TOKYO J. MATH.
VOL. 7, No. 1, 1984

On Normal Integral Bases

Fuminori KAWAMOTO

Gakushuin University
(Communicated by T. Mitsui)

Introduction

Let k be a number field, and K/k a finite Galois extension with Galois group G. Let $\mathfrak{o}_k$ and $\mathfrak{o}_K$ be the rings of integers in k and K. We denote by $\mathfrak{o}_kG$ the group ring of G over $\mathfrak{o}_k$. $\mathfrak{o}_K$ can be regarded as an $\mathfrak{o}_kG$-module by the action $r\cdot\alpha=\sum_{s\in G}a_s s\alpha$ for $\alpha\in\mathfrak{o}_K$, $r=\sum_{s\in G}a_s s\in\mathfrak{o}_kG$. These notations will be used throughout this paper. K/k is said to have a *normal integral basis* (abbr. n.i.b.) when there is an element $\alpha\in\mathfrak{o}_K$ such that $\{s\alpha\}_{s\in G}$ is a relative integral basis of K/k, and α is called a *generator* of this basis. It is known that a finite Galois extension with n.i.b. is tamely ramified ([4], Chapter 9, Theorem (1, 2)).

In case where k is the field $\boldsymbol{Q}$ of rational numbers, every tamely ramified abelian field has an n.i.b. (Hilbert-Speiser), so that when $k=\boldsymbol{Q}$ and G is abelian, K/k has an n.i.b. if and only if K/k is tamely ramified ([4], Chapter 9, Theorem (3, 4)). Furthermore, Fröhlich [2] has given a necessary and sufficient condition for K/k to have an n.i.b., when K/k is a Kummer extension. On the other hand, Okutsu [8] has shown that when $k=\boldsymbol{Q}(\zeta_l)$, $\zeta_l=\exp(2\pi i/l)$, l: odd prime, and $K=k(\sqrt[l]{a})$, $a\in\boldsymbol{Z}$, K/k has always a relative integral basis and given an explicit form of this basis. After preparations in §1, giving in particular a more precise form to the results of [2], we shall apply them in §2 to obtain a necessary and sufficient condition for K/k to have an n.i.b. for the case where k and K are as in [8]. We shall also give explicitly a generator of n.i.b. when this exists. In the final §3, we shall construct many examples of normal extensions K/k with n.i.b.'s where $k\neq\boldsymbol{Q}$, and K/k are tamely ramified. We shall also mention an example of such K/k without n.i.b..

ACKNOWLEDGEMENT: The author wishes to thank Dr. K. Okutsu for his kind advice and encouragement. He also wishes to thank Mr. S. Nakano for his kind advice.

Received June 17, 1983

§1. Preparations.

Let K/k be tamely ramified. For each prime ideal $\mathfrak{p}$ of k, let $k_{\mathfrak{p}}$ be the $\mathfrak{p}$-adic completion of k and $\mathfrak{o}_{\mathfrak{p}}$ be the valuation ring of $k_{\mathfrak{p}}$. $k_{\mathfrak{p}}$-algebra $K_{\mathfrak{p}}$ is defined by $k_{\mathfrak{p}} \otimes_k K$. Then $k_{\mathfrak{p}}$ and K are naturally embedded in $K_{\mathfrak{p}}$. We define $\mathfrak{o}_{\mathfrak{p}}$-algebra $\mathfrak{o}_{K,\mathfrak{p}}$ by $\mathfrak{o}_{\mathfrak{p}} \otimes_{\mathfrak{o}_k} \mathfrak{o}_K$. As $\mathfrak{o}_{\mathfrak{p}}$ is a flat $\mathfrak{o}_k$-module, $\mathfrak{o}_{K,\mathfrak{p}}$ is also naturally embedded in $K_{\mathfrak{p}}$. Consequently $\mathfrak{o}_{\mathfrak{p}}$ and $\mathfrak{o}_K$ are naturally embedded in $\mathfrak{o}_{K,\mathfrak{p}}$. $M_{\mathfrak{p}}$ denotes $\mathfrak{o}_{\mathfrak{p}} \otimes_{\mathfrak{o}_k} M$ for an $\mathfrak{o}_k$-submodule M of K. If M is an $\mathfrak{o}_k$-lattice of the k-vector space K, then

$$M = K \cap (\bigcap_{\mathfrak{p}} M_{\mathfrak{p}}) , \tag{1}$$

where $\mathfrak{p}$ ranges over all prime ideals of k ([10], Theorem (5, 3)). Since a finite Galois extension K/k has a normal basis and $\mathfrak{o}_K$ is a projective $\mathfrak{o}_k G$-module, $\mathfrak{o}_{K,\mathfrak{p}}$ and $\mathfrak{o}_{\mathfrak{p}} G$ are isomorphic as $\mathfrak{o}_{\mathfrak{p}} G$-modules for any prime $\mathfrak{p}$ of k (Swan [9], Corollary 6, 4). Hence there is an element $\beta_{\mathfrak{p}} \in \mathfrak{o}_{K,\mathfrak{p}}$ such that $\{s\beta_{\mathfrak{p}}\}_{s \in G}$ is an $\mathfrak{o}_{\mathfrak{p}}$-basis of $\mathfrak{o}_{K,\mathfrak{p}}$. We call this $\beta_{\mathfrak{p}}$ a *generator* of local normal basis for $\mathfrak{p}$. $b \in K$ is a *generator* of global basis if and only if $\{sb\}_{s \in G}$ is a k-basis of K.

In the remainder of this section, we assume as in [2] K/k to be a finite tamely ramified Kummer extension of exponent n with Galois group G. $\hat{G}$ denotes the character group of G. If A is an abelian group, let $M(\hat{G}, A)$ be the set of maps from $\hat{G}$ into A. If we define the product of maps $f_1, f_2 \colon \hat{G} \to A$ by $f_1 f_2(\chi) = f_1(\chi) f_2(\chi)$ for $\chi \in \hat{G}$, $M(\hat{G}, A)$ becomes an abelian group. For a map $f \colon \hat{G} \to K_{\mathfrak{p}}$, define $f^*(s)$ by $(1/|G|) \sum_{\chi \in \hat{G}} \chi(s) f(x)$ for $s \in G$, where $|G|$ is the order of G. Since k contains a primitive n-th root of unity, f^* is the map from $\hat{G}$ into $K_{\mathfrak{p}}$. Let J_k be the idele group of k and U_k be $\prod_{\mathfrak{p}:\text{ finite}} \mathfrak{o}_{\mathfrak{p}}^{\times} \times \prod_{\mathfrak{p}_\infty} k_{\mathfrak{p}_\infty}^{\times}$, where $\mathfrak{p}$ ranges over all finite primes and $\mathfrak{p}_\infty$ all infinite primes of k. (For a ring R, $R^{\times}$ means the unit group of R.)

