TOKYO J. MATH.
VOL. 19, NO. 1, 1996

On Normal Bases of Some Ring Extensions in Number Fields I

Fuminori KAWAMOTO

Gakushuin University

1. Introduction.

Let k be a number field and K/k a finite Galois extension with Galois group $G=Gal(K/k)$. For a number field N, $\mathfrak{o}_N$ denotes the ring of integers in N. Let S be a finite set of prime ideals of $\mathfrak{o}_k$ that contains all prime ideals which are wildly ramified in K/k. For a finite extension N/k, we simply denote by $\mathfrak{o}_N(S)$ the ring of elements a in N with $\mathrm{ord}_{\mathfrak{P}}(a)\geq 0$ for all prime ideals $\mathfrak{P}$ of $\mathfrak{o}_N$, not lying above S. The field K can be regarded as a module over the group ring kG of G over k by the action $\alpha^\lambda=\sum_{s\in G}a_s\alpha^s$ for $\alpha\in K$ and $\lambda=\sum_{s\in G}a_s s\in kG$. We say that a ring extension $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ has a normal basis if $\mathfrak{o}_K(S)$ is a free $\mathfrak{o}_k(S)[G]$-module, that is, there exists some α in $\mathfrak{o}_K(S)$ such that $\{\alpha^s\}_{s\in G}$ is a free $\mathfrak{o}_k(S)$-basis of $\mathfrak{o}_K(S)$. The extension $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ is called *ramified* if there exists some prime ideal of $\mathfrak{o}_k$, not belonging to S, which is ramified in K/k (this means that such prime ideal of $\mathfrak{o}_k$ is ramified in the Dedekind ring extension $\mathfrak{o}_K/\mathfrak{o}_k$, as usual). If not so, then it is called *unramified.*

We remark the following fact on the existence of normal bases of extensions of the rings of S-integers which was pointed out by H. Suzuki and whose proof is due to him. It says that we can take a sufficiently large set $U\cup S$, keeping the ramification of primes outside S, such that $\mathfrak{o}_K(U\cup S)/\mathfrak{o}_k(U\cup S)$ has a normal basis.

PROPOSITION 1.1. *Let the notations be as above and $T(\neq\emptyset)$ a finite set of prime ideals of $\mathfrak{o}_k$ that contains all prime ideals, not belonging to S, which are ramified in K/k. Then there exists a finite set U of prime ideals of $\mathfrak{o}_k$ such that $U\cap T=\emptyset$ and $\mathfrak{o}_K(U\cup S)/\mathfrak{o}_k(U\cup S)$ has a normal basis.*

PROOF. Let $V:=\mathfrak{o}_k-\bigcup_{\mathfrak{p}\in T}\mathfrak{p}$ be a multiplicative subset of $\mathfrak{o}_k$ and $V^{-1}\mathfrak{o}_k$ a ring of quotients of $\mathfrak{o}_k$. Then $V^{-1}\mathfrak{o}_k$ is a semi-local ring with maximal ideals $\{\mathfrak{p}\cdot(V^{-1}\mathfrak{o}_k)\}_{\mathfrak{p}\in T}$ and $V^{-1}\mathfrak{o}_K$ is a $(V^{-1}\mathfrak{o}_k)[G]$-module. Since all primes in T are tamely ramified, there exists some α in $\mathfrak{o}_K$ such that $1\otimes\alpha$ is a free generator of $\mathfrak{o}_{k_\mathfrak{p}}\otimes_{\mathfrak{o}_k}\mathfrak{o}_k$ over $\mathfrak{o}_{k_\mathfrak{p}}G$ for each $\mathfrak{p}\in T$ (Cf. [8, Lemma 2.6]), where $\mathfrak{o}_{k_\mathfrak{p}}$ denotes the valuation ring of the completion of

