# ON THE COMPUTATIONS OF THE INDICES OF THE GROUP OF NORM RESIDUES AND OF THE GROUP OF POWER RESIDUES WITHOUT EMPLOYING LOGARITHM*)

By

CHITOSE YAMASHITA

**1.** Let $K$ be a relatively cyclic algebraic number field over $k$ of degree $n$ and $s$ be a generating substitution of the Galois group of $K/k$. And we assume that the prime ideal $\mathfrak{p}$ in $k$ resolves in $K$ as $\mathfrak{p}=\mathfrak{P}^e$, where $\mathfrak{P}^s=\mathfrak{P}$.

The computation of the norm residue index in the class field theory is, as it is well known, reduced to the proof of the following equality in the above case;

$$(\alpha : \alpha_0 N_{K/k}\mathrm{A}) = e,$$

i. e., under the group $\alpha/\alpha_0$ of residue classes modulo $\mathfrak{p}^\lambda$, for sufficiently large $\lambda$, the index of the subgroup of classes represented by the norms of numbers A of $K$ is equal to $e$.

In the computation of this paper we introduce, for simplicity, the $\mathfrak{p}$-adic number field as usual, but we do not employ the logarithm, nor the group of $n$-th powers of numbers.

We can take $n$ numbers $s_i\Theta$ $(i=1, 2, \ldots, n)$ in the $\mathfrak{P}$-adic field $K_\mathfrak{P}$ which are conjugate with respect to $k_\mathfrak{p}$, and are linearly independent in $k_\mathfrak{p}$. In the sequel we use such numbers $s^i\Theta$, which are known as normal basis of $K_\mathfrak{P}/k_\mathfrak{p}$.

**2.** Without loss of generality we may assume that the numbers $s^i\Theta$ which constitute the normal basis are integers in $K_\mathfrak{P}$ and that the trace of $\Theta$ is an element of the prime ideal $\mathfrak{p}$, namely

$$\mathrm{Sp}\Theta = \sum s^i\Theta = \theta \in \mathfrak{p}. \tag{1}$$

If $\lambda \geqq 2$ and $\beta$ be an integer in $k_\mathfrak{p}$, we can take an integer $\gamma$ in $k_\mathfrak{p}$ such that

$$1 + \theta^{\lambda+1}\beta = N\mathrm{A} \quad \text{and} \quad \mathrm{A} = 1 + \theta^\lambda\gamma\Theta, \tag{2}$$

where $N\mathrm{A}$ is the norm of a number A in $K_\mathfrak{P}/k_\mathfrak{p}$.

PROOF. If we denote the $m$-th elementary symmetric function of $n$ numbers $s^i\Theta$ with $\theta_m$, from the equation

*) Received Oct. 6, 1949.

$$1 + \theta^{\lambda+1}\beta = N(1 + \theta^{\lambda}\gamma\Theta),$$

we have

$$1 + \theta^{\lambda+1}\beta = 1 + \theta^{\lambda}\gamma\theta + (\theta^{\lambda}\gamma)^2\theta_2 + \dots + (\theta^{\lambda}\gamma)^n\theta_n,$$

that is,

$$\theta\gamma + \theta^{\lambda-2}\theta_2(\theta\gamma)^2 + \theta^{2\lambda-3}\theta_3(\theta\gamma)^3 + \dots + \theta^{(n-1)\lambda-n}\theta_n(\theta\gamma)^n = \theta\beta.$$

This is an algebraic equation in $\theta\gamma$ of degree $n$ with integral coefficients in $k_{\mathfrak{p}}$, where the coefficient of $\theta\gamma$ is unity. Solving formally we get

$$\theta\gamma = \theta\beta - \theta^{\lambda-2}\theta_2(\theta\beta)^2 + \dots,$$

which is an infinite series of $\theta\beta$ with integral coefficients in $k_{\mathfrak{p}}$. Since $\theta\in\mathfrak{p}$, the infinite series converges as a $\mathfrak{p}$-adic number, and the sum is an element of the ideal $(\theta)$ in $k_{\mathfrak{p}}$, so that we can take an integer $\gamma$ in $k_{\mathfrak{p}}$, which satisfies the relation (2).