DEFINITION. For each prime ideal $\mathfrak{p}$ of k, let $M_0(\mathfrak{p})$ be the set of maps $f_{\mathfrak{p}} \colon \hat{G} \to \mathfrak{o}_{\mathfrak{p}}^{\times}$ satisfying $\operatorname{Im} f_{\mathfrak{p}}^* \subset \mathfrak{o}_{\mathfrak{p}}$. We define $M_0(\hat{G}, U_k)$ to be the set of maps $f = (f_{\mathfrak{p}}) \in M(\hat{G}, U_k)$ satisfying $f_{\mathfrak{p}} \in M_0(\mathfrak{p})$ for all prime ideals $\mathfrak{p}$.

It is easily seen that $M_0(\mathfrak{p})$ is a group and consequently $M_0(\hat{G}, U_k)$ is a subgroup of $M(\hat{G}, J_k)$. Let $\beta_{\mathfrak{p}} \in \mathfrak{o}_{K,\mathfrak{p}}$ be a generator of local normal basis for each $\mathfrak{p}$ and $b \in K$ be a generator of global normal basis. For an element $\alpha \in K_{\mathfrak{p}}$ and $\chi \in \hat{G}$, define $(\alpha|\chi) = \sum_{s \in G} \bar{\chi}(s) s\alpha$. Put $\varphi_{\mathfrak{p}}(\chi) = (\beta_{\mathfrak{p}}|\chi)/(b|\chi)$. Then $\varphi_{\mathfrak{p}}(\chi)$ is an element of $k_{\mathfrak{p}}^{\times}$. Putting $\varphi(\chi) = (\cdots, \varphi_{\mathfrak{p}}(\chi), \cdots) \in \prod_{\mathfrak{p}} k_{\mathfrak{p}}^{\times}$ for each $\chi \in \hat{G}$, we have $\varphi \in M(\hat{G}, J_k)$. The residue class of φ in the finite abelian group $M(\hat{G}, J_k)/M(\hat{G}, k^{\times}) M_0(\hat{G}, U_k)$ does not depend upon the choice of generators of global and local normal bases. The following lemma is proved in [2], §7, 7.2.

LEMMA 1. *Suppose that* $\mathfrak{p}$ *is a prime ideal of* k *and* $f_{\mathfrak{p}}$ *is a map from* $\hat{G}$ *into* $k_{\mathfrak{p}}$. *Set* $\alpha_{\mathfrak{p}}=(1/|G|)\sum_{\chi\in\hat{G}} f_{\mathfrak{p}}(\chi)(\beta_{\mathfrak{p}}|\chi)$. *Then* $\alpha_{\mathfrak{p}}$ *is a generator of local normal basis for* $\mathfrak{p}$ *if and only if* $f_{\mathfrak{p}}\in M_0(\mathfrak{p})$.

THEOREM 1. *A necessary and sufficient condition for* K/k *to have an* n.i.b. *is that* φ *lies in* $M(\hat{G}, k^{\times})M_0(\hat{G}, U_k)$. *If* $\varphi=gf$, $f=(f_{\mathfrak{p}})\in M_0(\hat{G}, U_k)$ *and* $g\in M(\hat{G}, k^{\times})$, *then* $(1/|G|)\sum_{\chi\in\hat{G}} g(\chi)(b|\chi)$ *generates an* n.i.b. *of* K/k.

PROOF. If K/k has an n.i.b., it is a local normal basis for each $\mathfrak{p}$ and a global normal basis at the same time. Hence we obtain $\varphi=1$. Conversely, if φ has the above decomposition, we have for all $\mathfrak{p}$ and all $\chi\in\hat{G}$

$$f_{\mathfrak{p}}^{-1}(\chi)(\beta_{\mathfrak{p}}|\chi)=g(\chi)(b|\chi)\ . \tag{2}$$

Let $\alpha_{\mathfrak{p}}$ be $(1/|G|)\sum_{\chi\in\hat{G}} f_{\mathfrak{p}}^{-1}(\chi)(\beta_{\mathfrak{p}}|\chi)$. Since $M_0(\mathfrak{p})$ is a group, we have $f_{\mathfrak{p}}^{-1}\in M_0(\mathfrak{p})$. Therefore $\alpha_{\mathfrak{p}}$ is a local normal basis for $\mathfrak{p}$ by Lemma 1. But $\alpha_{\mathfrak{p}}$ is independent of each $\mathfrak{p}$ by (2). So we may set $\alpha_{\mathfrak{p}}=\alpha=(1/|G|)\sum_{\chi\in\hat{G}} g(\chi)$ $(b|\chi)$. Then for all $\mathfrak{p}$,

$$\mathfrak{o}_{K,\mathfrak{p}}=\bigoplus_{s\in G}\mathfrak{o}_{\mathfrak{p}}s\alpha=(\bigoplus_{s\in G}\mathfrak{o}_k s\alpha)_{\mathfrak{p}}\ .$$

Hence, by (1), we have $\mathfrak{o}_K=\bigoplus_{s\in G}\mathfrak{o}_k s\alpha$. This proves our theorem.

§2. In case $k=\boldsymbol{Q}(\zeta_l)$, $K=k(\sqrt[l]{a})$.

In this §, we consider as in [8] the case $k=\boldsymbol{Q}(\zeta_l)$, $K=k(\sqrt[l]{a})$ where l is an odd prime, ζ_l is a primitive l-th root of unity, $a(\neq\pm1)$ is a rational integer without l-th power factor. a has the decomposition $\prod_{i=1}^{l-1}a_i^i$, where the a_i's are square-free integers and $(a_i, a_j)=1$ $(i\neq j)$. Put $\omega=(\sqrt[l]{a}-a)/(1-\zeta_l)$ and $b_m=\prod_{i=1}^{l-1}a_i^{[im/l]}$ $(0\leqq m\leqq l-1)$, where $[x]$ is the greatest integer$\leqq x$ as usual. The following theorem is proved in [8].

