$, then

$$(\varepsilon : \eta) = l \text{ and } g_{K/k} = h_k \cdot l^{t-2}.$$

Proof. (A) Let ρ be a primitive $(\mathfrak{R}(p)-1)$ -th root of unity for the prime divisor \mathfrak{p} of Δ ($p \neq l$).

(a₁) In the case where $\mathfrak{R}(p) \equiv 1 \pmod{l^2}$.

If $(\varepsilon : \eta_p) = 1$, i.e. $(\varepsilon) = (\eta_p) = (\varepsilon) \cap (N\mathfrak{R}_{\mathfrak{p}}^{\times} \times H_{\mathfrak{p}})$ by (1) and (2), then $\zeta \in N\mathfrak{R}_{\mathfrak{p}}^{\times}$. Since $N\mathfrak{R}_{\mathfrak{p}}^{\times} = \langle \rho^l \rangle$ by (3) and $e(\mathfrak{p}) = l$, $(\mathfrak{R}(p)-1)/l \equiv 0 \pmod{l}$. Therefore, if $\mathfrak{R}(p) \equiv 1 \pmod{l^2}$, then $(\varepsilon : \eta_p) \neq 1$ and $\zeta \notin N\mathfrak{R}_{\mathfrak{p}}^{\times}$. Hence we have $(\varepsilon : \eta_p) = l$ by (i) of the lemma.

Moreover, (ε) contains a primitive $2l$ -th root of unity and the roots of unity in (η_p) are ± 1 , a system of the fundamental units of (ε) can be chosen the same as that of (η_p) .

(a₂) In the case where $\mathfrak{R}(p) \not\equiv 1 \pmod{l^2}$ and l is a regular prime.

Let

$$\mathfrak{R}(p) \equiv 1 \pmod{l^{\mu}}, \quad \not\equiv 1 \pmod{l^{\mu+1}}, \quad \mu \geq 2.$$

We denote by ζ_j a primitive l -th root of unity and by (ε_j) the unit group of $k_j = Q(\zeta_j)$ for each j ($1 \leq j \leq \mu$, $\zeta_1 = \zeta$, $k_1 = k$, $(\varepsilon_1) = (\varepsilon)$).

Let $\mathfrak{p} = \mathfrak{p}_1 = \mathfrak{p}_1^{(1)} \cdots \mathfrak{p}_1^{(l^{\mu-1})}$ be the prime ideal decomposition of $\mathfrak{p} = \mathfrak{p}_1$ in k_μ . Since $\mathfrak{R}(\mathfrak{p}_1) = \mathfrak{R}(\mathfrak{p}_1^{(s)})$, $s=1, \dots, l^{-1}$, each ε_μ of (ε_μ) can be written as

$$\varepsilon_\mu = \rho^x \cdot \eta^{(s)}, \quad \rho^x \in \mathfrak{R}_{\mathfrak{p}}^\times, \quad \eta^{(s)} \in H_{\mathfrak{p}_1^{(s)}}, \quad s=1, \dots, l^{\mu-1},$$

where $H_{\mathfrak{p}_1^{(s)}}$ are the "Einseinheitengruppen" of the $\mathfrak{p}_1^{(s)}$ -completions of k_μ . Then

$$N_{k_\mu/k_1} \varepsilon_\mu = (\rho^l)^{x \cdot l^{\mu-2}} \cdot \prod_{s=1}^{l^{\mu-1}} \eta^{(s)}.$$

Since $N_{\mathfrak{R}_{\mathfrak{p}}^\times} = \langle \rho^l \rangle$ by (3) and $e(\mathfrak{p}) = l$, $N_{k_\mu/k_1} \varepsilon_\mu \in (\eta_{\mathfrak{p}_1}) = (\eta_{\mathfrak{p}})$ and $N_{k_\mu/k_1}(\varepsilon_\mu) \subset (\eta_{\mathfrak{p}})$.

For the regular prime l , we see in [6] that

$$N_{k_{j+1}/k_j}(\varepsilon_{j+1}) = (\varepsilon_j), \quad j=1, \dots, \mu-1, \dots$$

Hence $(\varepsilon : \eta_{\mathfrak{p}}) = 1$.

(B) We know by (a₁) that if $(\varepsilon : \eta_{\mathfrak{p}}) = (\varepsilon : \eta_{\mathfrak{p}'}) = l$ for two tamely ramified prime divisors \mathfrak{p} and \mathfrak{p}' of k , then $(\eta_{\mathfrak{p}}) = (\eta_{\mathfrak{p}'})$.

Now, it is proved in [1] that $l = (1 - \zeta)$ is unramified in K if and only if $d^{l-1} \equiv 1 \pmod{l^2}$. Thus the theorem is proved.

6. Example.

Let l be an odd prime and ζ be a primitive l -th root of unity. We put $k = Q(\zeta)$ and $K = k(\sqrt[l]{\Delta})$, where Δ is an l -th power free rational integer such that

$$\Delta = \prod_{i=1}^t A_i, \quad A_i \neq 1, \quad (A_i, A_j) = 1 \text{ for } 1 \leq i < j \leq t$$

and

$$d_i^{l-1} \equiv 1 \pmod{l^2} \quad (i = 1, \dots, t).$$

Then we have

$$d^{(l)} C_K \geq t - 1 + d^{(l)} C_k,$$

where $d^{(l)} C_k$ is the l -rank of the ideal class group C_k of k .

In particular, if l is a regular prime and $A_i = p_i$ are prime numbers satisfying the above conditions and their orders modulo l are all $l-1$, then

$$K^* = \bar{k}(\sqrt[l]{p_1}, \dots, \sqrt[l]{p_t}),$$

where \bar{k} is the absolute class field of k .

Proof. $K(\sqrt[l]{\Delta})/K$ are unramified extensions by [1] ($i=1, \dots, t$) and then

$\prod_{i=1}^t K(\sqrt[l]{\Delta_i}) = k(\sqrt[l]{\Delta_1}, \dots, \sqrt[l]{\Delta_t})$ is an unramified Abelian extension over K ,

of degree l^{t-1} .

In particular, if l is a regular prime and $\Delta_i = p_i$ are primes mentioned as above, then $(\varepsilon : \eta) = 1$ and p_i are all primes in k . Hence $g_{K/k} = h_k \cdot l^{t-1}$ and $K^* = \bar{k}(\sqrt[l]{p_1}, \dots, \sqrt[l]{p_t})$.

REFERENCES

- [1] Akiyama, S., On the class numbers of certain Kummer extensions (in Japanese), Sugaku (Tokyo), **21** (1967), 216-217.
- [2] Furuta, Y., The genus field and genus number in algebraic number fields, Nagoya Math. J., **29** (1967), 281-285.
- [3] Furuta, Y., Über das Geschlecht und die Klassenzahl eines relativ-Galoisschen Zahlkörpers vom Primzahlgrad, Nagoya Math. J., **37** (1970), 197-200.
- [4] Hasse, H., Zahlentheorie, Akademie-Verlag, Berlin, 1963.
- [5] Hasse, H., "Bericht", Physica-Verlag, 1965.
- [6] Kuroda, S-N., Über die Klassenzahl eines relativ-zyklischen Zahlkörpers vom Primzahlgrad, Proc. Japan Akad., XL(1964), 623-626.
- [7] Yokoi, H., On the class number of a relatively cyclic number field, Nagoya Math. J., **29** (1967), 31-44.