As far as the relation (2) is concerned, the integers $s^i\Theta$ need not constitute a normal basis, but they need only satisfy the relation (1).

In general let us represent the units in $K_{\mathfrak{P}}$ and $k_{\mathfrak{p}}$ (the integers which are prime to $\mathfrak{p}$) by $\mathrm{A}$ and $\alpha$ respectively. By $\alpha_0$ we understand the units $\alpha$ which satisfy the congruence $\alpha\equiv 1\ (\mathfrak{p}^{\lambda})$, where $\mathfrak{p}^{\lambda}\subset(\theta^3)$. Then from (2) we have, as groups of numbers, $\{\alpha_0\}\subset\{N\mathrm{A}\}$. Hence we have, as an index relation,

$$(\alpha : \alpha_0 N\mathrm{A}) = (\alpha : N\mathrm{A}). \tag{3}$$

**3.** As in the preceding section we take the fixed set of normal basis $s^i\Theta$, and we represent the set of numbers

$$\Gamma = \sum_{i=1}^{n}\beta_i s^i\Theta \tag{4}$$

by $\{\Gamma\}$, where $\beta$'s run through integers in $k_{\mathfrak{p}}$. $\{\Gamma\}$ is a subgroup of the additive group $\{\mathrm{B}\}$ of whole integers in $K_{\mathfrak{P}}$, and $\Gamma^s\in\{\Gamma\}$. Here we have $\beta\Gamma\in\{\Gamma\}$ and $\beta\theta=\sum\beta s^i\Theta\in\{\Gamma\}$, where $\beta$ represents an integer in $k_{\mathfrak{p}}$.

If $(1-s)\Gamma=0$, then we have $\Gamma=\beta\theta$, (5)

and if $\mathrm{Sp}\Gamma\in(\theta^{\lambda})$, then we have

$$\Gamma = (1-s)\Gamma' + \theta^{\lambda-1}\beta\Theta, \tag{6}$$

where $\lambda\geqq 1$ and $\Gamma'$ is a number of $\{\Gamma\}$.

PROOF OF (5). From (4) we have

$$(1-s)\Gamma = \sum_{i=1}^{n}(\beta_i - \beta_{i-1})s^i\Theta, \text{ where } \beta_0 = \beta_n.$$

As $n$ numbers $s^i\Theta$ are linearly independent in $k_{\mathfrak{p}}$ and $\sum(\beta_i-\beta_{i-1})s^i\Theta=0$ by the assumption, we have $\beta_i=\beta_{i-1}(i=1, 2, \dots, n$. Hence we can put $\beta_i=\beta$ and then from (4) we have $\Gamma=\sum\beta s^i\Theta=\beta\theta)$.

PROOF OF (6). From (4) we have $\mathrm{Sp}\,\Gamma=\sum\beta_i\theta$, and by the assumption $\sum\beta_i\theta\in(\theta^{\lambda})$. Hence we have $\sum\beta_i=\theta^{\lambda-1}\beta$. If we put $\beta'_0=\beta'_n=0$ and $\beta_1+\beta_2+\dots+\beta_i=\beta'_i$ $(i<n)$, we have $\beta_i=\beta'_i-\beta'_{i-1}$ $(i=1, 2, \dots, n-1)$ and

$\beta_n=\beta_n+\beta_1+\beta_2+\dots+\beta_{n-1}-\beta'_{n-1}=-\beta'_{n-1}+\sum\beta_i=\theta^{\lambda-1}\beta-\beta'_{n-1}=\beta'_n-\beta'_{n-1}+\theta^{\lambda-1}\beta$ since $\beta'_n=0$. Therefore we have

$$\begin{aligned}\Gamma &= \sum_{i=1}^{n}(\beta'_i-\beta'_{i-1})s^i\Theta+\theta^{\lambda-1}\beta s^n\Theta\\ &= (1-s)\Gamma'+\theta^{\lambda-1}\beta\Theta,\end{aligned}$$

where $\Gamma'=\sum\beta'_i s^i\Theta\in\{\Gamma\}$, because $\beta'_0=\beta'_n$.