OKUTSU'S THEOREM. $(1-\zeta_l)\mathfrak{o}_k$ *is unramified in* K/k *if and only if* $a^{l-1}\equiv1 \bmod l^2$. *Furthermore* $\{\omega^m/b_m\}_{0\leqq m\leqq l-1}$ *is a relative integral basis of* K/k *when* $(1-\zeta_l)\mathfrak{o}_k$ *is unramified. And the discriminant of* K/k *is* $\prod_{i=1}^{l-1}a_i^{l-1}$.

Now assume K/k is tamely ramified extension, i.e. $a^{l-1}\equiv1 \bmod l^2$. Let σ be a fixed generator of G, say $\sigma\sqrt[l]{a}=\sqrt[l]{a}\,\xi_l$ and χ be a fixed generator of $\hat{G}$, say $\chi(\sigma)=\zeta_l^{-1}$. We write $\zeta=\zeta_l$.

LEMMA 2. *Suppose that* α *is an element of* $\mathfrak{o}_K$ *and write* $\alpha=\sum_{m=0}^{l-1} u_m(\omega^m/b_m)$ $(u_m \in \mathfrak{o}_k)$. *Therefore there exists a matrix* A *in* $M_l(\mathfrak{o}_k)$ *such that* $(\alpha, \sigma\alpha, \cdots, \sigma^{l-1}\alpha)=(1, \omega/b_1, \cdots, \omega^{l-1}/b_{l-1})\,A$. *Then*

$$(3)\qquad (\alpha|\chi^j)=\frac{l}{(\zeta-1)^{l-1}}\frac{(-\sqrt[l]{a})^{l-j}}{b_{l-j}}\varepsilon_{l-j} \qquad (1\leqq j\leqq l)$$

and

$$(4)\qquad \det A=\zeta^{l(l-1)(l+1)/6}\cdot\prod_{i=2}^{l-1} t_i^{l-i}\prod_{j=0}^{l-1}\varepsilon_j\ ,$$

where $t_i=(\zeta^i-1)/(\zeta-1)$ *and* $\varepsilon_j=\sum_{m=j}^{l-1}(\zeta-1)^{l-1-m}\binom{m}{j}(a^{m-j}b_j/b_m)u_m$.

REMARK. The t_i's are units of k. Since $b_m|a$ $(0\leqq m\leqq l-1)$, the $a^{m-j}b_j/b_m$'s are rational integers. So we note that the ε_j's are elements of $\mathfrak{o}_k$.

PROOF OF LEMMA 2. We shall calculate $(\alpha|\chi^j)$ in the first place.

$$\begin{aligned}(\alpha|\chi^j)&=\sum_{i=0}^{l-1}\bar{\chi}^j(\sigma^i)\sum_{m=0}^{l-1}\frac{u_m}{b_m(1-\zeta)^m}(\sigma^i\sqrt[l]{a}-a)^m\\&=\sum_{m=0}^{l-1}\frac{u_m}{b_m(1-\zeta)^m}\sum_{i=0}^{l-1}\bar{\chi}^j(\sigma^i)\sum_{p=0}^{m}\binom{m}{p}(\sigma^i\sqrt[l]{a})^p(-a)^{m-p}\\&=\sum_{m=0}^{l-1}\frac{u_m}{b_m(1-\zeta)^m}\sum_{p=0}^{m}\binom{m}{p}(-a)^{m-p}(\sqrt[l]{a}^p|\chi^j)\ .\end{aligned}$$

And

$$\sqrt[l]{a}^p|\chi^j=\sqrt[l]{a}^p\sum_{i=0}^{l-1}\zeta^{i(j+p)}=\begin{cases}l\sqrt[l]{a}^p & \text{if } l\,|\,j+p\\ 0 & \text{if } l\nmid j+p\ .\end{cases}$$

Since $l|j+p$ is equivalent to $j+p=l$, we have

$$\begin{aligned}(\alpha|\chi^j)&=\sum_{m=l-j}^{l-1}\frac{u_m}{b_m(1-\zeta)^m}\binom{m}{l-j}(-a)^{m-(l-j)}l\sqrt[l]{a}^{l-j}\\&=l(-\sqrt[l]{a})^{l-j}\sum_{m=l-j}^{l-1}\frac{u_m}{b_m(\zeta-1)^m}\binom{m}{l-j}a^{m-(l-j)}\\&=\frac{l}{(\zeta-1)^{l-1}}\frac{(-\sqrt[l]{a})^{l-j}}{b_{l-j}}\varepsilon_{l-j}\ .\end{aligned}$$

For $\alpha_0, \cdots, \alpha_{l-1}\in K$, put $\Delta_{K/k}(\alpha_0, \cdots, \alpha_{l-1})=\det(\sigma^i\alpha_j)_{0\leqq i,j\leqq l-1}$. Then

$$(5)\qquad \Delta_{K/k}(\alpha, \sigma\alpha, \cdots, \sigma^{l-1}\alpha)=\Delta_{K/k}\left(1, \frac{\omega}{b_1}, \cdots, \frac{\omega^{l-1}}{b_{l-1}}\right)\det A\ .$$

Put $\theta=\sqrt[l]{a}-a$ and $\Delta=(-1)^{l(l-1)/2}\cdot\prod_{1\leq i<j\leq l}(\zeta^i-\zeta^j)$. By $\sigma^i\theta-\sigma^j\theta=\sqrt[l]{a}(\zeta^i-\zeta^j)$, we have

$$(6)\qquad \Delta_{K/k}\left(1, \frac{\omega}{b_1}, \cdots, \frac{\omega^{l-1}}{b_{l-1}}\right)=\left\{(1-\zeta)^{l(l-1)/2}\prod_{m=1}^{l-1}b_m\right\}^{-1}\Delta_{K/k}(1, \theta, \cdots, \theta^{l-1})$$
$$=\left\{(1-\zeta)^{l(l-1)/2}\prod_{m=1}^{l-1}b_m\right\}^{-1}a^{(l-1)/2}\Delta\ .$$

By using orthogonality relations of the character group of a finite abelian group, we obtain ([2], §7, (7, 2))

$$\prod_{j=1}^{l}(\alpha|\chi^j)=\det(\sigma^i\sigma^{-j}\alpha)_{0\leq i,j\leq l-1}=(-1)^{(l-1)/2}\Delta_{K/k}(\alpha, \sigma\alpha, \cdots, \sigma^{l-1}\alpha)\ .$$