Received October 17, 1994

k with respect to $\mathfrak{p}$. Therefore α is also a free generator of $V^{-1}\mathfrak{o}_K$ over $(V^{-1}\mathfrak{o}_k)[G]$. Put $M:=\mathfrak{o}_K/(\mathfrak{o}_kG\cdot\alpha)$. Then M has a finite number of generators over $\mathfrak{o}_k$, say $m_1,\cdots,m_r$. Since $V^{-1}M=0$, there is some u_i in V for each i such that $u_im_i=0$. If we put $u=\prod_{i=1}^r u_i$, then we have $\langle u\rangle^{-1}M=0$ where $\langle u\rangle$ denotes a multiplicative subset of $\mathfrak{o}_k$, generated by u. Let U be a set of prime divisors of u. Then $U\cap T=\varnothing$ and $\mathfrak{o}_k(U)\otimes_{\mathfrak{o}_k}M=\mathfrak{o}_k(U)\otimes_{\langle u\rangle^{-1}\mathfrak{o}_k}\langle u\rangle^{-1}M=0$. So $\mathfrak{o}_K(U)=\mathfrak{o}_k(U)[G]\cdot\alpha$. This proves our proposition. □

From now on, assume that K/k is abelian and let $\hat{G}$ be the group of characters of G. In the previous paper [8], for each $\chi\in\hat{G}$, an ideal $\mathfrak{b}(\chi)$ was defined by resolvents of elements of K (for its definition, see Section 2) and we gave a necessary and sufficient condition for $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ to have a normal basis in terms of these ideals. Since resolvents are connected with Gauss sums, Stickelberger's theorem gives an information on ideals $\mathfrak{b}(\chi)$. For this, we study a property of $\mathfrak{b}(\chi)$ in Section 2. After Section 3, we assume that k is a totally real number field or a CM-field, i.e., a totally imaginary quadratic extension of a totally real number field. In comparison with Proposition 1.1, we can give also sequences $\{S_n\}$ of finite sets of prime ideals of $\mathfrak{o}_k$ with $S_n\subsetneq S_{n+1}$, such that $\mathfrak{o}_K(S_n)/\mathfrak{o}_k(S_n)$ does not have a normal basis for each positive integer n (Propositions 4.3 and 4.5). This fact follows from results of Section 3 (Proposition 3.3 and Lemma 3.5) and a sufficient condition for the non-existence of normal basis of ramified ring extension $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ which is given in Section 4 (Theorem 4.1). In Section 5, let K be an abelian field with prime conductor over the field $\mathbf{Q}$ of rational numbers. Then using Proposition 4.3, we discuss a normal basis of $\mathfrak{o}_K/\mathfrak{o}_k$ $(S=\varnothing)$ (Theorem 5.3). When K is the pth cyclotomic field, p being an odd prime, and $[K:k]$ is a prime, a normal basis of $\mathfrak{o}_K/\mathfrak{o}_k$ was studied by Cougnard [4, 5] and Brinkhuis [2]. Theorem 5.3 generalizes their result. It should be noted that our results in Section 4, 5 are a development of Brinkhuis' idea [2].

Throughout this paper, the above and following notations are used. For a number field N and each $\chi\in\hat{G}$, $N(\chi)$ denotes the field generated by the values of χ on G over N. For a ring R and a group Γ, we denote by $R\Gamma$ (or $R[\Gamma]$) the group ring of Γ over R and by $R^\times$ the group of units in R. For a set R, $|R|$ denotes the cardinal of R. For a positive integer n, ζ_n denotes a primitive nth root of unity. We denote by $\mathbf{Z}$ and $\mathbf{R}$ the ring of rational integers and the field of real numbers, respectively. For a number field N, we denote by N^+ the maximal real subfield of N: $N^+:=N\cap\mathbf{R}$. For an integral divisor $\mathfrak{n}$ of k, $k(\mathfrak{n})$ denotes the ray class field of k mod $\mathfrak{n}$. Specially $\tilde{k}:=k(1)$ is the Hilbert class field of k. Let $\mathfrak{n}_0$ and $\mathfrak{n}_\infty$ denote the finite and infinite components of $\mathfrak{n}$, respectively.

ACKNOWLEDGMENTS. The author would like to thank Dr. Suzuki for pointing out Proposition 1.1 and a certain person for his/her useful suggestion to Section 2.