**4.** If we take any integer B in $K_{\mathfrak{P}}$, then B and $s^i\Theta$ are linearly dependent. Hence we have a linear relation of integral coefficients in $k_{\mathfrak{p}}$;

$$\beta\mathrm{B}+\sum\beta_i s^i\Theta=0.$$

Since $s^i\Theta$ are linearly independent, $\beta\neq 0$, so that we can take some power $\theta^b$ of $\theta$ such that $\theta^b/\beta$ is an integer, for $\theta\in\mathfrak{p}$ in $\mathfrak{p}$-adic number field. Hence $\theta^b\mathrm{B}=-(\theta^b/\beta)\cdot\sum\beta_i s^i\Theta\in\{\Gamma\}$. Let $\theta^t$ be the highest power of $\theta$ among the corresponding $\theta^b$, when B represents each element of the absolute basis of the integers in $K_{\mathfrak{P}}$ with respect to the field of rational $p$-adic numbers. Then we have $\theta^t\mathrm{B}\in\{\Gamma\}$ for all integers B in $K_{\mathfrak{P}}$, and hence, for ideals in $K_{\mathfrak{P}}$ we have

$$(\theta^t)\subset\{\Gamma\}\subset(1). \tag{7}$$

If we put $\mathrm{A}_\lambda=1+\theta^\lambda\mathrm{B}$ for each integer $\lambda$, the set of numbers $\{\mathrm{A}_\lambda\}$ is the multiplicative group of the units A of $K_{\mathfrak{P}}$ such that $\mathrm{A}\equiv 1$ (mod. $(\theta^\lambda)$), and as sets of numbers we have

$$\{\mathrm{A}_{\lambda+t}\}\subset\{1+\theta^\lambda\Gamma\}\subset\{\mathrm{A}_\lambda\}.$$

*In the following we put* $\overline{\mathrm{A}}=1+\theta^\lambda\Gamma=1+\theta^\lambda\sum_{i=1}^{n}\beta_i s^i\Theta$ *for a fixed integer* $\lambda\geqq t+2$, *then we have*

$$\{\mathrm{A}_{2\lambda}\}\subset\{\mathrm{A}_{\lambda+t}\}\subset\{\overline{\mathrm{A}}\}\subset\{\mathrm{A}_\lambda\}.$$

$\{\overline{\mathrm{A}}\}$ *is a multiplicative group and* $\overline{\mathrm{A}}^s\in\{\overline{\mathrm{A}}\}$.

PROOF. The product of two numbers of $\{\overline{\mathrm{A}}\}$ is also a number of $\{\overline{\mathrm{A}}\}$ as follows;

$$(1+\theta^\lambda\Gamma)(1+\theta^\lambda\Gamma')=1+\theta^\lambda(\Gamma+\Gamma'+\theta^\lambda\Gamma\Gamma')\in\{\mathrm{A}\},$$

because $\theta^\lambda\Gamma\Gamma'\in(\theta^\lambda)\subset(\theta^t)\subset\{\Gamma\}$.

If for $\overline{\mathrm{A}}=1+\theta^\lambda\Gamma$ we put $\overline{\mathrm{A}}'=1-\theta^\lambda\Gamma$ and $\overline{\mathrm{A}}''=(\overline{\mathrm{A}}\,\overline{\mathrm{A}}')^{-1}$, we have

$$\overline{\mathrm{A}}''=(1-\theta^{2\lambda}\Gamma^2)^{-1}\in\{\mathrm{A}_{2\lambda}\}\subset\{\overline{\mathrm{A}}\},\quad \overline{\mathrm{A}}^{-1}=\overline{\mathrm{A}}'\overline{\mathrm{A}}''\in\{\overline{\mathrm{A}}\};$$

thus the inverse of any number of $\{\overline{\mathrm{A}}\}$ is also the number of $\{\overline{\mathrm{A}}\}$.