Therefore by (3),

$$(7)\qquad \Delta_{K/k}(\alpha, \sigma\alpha, \cdots, \sigma^{l-1}\alpha)=\left\{(\zeta-1)^{l(l-1)}\prod_{j=0}^{l-1}b_j\right\}^{-1}l^l a^{(l-1)/2}\prod_{j=0}^{l-1}\varepsilon_j\ .$$

By (5), (6), (7), we have

$$\det A=(-1)^{l(l-1)/2}l^l(\zeta-1)^{-(l(l-1)/2)}\Delta^{-1}\prod_{j=0}^{l-1}\varepsilon_j\ .$$

Since $\Delta^2=(-1)^{l(l-1)/2}\prod_{i=1}^{l}f'(\zeta^i)=(-1)^{l(l-1)/2}l^l$ ($f(x)=x^l-1$), we have $\det A=\zeta^{l(l-1)(l+1)/6}\cdot\prod_{i=2}^{l-1}t_i^{l-i}\prod_{j=0}^{l-1}\varepsilon_j$. This proves our lemma.

THEOREM 2. *Suppose that l is an odd prime and $a(\neq\pm1)$ is a rational integer without l-th power factor such that $a^{l-1}\equiv 1 \bmod l^2$. Then a necessary and sufficient condition for $\boldsymbol{Q}(\zeta_l, \sqrt[l]{a})/\boldsymbol{Q}(\zeta_l)$ to have an* n.i.b. *is that there are units u_j ($j=0, \cdots, l-1$) of $\boldsymbol{Q}(\zeta_l)$ such that*

$$(8)\qquad \sum_{j=0}^{l-1}\binom{l-1}{j}\zeta_l^{ij}u_j a^{l-1-j}b_j\equiv 0 \bmod l$$

for any $i=0, \cdots, l-1$.

Furthermore, if there are such u_j's, then $(1/l)\sum_{i=0}^{l-1}u_j^{-1}((-\sqrt[l]{a})^j/b_j)$ *generates an* n.i.b. *of $\boldsymbol{Q}(\zeta_l, \sqrt[l]{a})/\boldsymbol{Q}(\zeta_l)$.*

PROOF. As we are used to in this section, we write $k=\boldsymbol{Q}(\zeta)$ and $K=\boldsymbol{Q}(\zeta, \sqrt[l]{a})$. Let $\beta_\mathfrak{p}\in\mathfrak{o}_{K,\mathfrak{p}}$ be a generator of local normal basis for each prime ideal $\mathfrak{p}$ of k and $b\in\mathfrak{o}_K$ be a generator of global normal basis of K/k. We write $b=\sum_{m=0}^{l-1}u_m(\omega^m/b_m)(u_m\in\mathfrak{o}_k)$. We note that $\{\omega^m/b_m\}_{0\leq m\leq l-1}$ is also an $\mathfrak{o}_{\mathfrak{p}}$-basis of $\mathfrak{o}_{K,\mathfrak{p}}$. Hence we can write $\beta_{\mathfrak{p}}=\sum_{m=0}^{l-1} u_{m,\mathfrak{p}}(\omega^m/b_m)(u_{m,\mathfrak{p}}\in\mathfrak{o}_{\mathfrak{p}})$. Then we can hold the results for $\beta_{\mathfrak{p}}$ similar to the calculations of Lemma 2. Therefore, if we put $\varepsilon_{j,\mathfrak{p}}=\sum_{m=j}^{l-1}(\zeta-1)^{l-1-m}\binom{m}{j}(a^{m-j}b_j/b_m)u_{m,\mathfrak{p}}$, we obtain for each $\mathfrak{p}$ and $j=1,\cdots,l$, by (3),

$$\varphi_{\mathfrak{p}}(\chi^j)=\frac{(\beta_{\mathfrak{p}}|\chi^j)}{(b|\chi^j)}=\frac{\varepsilon_{l-j,\mathfrak{p}}}{\varepsilon_{l-j}}.$$

Now we put $f_{\mathfrak{p}}(\chi^j)=\varepsilon_{l-j,\mathfrak{p}}$ and $g(\chi^j)=\varepsilon_{l-j}^{-1}$. Since $\beta_{\mathfrak{p}}$ and b are local and global normal bases, we have $f=(f_{\mathfrak{p}})\in M(\hat{G},U_k)$ and $g\in M(\hat{G},k^\times)$ by (4). Let $\varphi=g'f'$, $f'\in M(\hat{G},U_k)$ and $g'\in M(\hat{G},k^\times)$ be another decomposition of φ. Then it is easy to see that there is $u\in M(\hat{G},\mathfrak{o}_k^\times)$ such that $f'=uf$ and $g'=u^{-1}g$. Hence, by Theorem 1, K/k has an n.i.b. if and only if there is $u\in M(\hat{G},\mathfrak{o}_k^\times)$ such that $uf_{\mathfrak{p}}\in M_0(\mathfrak{p})$ for every prime ideal $\mathfrak{p}$ of k. Since $(uf_{\mathfrak{p}})^*(\sigma^i)=(1/l)\sum_{j=0}^{l-1}\zeta^{ij}u(\chi^{l-j})\varepsilon_{j,\mathfrak{p}}$ $(0\leqq i\leqq l-1)$, it is sufficient to show $uf_{\mathfrak{p}}\in M_0(\mathfrak{p})$ only for a prime ideal of k dividing l for proving that $uf_{\mathfrak{p}}\in M_0(\mathfrak{p})$ takes place for all $\mathfrak{p}$'s. Now let $\mathfrak{p}|l$. Putting $u_{0,\mathfrak{p}}=\cdots=u_{l-2,\mathfrak{p}}=0$ and $u_{l-1,\mathfrak{p}}=b_{l-1}$, by $l\nmid a$, we have $\varepsilon_{j,\mathfrak{p}}=\binom{l-1}{j}a^{l-1-j}b_j\in\mathfrak{o}_{\mathfrak{p}}^\times$ $(0\leqq j\leqq l-1)$. Therefore $\beta_{\mathfrak{p}}=\omega^{l-1}$ generates a local normal basis for $\mathfrak{p}$ by (4). Then

$$(uf_{\mathfrak{p}})^*(\sigma^i)=\frac{1}{l}\sum_{j=0}^{l-1}\binom{l-1}{j}\zeta^{ij}u(\chi^{l-j})a^{l-1-j}b_j \qquad (0\leqq i\leqq l-1).$$

Setting $u_j=u(\chi^{l-j})$, the first part of the theorem is established. By (3),

$$\frac{1}{|G|}\sum_{j=1}^{l}u^{-1}g(\chi^j)(b|\chi^j)=\frac{1}{(\zeta-1)^{l-1}}\sum_{j=0}^{l-1}u_j^{-1}\frac{(-\sqrt[l]{a})^j}{b_j}.$$

This gives a generator of the n.i.b. by Theorem 1. Since $(\zeta-1)^{l-1}/l\in\mathfrak{o}_k^\times$, $(1/l)\sum_{j=0}^{l-1}u_j^{-1}((-\sqrt[l]{a})^j/b_j)$ is also a generator and the proof is completed.