2. Properties of ideals $\mathfrak{b}(\chi)$.

For $\alpha \in K$ and each $\chi \in \hat{G}$, we define the resolvent of α with values in $K(\chi)$ by

$$\langle \alpha, \chi \rangle = \langle \alpha, \chi \rangle_{K/k} := \sum_{s \in G} \chi(s^{-1}) \alpha^s .$$

For each $\chi \in \hat{G}$, let $L(\chi)$ be the $\mathfrak{o}_{k(\chi)}(S)$-module of rank one generated by all $\langle \alpha, \chi \rangle$ with $\alpha \in \mathfrak{o}_K(S)$. Let $\beta \in \mathfrak{o}_K$ be a free generator of K over kG. Then there exists a fractional ideal $\mathfrak{b}(\chi)$ of $\mathfrak{o}_{k(\chi)}(S)$ such that

$$L(\chi) = \mathfrak{b}(\chi) \langle \beta, \chi \rangle , \tag{2.1}$$

and we have

$$\mathfrak{b}(\chi^\omega) = \mathfrak{b}(\chi)^\omega , \tag{2.2}$$

for all $\omega \in Gal(k(\chi)/k)$, where we define $\chi^\omega(s) := \chi(s)^\omega$ for each $s \in G$ so that $\chi^\omega \in \hat{G}$.

In [8], we have chosen $\beta \in \mathfrak{o}_K$ such that $1 \otimes \beta$ is a free generator of $\mathfrak{o}_{k_\mathfrak{p}} \otimes_{\mathfrak{o}_k} \mathfrak{o}_K$ over $\mathfrak{o}_{k_\mathfrak{p}} G$ for each prime ideal $\mathfrak{p}$ of $\mathfrak{o}_k$, dividing the order of G and not belonging to S. Then we have proved that $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ has a normal basis if and only if for each $\chi \in \hat{G}$, $\mathfrak{b}(\chi)$ (depending on this β) is a principal ideal of $\mathfrak{o}_{k(\chi)}(S)$ and its generators satisfy some congruence conditions and some conditions (as in (2.2)) for Galois actions (See [8, Theorem 2.10 and Remark 2.11]). We have to use these results in this paper. In this section, we study the properties of these ideals in the ramified case (For the unramified case, see [8, Lemma 3.2]).

Let $g = g_\chi$ be the order of χ in $\hat{G}$ and $\mathfrak{a}(\chi)$ the module generated by the products $\prod_{i=1}^{g} \alpha_i$ with $\alpha_i \in L(\chi)$ so that $\mathfrak{a}(\chi)$ is an ideal of $\mathfrak{o}_{k(\chi)}(S)$ and it follows from (2.1) that

$$(\langle \beta, \chi \rangle^{g_\chi}) \mathfrak{o}_{k(\chi)}(S) = \mathfrak{a}(\chi) \mathfrak{b}(\chi)^{-g_\chi} . \tag{2.3}$$

Let $V(\chi)$ be the one dimensional $k(\chi)$-vector space of elements α of $K(\chi)$ with $\alpha^s = \chi(s)\alpha$ for all $s \in Gal(K(\chi)/k(\chi)) \hookrightarrow G$. Let $\tilde{L}(\chi) := V(\chi) \cap \mathfrak{o}_{K(\chi)}(S)$ so that this is also a $\mathfrak{o}_{k(\chi)}(S)$-module of rank one. Therefore there exists a fractional ideal $\tilde{\mathfrak{b}}(\chi)$ of $\mathfrak{o}_{k(\chi)}(S)$ such that $\tilde{L}(\chi) = \tilde{\mathfrak{b}}(\chi) \langle \beta, \chi \rangle$. Similarly we define an ideal $\tilde{\mathfrak{a}}(\chi)$ of $\mathfrak{o}_{k(\chi)}(S)$. Then the formulas (2.2) and (2.3) for these also hold. Since $\mathfrak{b}(\chi) \subset \tilde{\mathfrak{b}}(\chi)$, there exists an ideal $\mathfrak{c}(\chi)$ of $\mathfrak{o}_{k(\chi)}(S)$ such that

$$\mathfrak{b}(\chi) = \tilde{\mathfrak{b}}(\chi) \mathfrak{c}(\chi) . \tag{2.4}$$