**5.** Let us put $\overline{\mathrm{A}}=\overline{\alpha}$ if $\overline{\mathrm{A}}^{1-s}=1$, and put $\overline{\mathrm{A}}=\overline{\mathrm{A}}^*$ if $N\overline{\mathrm{A}}=1$, then, as groups of numbers, we have

$$\{\overline{\alpha}\}=\{N\overline{\mathrm{A}}\}, \tag{8}$$

and

$$\{\overline{\mathrm{A}}^*\}=\{\overline{\mathrm{A}}^{1-s}\}, \tag{9}$$

PROOF. Let us put $\overline{\alpha}=1+\theta^\lambda\Gamma$. As $\overline{\alpha}^{1-s}=1$, $\overline{\alpha}=\overline{\alpha}^s$ and $(1-s)\overline{\alpha}=0$, we have $(1-s)\Gamma=0$, so that from (5) we have $\Gamma=\beta\theta$ and $\overline{\alpha}=1+\theta^\lambda\cdot\beta\theta$, thus from (2) we get $\alpha = NA$, $A = 1+\theta^\lambda\gamma\Theta \in \{1+\theta^\lambda\Gamma\} = \{\bar{A}\}$. Therefore we have the relation $\bar{\alpha} \in \{N\bar{A}\}$. Conversely, as $(N\bar{A})^{1-s} = 1$ and $N\bar{A} = \Pi(s^i\bar{A}) \in \{\bar{A}\}$, $N\bar{A} \in \{\bar{\alpha}\}$, so that the relation (8) is proved.

Now let us put $\bar{A}^* = 1+\theta^\lambda\Gamma$. As $1 = N\bar{A}^* = 1+\theta^\lambda \operatorname{Sp}\Gamma + (\theta^{2\lambda})$, we have $\operatorname{Sp}\Gamma \in (\theta^\lambda)$, so that from (6) we have

$$\Gamma = (1-s)\Gamma^1 + \theta^{\lambda-1}\beta\Theta.$$

Here let us put $\bar{A}' = 1+\theta^\lambda\Gamma'$ and $\bar{A}^*\bar{A}'^{s-1} = A$, then

$$\begin{aligned} A &= (1+\theta^\lambda\Gamma)(1+\theta^\lambda\Gamma')^{s-1} \\ &\equiv (1+\theta^\lambda\Gamma)(1-\theta^\lambda(1-s)\Gamma') && ((\theta^{2\lambda})) \\ &\equiv 1+\theta^\lambda(\Gamma-(1-s)\Gamma') && ((\theta^{2\lambda})) \\ &= 1+\theta^{2\lambda-1}\beta\Theta \equiv 1, && ((\theta^{3\lambda-1}), \\ A^{1+s+\dots+s^t} &\equiv 1 && ((\theta^{2\lambda-1})). \end{aligned}$$

Next let us put

$$B = \Theta + As\Theta + A^{1+s}s^2\Theta + \dots + A^{1+s+\dots+s^{n-2}}s^{n-1}\Theta,$$

where $s^i\Theta$ are the normal basis, then we get $B^sA = B$, because $A^{1+s+\dots+s^{n-1}} = NA = N(\bar{A}^*\bar{A}'^{s-1}) = 1$.

From
$$\begin{aligned} B-\theta &= B-\Theta-s\Theta-s^2\Theta-\dots-s^{n-1}\Theta \\ &= (A-1)s\Theta+(A^{1+s}-1)s^2\Theta+\dots \\ &\in (\theta^{2\lambda-1}) \subset (\theta^{\lambda+1+t}) \subset \{\theta^{\lambda+1}\Gamma\} \end{aligned}$$

(because $\lambda \geqq t+2$ and by (7)), we can put $B-\theta = \theta^{\lambda+1}\Gamma''$ and $\bar{A}'' = B/\theta = 1+\theta\Gamma'' \in \{\bar{A}\}$, so that we have $\bar{A}''^{1-s} = B^{1-s} = A = \bar{A}^*\bar{A}'^{s-1}$, $\bar{A}^* = (\bar{A}''\bar{A}')^{1-s} \in \{\bar{A}^{1-s}\}$. On the contrary, as $N(\bar{A}^{1-s}) = 1$ and $\bar{A}^{1-s} \in \{\bar{A}\}$, $\bar{A}^{1-s} \in \{\bar{A}^*\}$, so that the relation (9) is proved.