Now we examine the case in which (8) holds for $u_j=b_j=1$ $(j=0,\cdots,l-1)$. Let $\mathfrak{p}=(\zeta-1)\mathfrak{o}_k$. Since $\sum_{j=0}^{l-1}\binom{l-1}{j}\zeta^{ij}a^{l-1-j}=(a+\zeta^i)^{l-1}=(a+1+\zeta^i-1)^{l-1}$ and $l=\mathfrak{p}^{l-1}$, (8) implies $a\equiv -1 \bmod l$. By the definition, $b_j=1$ $(j=0,\cdots,l-1)$ means that a is a square-free integer. Furthermore $a^{l-1}\equiv 1 \bmod l^2$ and $a\equiv -1 \bmod l$ mean $a\equiv -1 \bmod l^2$, and since l is an odd prime, we have $k(\sqrt[l]{a})=k(\sqrt[l]{-a})$. By Theorem 2, we obtain the following theorem.

THEOREM 3. *Suppose that l is odd prime and a $(\neq\pm1)$ is square-free rational integer such that $a\equiv\pm1 \bmod l^2$. Then $\alpha=(1/l)\sum_{j=0}^{l-1}(-\sqrt[l]{\varepsilon a})^j$ generates an* n.i.b. *of $\boldsymbol{Q}(\zeta_l,\sqrt[l]{a})/\boldsymbol{Q}(\zeta_l)$, where*

$$\varepsilon=\begin{cases} 1 & if \quad a\equiv -1 \bmod l^2 \\ -1 & if \quad a\equiv 1 \bmod l^2 . \end{cases}$$

COROLLARY. *Let l, a and α be as in Theorem 3. Then $\zeta_l\alpha$ generates an* n.i.b. *of the non-abelian extension* $\boldsymbol{Q}(\zeta_l, \sqrt[l]{a})/\boldsymbol{Q}$.

PROOF. Since $\boldsymbol{Q}(\zeta_l, \sqrt[l]{a})=\boldsymbol{Q}(\zeta_l, \sqrt[l]{-a})$, we may prove in case where $a\equiv -1 \bmod l^2$. Put $\Gamma=\mathrm{Gal}(K/\boldsymbol{Q})$. Let σ, τ be fixed elements of Γ, say $\sigma\zeta=\zeta$, $\sigma\sqrt[l]{a}=\sqrt[l]{a}\zeta$, $\tau\zeta=\zeta^g$ and $\tau\sqrt[l]{a}=\sqrt[l]{a}$, where g is a primitive root mod l. Then we have $\Gamma=\{\sigma^i\tau^j|i=0, \cdots, l-1, \ j=1, \cdots, l-1\}$. By Theorem 3, we obtain $\mathfrak{o}_K=\bigoplus_{i=0}^{l-1}\mathfrak{o}_k\sigma^i\alpha$ and also $\mathfrak{o}_k=\bigoplus_{j=1}^{l-1}\boldsymbol{Z}\tau^j\zeta$. Consequently, we have $\mathfrak{o}_K=\bigoplus_{i=0}^{l-1}\bigoplus_{j=1}^{l-1}\boldsymbol{Z}\sigma^i\alpha\tau^j\zeta$. Since α has the explicit form given above, we have $\sigma^i\tau^j(\zeta\alpha)=\sigma^i\alpha\tau^j\zeta$. Hence we have $\mathfrak{o}_K=\bigoplus_{i=0}^{l-1}\bigoplus_{j=1}^{l-1}\boldsymbol{Z}\sigma^i\tau^j(\zeta\alpha)$ and this proves our corollary.

§3. Examples of K/k with or without n.i.b..

We can construct many examples of normal extensions K/k with n.i.b., $k\neq\boldsymbol{Q}$, using our theorem 3, its corollary and Hilbert-Speiser's theorem in the abelian extensions of $\boldsymbol{Q}$ on ground of the following lemma 3.

NOTATIONS. For an extension K/k, $d_{K/k}$, $D_{K/k}$ mean the discriminant and the different of K/k, respectively. Let K/k be of degree n. If $\alpha_1, \cdots, \alpha_n\in K$, $d_{K/k}(\alpha_1, \cdots, \alpha_n)$ denotes the discriminant of $\alpha_1, \cdots, \alpha_n$.

LEMMA 3. *Suppose that K_1/k is a Galois extension of degree n and K_2/k is an extension of degree m, where $K_1\cap K_2=k$. Let L be the composite field of K_1 and K_2. Suppose $(d_{K_1/k}, d_{K_2/k})=1$.*

(i) *If $\{\alpha_i\}_{i=1,\cdots,n}$ is a relative (normal) integral basis of K_1/k, then it is also a relative (normal) integral basis of L/K_2.*

(ii) *If $\{\alpha_i\}_{i=1,\cdots,n}$ and $\{\beta_j\}_{j=1,\cdots,m}$ are relative integral bases of K_1/k and K_2/k, then $\{\alpha_i\beta_j\}_{i=1,\cdots,n,j=1,\cdots,m}$ is a relative integral basis of L/k.*

PROOF. (ii) is well-known (Cf. Lang [3], Chapter III, Proposition 17). Through (i) seems also known, a proof of (i) will be given here, as no reference for it is known to the author.