Now we consider the gap $\mathfrak{c}(\chi)$ between $\mathfrak{b}(\chi)$ and $\tilde{\mathfrak{b}}(\chi)$ and it gives a position of $\mathfrak{b}(\chi)$ in the decomposition (2.3) of a resolvent into ideals (See Proposition 2.1, Example 2.2 and Proposition 2.3). It follows from (2.4) and the formulas (2.3) for $L(\chi)$ and $\tilde{L}(\chi)$ that $\mathfrak{a}(\chi) = \tilde{\mathfrak{a}}(\chi) \mathfrak{c}(\chi)^g$. Let $\mathfrak{f}(\chi)$ be the Artin conductor of χ in K/k which is an ideal of $\mathfrak{o}_k$. By Fröhlich's result, $L(\chi) L(\bar{\chi}) = \mathfrak{f}(\chi)$, where let $\bar{\chi} := \chi^{-1}$ (See [8, Lemma 3.1]), hence $\mathfrak{a}(\chi) \mathfrak{a}(\bar{\chi}) = \mathfrak{f}(\chi)^g$. So,

$$\tilde{\mathfrak{a}}(\chi)\tilde{\mathfrak{a}}(\bar{\chi})\{\mathfrak{c}(\chi)\mathfrak{c}(\bar{\chi})\}^{g}=\mathfrak{f}(\chi)^{g}\mathfrak{o}_{k(\chi)}(S)\,. \tag{2.5}$$

From now on, let χ be a non-trivial character of G and k_χ the fixed field of $\operatorname{Ker}\chi$ in K/k so that k_χ/k is a cyclic extension of degree g. Let

$$l=l_\chi:=[k_\chi(\chi):k(\chi)]\ (>1)$$

so that $l|g$. Recall that $k_\chi(\chi)/k(\chi)$ is a cyclic Kummer extension of degree l with primitive element $\langle\beta,\chi\rangle$ (See [8, Section 3]). So there are an l-power free ideal A_χ and an ideal B_χ of $\mathfrak{o}_{k(\chi)}(S)$ such that

$$(\langle\beta,\chi\rangle^{l})\mathfrak{o}_{k(\chi)}(S)=A_\chi B_\chi^{l}\,. \tag{2.6}$$

Since $\tilde{\mathfrak{a}}(\chi)$ is g-power free by [8, Lemma 2.8, (i)], it follows from the formula (2.3) for $\tilde{L}(\chi)$ that

$$\tilde{\mathfrak{a}}(\chi)=A_\chi^{g/l}\qquad(\tilde{\mathfrak{b}}(\chi)^{-1}=B_\chi)\,. \tag{2.7}$$

Let ζ be a fixed primitive gth root of unity and $\Omega=\Omega_\chi:=Gal(k(\chi)/k)$. Then there exists a group injection ι from Ω into $(\mathbf{Z}/g\mathbf{Z})^{\times}$ such that

$$\zeta^{\omega}=\zeta^{\iota(\omega)}\qquad\text{for all}\quad\omega\in\Omega\,.$$

If $1<d|g$, we write ι_d for the composition of ι and the canonical quotient map $(\mathbf{Z}/g\mathbf{Z})^{\times}\to(\mathbf{Z}/d\mathbf{Z})^{\times}$. For each $\omega\in\Omega/\operatorname{Ker}\iota_d$, let $t_d(\omega)$ be the integer satisfying

$$\iota_d(\omega)=t_d(\omega)\bmod d\,,\qquad 0<t_d(\omega)<d\,,$$

and put

$$\theta:=\sum_{\omega\in\Omega}t_{g_\chi}(\omega)\omega^{-1}\,, \tag{2.8}$$

which is in $\mathbf{Z}\Omega$. As $k_\chi(\chi)/k$ is an abelian extension, $A_\chi^{\omega-t_l(\omega)}$ is the lth power of a fractional ideal of $\mathfrak{o}_{k(\chi)}(S)$ for each $\omega\in\Omega$. Hence