**6.** Let us represent the units in $K_{\mathfrak{P}}$ (integers in $K_{\mathfrak{P}}$ which are prime to $\mathfrak{p}$) by A in general, and put $A = A^*$ if $NA = 1$, then we have the relation of the index

$$(A^* : A^{1-s}) = e. \tag{10}$$

Proof. By Hilbert's lemma, for each $A^*$ we can take a number B in $K_{\mathfrak{P}}$ such that $A^* = B^{1-s}$. If we take an integer $\Pi$ in $K_{\mathfrak{P}}$ such that the exponential $\mathfrak{P}$-adic value $O(\Pi) = 1$, $E = \Pi^{1-s}$ is an unit in $K_{\mathfrak{P}}$ and $NE = 1$, so that $E \in \{A^*\}$. If $O(B) = m$ (positive or negative rational integer or zero), $A = B\Pi^{-m}$ is an unit, so that $B = \Pi^m A$, $A^* = B^{1-s} = E^m A^{1-s}$, hence $A^* \in \{E^m A^{1-s}\}$. Conversely $E^m A^{1-s} \in \{A^*\}$, so that we have

$$(A^* : A^{1-s}) = (E^m A^{1-s} : A^{1-s}).$$

It is thus sufficient to show that the condition $E^m \in \{A^{1-s}\}$ is equivalent to the divisibility of $m$ by $e$. In fact, if $\Pi^{m(1-s)} = E^m = A^{1-s}$, then $(\Pi^m/A)^{1-s} = 1$, $\Pi^m/A$ is a number in $k_{\mathfrak{p}}$, so that $m = O(\Pi^m/A)$ is divisible by $e$, because $\mathfrak{p} = \mathfrak{P}^e$ in $K_{\mathfrak{P}}/k_{\mathfrak{p}}$. Conversely, if $m$ is divisible by $e$, we can take a number $\rho$ in $k_{\mathfrak{p}}$ such that $O(\rho) = m$. Then $A = \Pi^m/\rho$ is an unit in $K_{\mathfrak{P}}$, so that $E^m = \Pi^{m(1-s)} = A^{1-s}$.

7. From (3) we can see that the index

$$(\alpha : NA) = (\alpha : \alpha_0 NA) = a$$

is a finite number. From (10) we have

$$\frac{(A^* : A^{1-s})}{(\alpha : NA)} = \frac{e}{a}.$$

$N(A^{1-s}) = (NA)^{1-s} = 1$, $A = A^*$ if and only if $NA = 1$ and $A = \alpha$ if and only if $A^{1-s} = 1$, so that we can apply Herbrand's lemma in (11). In place of the group $\{A\}$ of units, we take its subgroup $\{\bar{A}\}$, then, since $\{A_{\lambda+t}\} \subset \{\bar{A}\} \subset \{A\}$ and so the index $(A : \bar{A}) \leqq (A : A_{\lambda+t})$ is finite, we have

$$\frac{(\bar{A}^* : \bar{A}^{1-s})}{(\bar{\alpha} : N\bar{A})} = \frac{e}{a}.$$

Now, from (8) and (9) we have $(\bar{\alpha} : N\bar{A}) = 1$ and $(\bar{A}^* : \bar{A}^{1-s}) = 1$ respectively, so that $a = e$. Thus, for the index of the group of the norm residues, it is proved in $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ that

$$(\alpha : \alpha_0 NA) = (\alpha : NA) = e.$$

---

8. Now let us compute the index of the group of power residues. Let $n$ be a natural number and $\mathfrak{p}$ be a prime ideal in an algebraic number field $k$. It is also well known that, under the group of residue classes of numbers in $k$ modulo $\mathfrak{p}^\lambda$, for sufficiently large $\lambda$, the index of the subgroup of those which are represented by the $n$-th powers of numbers in $k$, that is, the index of the group of residues of $n$-th powers, is

$$(\alpha : \nu) = n'' N_k \mathfrak{p}^t, \; n' \leqq n'' \leqq n\,;$$

where $\mathfrak{p}^t$ is the $\mathfrak{p}$-component of $n$, and the number of the $n$-th roots of unity in $k$ is $n'$, (and the number of those in the $\mathfrak{p}$-adic number field $k_{\mathfrak{p}}$ is $n''$).