As $(d_{K_1/k}, d_{K_2/k})=1$, we have $D_{K_1/k}=D_{L/K_2}$ (Cf. Lang [3], Chapter III, Proposition 17). Since K_1/k and L/K_2 are Galois extensions of degree n, $d_{K_1/k}=D^n_{K_1/k}$ and $d_{L/K_2}=D^n_{L/K_2}$. Hence $d_{K_1/k}=d_{L/K_2}$. By the hypothesis, $d_{K_1/k}=d_{K_1/k}(\alpha_1, \cdots, \alpha_n)$ (Mann [5], Theorem 1). Therefore $d_{L/K_2}=d_{L/K_2}(\alpha_1, \cdots, \alpha_n)$. Consequently $\{\alpha_i\}_{i=1,\cdots,n}$ is a relative integral basis of L/K_2 (Mann [5], Theorem 1 Corollary).

In the following proposition, suppose that l_i is an odd prime and $a_i(\neq\pm1)$ is a square-free rational integer such that $a_i\equiv\pm1 \bmod l_i^2$ and put $\alpha_i=(1/l_i)\sum_{j=0}^{l_i-1}(-\sqrt[l_i]{\varepsilon_i a_i})^j$, where

$$\varepsilon_i=\begin{cases}-1 & \text{if } a_i\equiv 1 \bmod l_i^2 \\ 1 & \text{if } a_i\equiv -1 \bmod l_i^2\end{cases} \quad (1\leqq i\leqq s)\,.$$

PROPOSITION 1. (I) *Let k be an abelian extension of $\boldsymbol{Q}$ whose conductor n is odd and square-free (i.e. $k/\boldsymbol{Q}$ is tamely ramified). Let K be a number field such that $(d_{K/\boldsymbol{Q}}, n)=1$. Then* $\mathrm{Tr}_{\boldsymbol{Q}(\zeta_n)/k}(\zeta_n)$ *generates an* n.i.b. *of the abelian extension kK/K.* ($\mathrm{Tr}_{\boldsymbol{Q}(\zeta_n)/k}(\zeta_n)$ *denotes the trace of ζ_n in $\boldsymbol{Q}(\zeta_n)/k$ and ζ_n is a primitive n-th root of unity.*)

(II) *Let k be as in* (I) *and $a_1, \cdots, a_s, l_1, \cdots, l_s$ be pairwise prime and suppose $(n, \prod_{i=1}^s a_i l_i)=1$. Then $\prod_{i=1}^s \alpha_i\cdot\zeta_{l_1\cdots l_s}\cdot\mathrm{Tr}_{\boldsymbol{Q}(\zeta_n)/k}(\zeta_n)$ generates an* n.i.b. *of the non-abelian extension $k(\sqrt[l_1]{a_1}, \cdots, \sqrt[l_s]{a_s}, \zeta_{l_1\cdots l_s})/\boldsymbol{Q}$.*

(III) *Let k be a number field and $a_1, \cdots, a_s, l_1, \cdots, l_s$ be pairwise prime and suppose $(d_{k/\boldsymbol{Q}}, \prod_{i=1}^s a_i l_i)=1$. Then $\prod_{i=1}^s \alpha_i\cdot\zeta_{l_1\cdots l_s}$ generates an* n.i.b. *of the non-abelian extension $k(\sqrt[l_1]{a_1}, \cdots, \sqrt[l_s]{a_s}, \zeta_{l_1\cdots l_s})/k$.*

(IV) *Let n be the product of all the distinct primes among $l_1, \cdots, l_s$. Let k be a number field which contains ζ_n and m be an odd and square-free integer. Suppose $a_1, \cdots, a_s$ are pairwise prime and $(l_i, a_j)=1$ $(1\leqq i, j\leqq s)$. Suppose $(m, n\prod_{i=1}^s a_i)=1$, $(d_{k/\boldsymbol{Q}(\zeta_n)}, m\prod_{i=1}^s a_i)=1$ and $\boldsymbol{Q}(\sqrt[l_1]{a_1}, \cdots, \sqrt[l_s]{a_s}, \zeta_{mn})\cap k=\boldsymbol{Q}(\zeta_n)$. Then $\prod_{i=1}^s \alpha_i\zeta_m$ generates an* n.i.b. *of the abelian extension $k(\sqrt[l_1]{a_1}, \cdots, \sqrt[l_s]{a_s}, \zeta_{mn})/k$.*

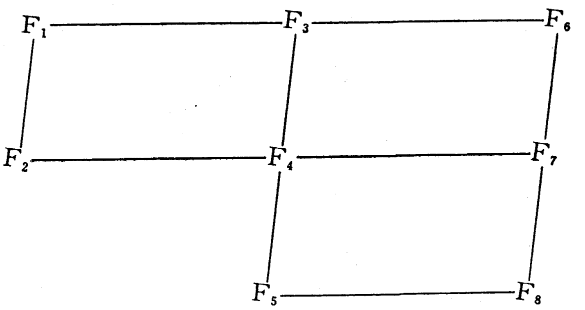
PROOF. (I) Since ζ_l generates an n.i.b. of $\boldsymbol{Q}(\zeta_l)/\boldsymbol{Q}$ (l: odd prime), ζ_n generates, by Lemma 3 (ii), an n.i.b. of $\boldsymbol{Q}(\zeta_n)/\boldsymbol{Q}$. Hence $\mathrm{Tr}_{\boldsymbol{Q}(\zeta_n)/k}(\zeta_n)$ generates an n.i.b. of $k/\boldsymbol{Q}$ ([4], Chapter 9, Theorem (3, 4)). As $(d_{K/\boldsymbol{Q}}, n)=1$, we have $K\cap k=\boldsymbol{Q}$. Therefore, by Lemma 3 (i), $\mathrm{Tr}_{\boldsymbol{Q}(\zeta_n)/k}(\zeta_n)$ generates an n.i.b. of kK/K.