$$\operatorname{ord}_{\mathfrak{P}}(A_\chi)=\operatorname{ord}_{\mathfrak{P}^{\omega}}(A_\chi^{\omega})\equiv t_l(\omega)\operatorname{ord}_{\mathfrak{P}^{\omega}}(A_\chi)\ (\mathrm{mod}\ l)\,, \tag{2.9}$$

for any prime ideal $\mathfrak{P}$ of $\mathfrak{o}_{k(\chi)}$, not lying above S, and any $\omega\in\Omega$.

Definition. For a prime ideal $\mathfrak{p}$ of $\mathfrak{o}_k$, we denote by $e_{\mathfrak{p}}$ and $Z_{\mathfrak{p}}$ the ramification index and the decomposition group of $\mathfrak{p}$ in $k(\chi)/k$ respectively. Let $\mathscr{U}=\mathscr{U}_\chi$ be the set of prime ideals of $\mathfrak{o}_k$, not belonging to S, which are ramified in k_χ/k, and $\mathscr{V}=\mathscr{V}_\chi$ the set of prime ideals $\mathfrak{p}$ of $\mathfrak{o}_k$, not belonging to S, such that $\mathfrak{P}|\mathfrak{p}$ and $\mathfrak{P}|A_\chi$ with some prime ideal $\mathfrak{P}$ of $\mathfrak{o}_{k(\chi)}$.

We claim that $\mathscr{V}\subset\mathscr{U}$. If $\mathfrak{p}\in\mathscr{V}$, then $\mathfrak{P}|\mathfrak{p}$ and $\mathfrak{P}|A_\chi$ with some prime ideal $\mathfrak{P}$ of $\mathfrak{o}_{k(\chi)}$. Since A_χ is l-power free, $\mathfrak{P}$ is ramified in $k_\chi(\chi)/k(\chi)$. Therefore $\mathfrak{p}$ is ramified in k_χ/k so that $\mathfrak{p}\in\mathscr{U}$. Next we claim that

$$\tilde{\mathfrak{a}}(\chi)\tilde{\mathfrak{a}}(\bar{\chi}) = \prod_{\mathfrak{p} \in \mathscr{V}} \prod_{\omega \in \Omega/Z_{\mathfrak{p}}} \mathfrak{P}^{g\omega}, \tag{2.10}$$

where $\mathfrak{P}$ is any prime ideal of $\mathfrak{o}_{k(\chi)}$ lying above $\mathfrak{p}$. By (2.7) and noting that $l = l_\chi = l_{\bar{\chi}}$, it is sufficient to prove that

$$A_\chi A_{\bar{\chi}} = \prod_{\mathfrak{p} \in \mathscr{V}} \prod_{\omega \in \Omega/Z_{\mathfrak{p}}} \mathfrak{P}^{l\omega}. \tag{2.11}$$

This is equivalent to the three statements: for all prime ideals $\mathfrak{P}$ of $\mathfrak{o}_{k(\chi)}$, not lying above S,

$$\operatorname{ord}_{\mathfrak{P}}(A_\chi A_{\bar{\chi}}) = 0 \text{ or } l, \tag{2.12}$$

$$\operatorname{ord}_{\mathfrak{P}}(A_\chi A_{\bar{\chi}}) > 0 \implies \forall \omega \in \Omega : \operatorname{ord}_{\mathfrak{P}^\omega}(A_\chi A_{\bar{\chi}}) > 0, \tag{2.13}$$

$$\mathscr{V} = \{\mathfrak{P} \cap k \mid \mathfrak{P} \text{ is a prime divisor of } A_\chi A_{\bar{\chi}}\}. \tag{2.14}$$

It follows from (2.6) for χ and for $\bar{\chi}$ that

$$A_\chi A_{\bar{\chi}} = (\langle \beta, \chi \rangle \langle \beta, \bar{\chi} \rangle B_\chi^{-1} B_{\bar{\chi}}^{-1})^l.$$