By the computation of this index, we introduce the $\mathfrak{p}$-adic number field $k_{\mathfrak{p}}$ as usual, but we do not employ the logarithm this time too.

Let $\alpha$ denote the numbers in $k_{\mathfrak{p}}$ which are prime to $\mathfrak{p}$ and let $\{\alpha\}$ be their multiplicative group. Let us put $\alpha = \alpha_\lambda$ if $\alpha \equiv 1 \; (n^\lambda \mathfrak{p})$, where $\lambda$ is any natural number. If $\alpha_\lambda = 1 + n^\lambda \beta$, $\beta$ is a number in $\mathfrak{p}$, and

$$(1 + n^\lambda \beta)^n \equiv 1 (n^{\lambda+1} \mathfrak{p}),$$

so that we have $\alpha_\lambda^n \in \{\alpha_{\lambda+1}\}$. Conversely if $\alpha_{\lambda+1} = 1 + n^{\lambda+1}\beta$, $\beta$ is a number in $\mathfrak{p}$, and we can take a number $\gamma$ in $\mathfrak{p}$ such that

$$1 + n^{\lambda+1}\beta = (1 + n^\lambda \gamma)^n,$$

so that we have $\alpha_{\lambda+1} \in \{\alpha_\lambda^n\}$. Therefore, as groups of numbers, we have $\{\alpha_\lambda^n\} = \{\alpha_{\lambda+1}\}$.

If $\zeta$ be a primitive $n$-th root of unity,

$$(1-\zeta)(1-\zeta^2)\dots(1-\zeta^{n-1})=n\not\equiv 0 \quad (n^\lambda\mathfrak{p}),$$

so that unity is the only $n$-th root of unity which is included in the group $\{\alpha_\lambda\}$.

By the correspondence of numbers $\alpha\to\alpha^n$, those which correspond to unity are the $n$-th roots of unity in $k_\mathfrak{p}$, and their number is $n''$, while only one of them is included in $\{\alpha_\lambda\}$, so that we have the relations between the indices of groups

$$\frac{(\alpha:\alpha_\lambda)}{n''}=(\alpha^n:\alpha_\lambda^n)=(\alpha^n:\alpha_{\lambda+1})=\frac{(\alpha:\alpha_{\lambda+1})}{(\alpha:\alpha^n)},$$

where $(\alpha:\alpha_\lambda)=\varphi(n^\lambda\mathfrak{p})$ and $(\alpha:\alpha_{\lambda+1})=\varphi(n^\lambda\mathfrak{p}\cdot\mathfrak{p}^t)=\varphi(n^\lambda\mathfrak{p})\cdot N_k\mathfrak{p}^t$ are finite numbers. Hence we have

$$(\alpha:\alpha^n)=n''N_k\mathfrak{p}^t.$$

Let us now put $\alpha=\alpha^*$ if $\alpha\equiv 1\ (\mathfrak{p}^\lambda)$, where $\lambda\geqq 2t+1$. As $\alpha^*\equiv 1(n^2\mathfrak{p})$, $\alpha^*\in\{\alpha_2\}=\{\alpha_1^n\}\subset\{\alpha^n\}$, so that we have in $k_\mathfrak{p}$

$$(\alpha:\nu)=(\alpha:\alpha^*\alpha^n)=(\alpha:\alpha^n).$$

This is the ratio of the number $(\alpha:\alpha^*)=\varphi(\mathfrak{p}^\lambda)$ of the cosets of $\{\alpha^*\}$ to the number $(\alpha^n\alpha^*:\alpha^*)$ of those which are represented by the $n$-th powers of numbers in $k_\mathfrak{p}$, so that this index in $k$ is the same as in $k_\mathfrak{p}$. Therefore the index of the group of the residues of $n$-th powers in $k$ modulo $\mathfrak{p}^\lambda$ $(\lambda\geqq 2t+1)$ is obtained;

$$(\alpha:\nu)=n''N_k\mathfrak{p}^t.$$

Tôhoku University, Sendai.