(II) We note $d_{\boldsymbol{Q}(\zeta_{l_i}, \sqrt[l_i]{a_i})/\boldsymbol{Q}(\zeta_{l_i})}=(a_i^{l_i-1})$ by Okutsu's theorem. Hence only prime divisors of $a_i l_i$ ramify in $\boldsymbol{Q}(\zeta_{l_i}, \sqrt[l_i]{a_i})/\boldsymbol{Q}$. Therefore, since $a_1, \cdots, a_s, l_1, \cdots, l_s$ are pairwise prime, $\prod_{i=1}^s \alpha_i\zeta_{l_1\cdots l_s}$ generates, by Corollary of Theorem 3 and Lemma 3 (ii), an n.i.b. of $\boldsymbol{Q}(\sqrt[l_1]{a_1}, \cdots, \sqrt[l_s]{a_s}, \zeta_{l_1\cdots l_s})/\boldsymbol{Q}$. As $(n, \prod_{i=1}^s a_i l_i)=1$, we have $k\cap\boldsymbol{Q}(\sqrt[l_1]{a_1}, \cdots, \sqrt[l_s]{a_s}, \zeta_{l_1\cdots l_s})=\boldsymbol{Q}$. In (I), we have seen that $\mathrm{Tr}_{\boldsymbol{Q}(\zeta_n)/k}(\zeta_n)$ generates an n.i.b. of $k/\boldsymbol{Q}$. Consequently, by Lemma 3 (ii), $\prod_{i=1}^s \alpha_i\cdot\zeta_{l_1\cdots l_s}\cdot\mathrm{Tr}_{\boldsymbol{Q}(\zeta_n)/k}(\zeta_n)$ generates an n.i.b. of $k(\sqrt[l_1]{a_1}, \cdots, \sqrt[l_s]{a_s}, \zeta_{l_1\cdots l_s})/\boldsymbol{Q}$.

(III) As $(d_{k/\boldsymbol{Q}}, \prod_{i=1}^s a_i l_i)=1$, we have $k\cap\boldsymbol{Q}(\sqrt[l_1]{a_1}, \cdots, \sqrt[l_s]{a_s}, \zeta_{l_1\cdots l_s})=\boldsymbol{Q}$. Hence, using Lemma 3 (i) in place of Lemma 3 (ii) which is used in (II), we can show that $\prod_{i=1}^s \alpha_i\cdot\zeta_{l_1\cdots l_s}$ generates an n.i.b. of $k(\sqrt[l_1]{a_1}, \cdots,$

$\sqrt[l_s]{a_s}, \zeta_{l_1\cdots l_s})/k$.

(IV) In the first place, we shall show by induction in s that $\prod_{i=1}^{s} \alpha_i$ generates an n.i.b. of $\boldsymbol{Q}(\sqrt[l_1]{a_1}, \cdots, \sqrt[l_s]{a_s}, \zeta_n)/\boldsymbol{Q}(\zeta_n)$. Let n_r be the product of all the distinct primes among $l_1, \cdots, l_r$ $(1 \leqq r \leqq s)$. The case $s=1$ is just Theorem 3 $(n=n_s=l_1)$. To prove that $\prod_{i=1}^{s} \alpha_i$ generates an n.i.b. of $\boldsymbol{Q}(\sqrt[l_1]{a_1}, \cdots, \sqrt[l_s]{a_s}, \zeta_{n_s})/\boldsymbol{Q}(\zeta_{n_s})$ for $s=r+1$ assuming it true for $s=r$, we put $F_1=\boldsymbol{Q}(\zeta_{n_r}, \sqrt[l_1]{a_1}, \cdots, \sqrt[l_r]{a_r})$, $F_2=\boldsymbol{Q}(\zeta_{n_r})$, $F_3=\boldsymbol{Q}(\zeta_{n_{r+1}}, \sqrt[l_1]{a_1}, \cdots, \sqrt[l_r]{a_r})$,



$F_4=\boldsymbol{Q}(\zeta_{n_{r+1}})$, $F_5=\boldsymbol{Q}(\zeta_{l_{r+1}})$, $F_6=\boldsymbol{Q}(\zeta_{n_{r+1}}, \sqrt[l_1]{a_1}, \cdots, \sqrt[l_{r+1}]{a_{r+1}})$, $F_7=\boldsymbol{Q}(\zeta_{n_{r+1}}, \sqrt[l_{r+1}]{a_{r+1}})$ and $F_8=\boldsymbol{Q}(\zeta_{l_{r+1}}, \sqrt[l_{r+1}]{a_{r+1}})$. If $l_{r+1}|n_r$, we have $n_{r+1}=n_r$, $F_3=F_1$ and $F_4=F_2$. Then, by the hypothesis of induction, $\prod_{i=1}^{s} \alpha_i$ generates an n.i.b. of F_3/F_4. If $l_{r+1}\nmid n_r$, we have $n_{r+1}=n_r l_{r+1}$. By Okutsu's theorem, prime ideals ramified in F_1/F_2 divide $\prod_{i=1}^{r} a_i$. And only prime divisors of l_{r+1} ramify in F_4/F_2. As $(l_{r+1}, \prod_{i=1}^{r} a_i)=1$ we have $(d_{F_1/F_2}, d_{F_4/F_2})=1$ and $F_1 \cap F_4=F_2$. Hence, by the hypothesis of induction and Lemma 3 (i), $\prod_{i=1}^{r} \alpha_i$ generates an n.i.b. of F_3/F_4. As $(n_{r+1}/l_{r+1}, a_{r+1})=1$, we have $(d_{F_4/F_5}, d_{F_8/F_5})=1$ and $F_4 \cap F_8=F_5$. Consequently, by Lemma 3(i), α_{r+1} generates an n.i.b. of F_7/F_4. Prime ideals ramified in F_3/F_4 divide $\prod_{i=1}^{r} a_i$ and prime ideals ramified in F_7/F_4 divide a_{r+1}. As $(\prod_{i=1}^{r} a_i, a_{r+1})=1$, we have $(d_{F_3/F_4}, d_{F_7/F_4})=1$ and $F_3 \cap F_7=F_4$. By Lemma 3 (ii), $\prod_{i=1}^{r+1} \alpha_i$ generates an n.i.b. of F_6/F_4. Thus, we have proved that $\prod_{i=1}^{s} \alpha_i$ generates an n.i.b. of $\boldsymbol{Q}(\sqrt[l_1]{a_1}, \cdots, \sqrt[l_s]{a_s}, \zeta_n)/\boldsymbol{Q}(\zeta_n)$. As $(m, n)=1$, ζ_m generates, by Lemma 3 (i), an n.i.b. of $\boldsymbol{Q}(\zeta_{mn})/\boldsymbol{Q}(\zeta_n)$. As $(\prod_{i=1}^{s} a_i, m)=1$, we have $\boldsymbol{Q}(\zeta_{mn}) \cap L=\boldsymbol{Q}(\zeta_n)$ and $(d_{\boldsymbol{Q}(\zeta_{mn})/\boldsymbol{Q}(\zeta_n)}, d_{L/\boldsymbol{Q}(\zeta_n)})=1$, where we put $L=\boldsymbol{Q}(\sqrt[l_1]{a_1}, \cdots, \sqrt[l_s]{a_s}, \zeta_n)$. Consequently, by Lemma 3 (ii), $\prod_{i=1}^{s} \alpha_i \zeta_m$ generates an n.i.b. of $\boldsymbol{Q}(\sqrt[l_1]{a_1}, \cdots, \sqrt[l_s]{a_s}, \zeta_{mn})/\boldsymbol{Q}(\zeta_n)$. Since $(d_{k/\boldsymbol{Q}(\zeta_n)}, m\prod_{i=1}^{s} a_i)=1$ and $k \cap \boldsymbol{Q}(\sqrt[l_1]{a_1}, \cdots, \sqrt[l_s]{a_s}, \zeta_{mn})=\boldsymbol{Q}(\zeta_n)$, $\prod_{i=1}^{s} \alpha_i \zeta_m$ generates, by Lemma 3 (i), an n.i.b. of $k(\sqrt[l_1]{a_1}, \cdots, \sqrt[l_s]{a_s}, \zeta_{mn})/k$. This proves our proposition.