Since $\langle \beta, \chi \rangle \langle \beta, \bar{\chi} \rangle$ is in $k(\chi)$ (Cf. [8, Lemma 2.3, (iv)]), we have

$$l \mid (\operatorname{ord}_{\mathfrak{P}}(A_\chi) + \operatorname{ord}_{\mathfrak{P}}(A_{\bar{\chi}})).$$

So the fact that A_χ and $A_{\bar{\chi}}$ are l-power free implies (2.12) and also that

$$\operatorname{ord}_{\mathfrak{P}}(A_\chi) > 0 \iff \operatorname{ord}_{\mathfrak{P}}(A_\chi A_{\bar{\chi}}) > 0. \tag{2.15}$$

It follows from (2.9) that $\operatorname{ord}_{\mathfrak{P}}(A_\chi) > 0 \Rightarrow \operatorname{ord}_{\mathfrak{P}^\omega}(A_\chi) > 0$. This fact, together with (2.15) for $\mathfrak{P}$ and for $\mathfrak{P}^\omega$, gives (2.13). (2.14) follows from (2.15) and the definition of $\mathscr{V}$. Thus we have proved the claim (2.11), hence (2.10). By the definition of Artin conductors, $\mathfrak{f}(\chi)$ becomes the Artin conductor of the character of $Gal(k_\chi/k)$ associated with χ. So by the assumed tameness outside S,

$$\mathfrak{f}(\chi)\mathfrak{o}_k(S) = \prod_{\mathfrak{p} \in \mathscr{U}} \mathfrak{p}. \tag{2.16}$$

By the definition of $e_{\mathfrak{p}}$ and $Z_{\mathfrak{p}}$, we have $\mathfrak{p} = \prod_{\omega \in \Omega/Z_{\mathfrak{p}}} \mathfrak{P}^{e_{\mathfrak{p}}\omega}$. Hence (2.5), (2.10) and (2.16) yield the following proposition:

Proposition 2.1. *Let $\beta \in \mathfrak{o}_K$ be a free generator of K over kG and $\chi(\neq 1) \in \hat{G}$. Let the ideal $\mathfrak{c}(\chi)$ of $\mathfrak{o}_{k(\chi)}(S)$ be as in* (2.4). *Then under the above notations, we have*

$$\mathfrak{c}(\chi)\mathfrak{c}(\bar{\chi}) = \prod_{\mathfrak{p} \in \mathscr{U}_\chi - \mathscr{V}_\chi} \mathfrak{p} \cdot \prod_{\mathfrak{p} \in \mathscr{V}_\chi} \left(\prod_{\omega \in \Omega_\chi/Z_{\mathfrak{p}}} \mathfrak{P}^\omega \right)^{e_{\mathfrak{p}}-1},$$

where $\mathfrak{P}$ is any prime ideal of $\mathfrak{o}_{k(\chi)}$ lying above $\mathfrak{p} \in \mathscr{V}_\chi$. In particular, if $\mathscr{U}_\chi = \emptyset$ or k contains a primitive g_χth root of unity (i.e., $k = k(\chi)$, therefore $\mathscr{U}_\chi = \mathscr{V}_\chi$ and $e_{\mathfrak{p}} = 1$ for all $\mathfrak{p}$ in $\mathscr{V}_\chi$), *then we have* $\mathfrak{c}(\chi)=(1)$ *so that* $\mathfrak{b}(\chi)=\tilde{\mathfrak{b}}(\chi)$ *and* $\mathfrak{a}(\chi)=\tilde{\mathfrak{a}}(\chi)$.

EXAMPLE 2.2. We shall give an abelian extension K/k with $\mathscr{V}_\chi \subsetneq \mathscr{U}_\chi$ for a certain χ in $\hat{G}$. Then we have $\mathfrak{c}(\chi)\neq(1)$ by Proposition 2.1 so that $\mathfrak{b}(\chi)\neq\tilde{\mathfrak{b}}(\chi)$. Let p_1, p_2 be odd prime numbers such that $p_2\equiv 1 \bmod p_1$. Let K be a subfield of $\mathbf{Q}(\zeta_{p_1p_2})$ with $\mathbf{Q}(\zeta_{p_2})\subset K$ and $[K:\mathbf{Q}(\zeta_{p_2})]>1$ and k the unique subfield of $\mathbf{Q}(\zeta_{p_2})$ with $[\mathbf{Q}(\zeta_{p_2}):k]=p_1$. Assume that the set S does not contain any prime ideal of $\mathfrak{o}_k$ lying above p_1 or p_2. Let F be the unique subfield of $\mathbf{Q}(\zeta_{p_1})$ with $[F:\mathbf{Q}]=[K:\mathbf{Q}(\zeta_{p_2})]$, so that $Gal(K/\mathbf{Q}(\zeta_{p_2}))\cong Gal(Fk/k)\cong Gal(F/\mathbf{Q})$. Let ψ_1 be a non-trivial character of $Gal(Fk/k)$ of order m and ψ_2 a character of $Gal(\mathbf{Q}(\zeta_{p_2})/k)$ of order p_1. Let χ be the character of G corresponding to (ψ_1, ψ_2) by the canonical isomorphism:

$$\hat{G}\cong Gal(Fk/k)^\wedge \times Gal(\mathbf{Q}(\zeta_{p_2})/k)^\wedge ,$$

so that $g_\chi=mp_1$ by $(p_1, m)=1$. Since $(p_2, mp_1)=1$, we have $k\cap\mathbf{Q}(\chi)=\mathbf{Q}$. Also $\mathbf{Q}(\zeta_{p_2})\subset k_\chi\subset K$, $[k_\chi:\mathbf{Q}(\zeta_{p_2})]=m$. Therefore

$$\mathscr{U}=\{\mathfrak{p};\ \text{prime in } \mathfrak{o}_k\,;\ \mathfrak{p}\,|\,p_1 \text{ or } \mathfrak{p}\,|\,p_2\}\,.$$

Since a prime ideal of $\mathfrak{o}_{k(\chi)}$ lying above p_2 is the only ramified ideal in $k_\chi(\chi)/k(\chi)$ and it is tamely ramified, a prime divisor of the ideal A_χ divides p_2. Hence

$$\mathscr{V}=\{\mathfrak{p};\ \text{prime in } \mathfrak{o}_k\,;\ \mathfrak{p}\,|\,p_2\}\,.$$

So $\mathscr{V}\subsetneq\mathscr{U}$. (Note that $e_\mathfrak{p}=1$ for all $\mathfrak{p}$ in $\mathscr{V}$ now.)

The following proposition is a generalization of Sodaïgui [9, Théorème 2.2]:

PROPOSITION 2.3. *Let* β, χ *be as in Proposition* 2.1 *and* $\mathfrak{b}(\chi)$ (*resp.* $\mathfrak{a}(\chi)$) *a fractional ideal of* $\mathfrak{o}_{k(\chi)}(S)$ *depending on* β *as in* (2.1) (*resp.* (2.3)). *Suppose that* $\mathscr{U}_\chi\neq\varnothing$.

(i) *Assume that* (A1): $\mathfrak{p}\in\mathscr{U}_\chi\Rightarrow\mathfrak{p}\nmid g_\chi$. *Then* $\mathfrak{a}(\chi)$ *is* g_χ*-power free.*

(ii) *Assume that the map* ι *is an isomorphism (i.e.,* $k\cap\mathbf{Q}(\chi)=\mathbf{Q}$) *and* (A2): *for all* $\mathfrak{p}$ *in* $\mathscr{U}_\chi$, $\mathfrak{p}$ *is totally ramified in* k_χ/k. *Then any* $\mathfrak{p}$ *in* $\mathscr{U}_\chi$ *is completely decomposed in* $k(\chi)/k$ *and we have*

$$(\langle\beta, \chi\rangle^{g_\chi})\mathfrak{o}_{k(\chi)}(S)=\prod_{\mathfrak{p}\in\mathscr{U}_\chi}\mathfrak{P}^\theta\mathfrak{b}(\chi)^{-g_\chi}\,,$$

where $\mathfrak{P}$ *is some prime ideal of* $\mathfrak{o}_{k(\chi)}$ *lying above* $\mathfrak{p}$ *and* θ *is defined in* (2.8).