In general, it is not easy to construct a Galois extension without n.i.b. by applying Theorem 2. For $l=3$, the unit group of quadratic field k is $\langle -1, \zeta_3 \rangle$ and no distinct elements of this group are pairwise congruent modulo 3. Consequently, we can check that $\boldsymbol{Q}(\zeta_3, \sqrt[3]{a})/\boldsymbol{Q}(\zeta_3)$ always has an n.i.b. ($a^2 \equiv 1 \bmod 9$).

The following proposition shows on the other hand that there are infinitely many tamely ramified extensions K/k ($k \neq \boldsymbol{Q}$) without n.i.b..

PROPOSITION 2. *Let m, n be square-free rational integers. Suppose that $m, n \equiv 3 \bmod 4$, $m < -1$, $n < 0$ and $(m, n) = 1$. Then $\boldsymbol{Q}(\sqrt{m}, \sqrt{n})/\boldsymbol{Q}(\sqrt{m})$ is a tamely ramified quadratic extension without n.i.b..*

PROOF. Put $K = \boldsymbol{Q}(\sqrt{m}, \sqrt{n})$ and $k = \boldsymbol{Q}(\sqrt{m})$. By the hypothesis, $\{1, (\sqrt{m} + \sqrt{n})/2\}$ is an $\mathfrak{o}_k$-basis of $\mathfrak{o}_K$ (Bird and Parry [1], Theorem I) and $\{1, \sqrt{m}, (\sqrt{m} + \sqrt{n})/2, (1 + \sqrt{mn})/2\}$ is $\boldsymbol{Z}$-basis of $\mathfrak{o}_K$ (Williams [11]). Let α be an element of $\mathfrak{o}_K$ and $\alpha = a + b\sqrt{m} + c(\sqrt{m} + \sqrt{n})/2 + d(1 + \sqrt{mn})/2$ ($a, b, c, d \in \boldsymbol{Z}$). Noting $\sqrt{m}\sqrt{n} = -\sqrt{mn}$, we obtain

$$\begin{pmatrix} \alpha \\ \alpha' \end{pmatrix} = A \begin{pmatrix} 1 \\ (\sqrt{m} + \sqrt{n})/2 \end{pmatrix}, \quad A = \begin{pmatrix} a + b\sqrt{m} + d(1+m)/2 & c - d\sqrt{m} \\ a + (b+c)\sqrt{m} + d(1-m)/2 & -(c - d\sqrt{m}) \end{pmatrix},$$

where α' is the conjugate element of α in K/k. Hence, we have

$$\det A = -(c - d\sqrt{m})\{(2a+d) + (2b+c)\sqrt{m}\}.$$

α generates an n.i.b. of K/k if and only if $\det A \in \mathfrak{o}_k^{\times}$, i.e. if and only if there exist $a, b, c, d \in \boldsymbol{Z}$ such that

$$(9) \qquad (2a+d)^2 - m(2b+c)^2 = \pm 1$$

$$(10) \qquad c^2 - md^2 = \pm 1 .$$

Since $-m > 1$, we have $2a + d = \pm 1$, $2b + c = 0$, $c = \pm 1$ and $d = 0$ from (9), (10). Therefore we obtain $2a = \pm 1$. So the simultaneous Diophantine equation (9), (10) has no solution and K/k has no n.i.b.. Since 2 is unramified in $\boldsymbol{Q}(\sqrt{mn})/\boldsymbol{Q}$, K/k is tamely ramified. This proves our assertion.

References

[1] R. H. BIRD and C. J. PARRY, Integral bases for bicyclic biquadratic fields over quadratic subfields, Pacific J. Math., **66** (1976), 29-36.

[2] A. FRÖHLICH, The module structure of Kummer extensions over Dedekind domains, J. Reine Agnew. Math., **209** (1962), 39-53.

[3] S. LANG, Algebraic Number Theory, Addison Wesley, Reading Ma., 1970.

[4] R. LONG, Algebraic Number Theory, Marcel Dekker, New York, 1977.

[5] H. B. MANN, On integral bases, Proc. Amer. Math. Soc., **9** (1958), 167-172.

[6] K. OKUTSU, Construction of integral basis I-IV, Proc. Japan Acad., **58 A** (1982), 47-49, 87-89, 117-119, 167-169.

[7] K. OKUTSU, On extensions of Dedekind domains I, II, preprint.

[8] K. OKUTSU, Construction of relative integral basis of $\mathbf{Q}(\sqrt[l]{a}, \zeta_l)$ over $\mathbf{Q}(\zeta_l)$ (in Japanese), Seisūron kenkyūshūkai hōkokushū in Kyushu University, 1982.
[9] R. G. SWAN, Induced representations and projective modules, Ann. of Math., **71** (1960), 552–578.
[10] I. REINER, Maximal Orders, Academic Press, London, 1975.
[11] K. S. WILLIAMS, Integers of biquadratic fields, Canad. Math. Bull., **13** (1970), 519–526.

Present Address:
DEPARTMENT OF MATHEMATICS
GAKUSHUIN UNIVERSITY
MEJIRO, TOSHIMA-KU, TOKYO 171