REMARK 2.4. If g_χ is a prime power, then the assumption (A1) holds, because any $\mathfrak{p}$ in $\mathscr{U}$ is tamely ramified in k_χ/k.

PROOF OF PROPOSITION 2.3. (i) By (A1), we have $e_\mathfrak{p}=1$ for all $\mathfrak{p}\in\mathscr{U}$. Let $\mathfrak{p}\in\mathscr{U}$ and $\mathfrak{P}$ be a prime ideal of $\mathfrak{o}_{k(\chi)}$ with $\mathfrak{P}\,|\,\mathfrak{p}$. Since $e_\mathfrak{p}=1$, $\mathfrak{P}$ is ramified in $k_\chi(\chi)/k(\chi)$. Also $\mathfrak{P}\nmid l$. Therefore by Kummer theory, $\mathfrak{P}\,|\,A_\chi$ so that $\mathfrak{p}\in\mathscr{V}$. Thus $\mathscr{U}=\mathscr{V}$. Hence $\mathfrak{c}(\chi)=(1)$ by Proposition 2.1. So by (2.4), $\mathfrak{b}(\chi)=\tilde{\mathfrak{b}}(\chi)$ so that $\mathfrak{a}(\chi)=\tilde{\mathfrak{a}}(\chi)$. This proves the assertion (i).

(ii) By (A2), the assumption (A1) holds so that the assertion (i) is true. For $\mathfrak{p}\in\mathscr{U}$, since $e_{\mathfrak{p}}=1$ and $\mathfrak{p}$ is totally ramified, we have $k_\chi \cap k(\chi)=k$, therefore $l=g$. Consequently $\mathfrak{a}(\chi)=\tilde{\mathfrak{a}}(\chi)=A_\chi$ by (2.7). We define a subset $\mathscr{V}_1$ of $\mathscr{V}$ by

$$\mathscr{V}_1:=\{\mathfrak{P}\cap k \mid \mathfrak{P} \text{ is a prime ideal of } \mathfrak{o}_{k(\chi)} \text{ with } \mathrm{ord}_{\mathfrak{P}}(A_\chi)=1\}\,.$$

Claim that $\mathscr{U}=\mathscr{V}_1$. Let $\mathfrak{p}\in\mathscr{U}$ and $\mathfrak{P}$ be a prime ideal of $\mathfrak{o}_{k(\chi)}$ with $\mathfrak{P}|\mathfrak{p}$. Then $i:=\mathrm{ord}_{\mathfrak{P}}(A_\chi)\geq 1$ (i.e., $\mathfrak{p}\in\mathscr{V}$) as seen above. Since g is the ramification index of $\mathfrak{P}$ in $k_\chi(\chi)/k(\chi)$, we have $g=g/(i,g)$ from Kummer theory ([3, p. 92]). So $(i,g)=1$. Since ι is surjective, there is some ω in Ω such that $i=t_g(\omega)$, therefore $1\equiv t_g(\omega^{-1})i\equiv \mathrm{ord}_{\mathfrak{P}^\omega}(A_\chi)$ mod g by (2.9). As $0<\mathrm{ord}_{\mathfrak{P}^\omega}(A_\chi)<g$, we have $\mathrm{ord}_{\mathfrak{P}^\omega}(A_\chi)=1$. Hence $\mathfrak{p}=\mathfrak{P}^\omega\cap k\in\mathscr{V}_1$. Thus $\mathscr{U}=\mathscr{V}_1$. For $\mathfrak{p}\in\mathscr{U}$, let $\omega\in Z_{\mathfrak{p}}$ and $\mathfrak{P}$ a prime ideal of $\mathfrak{o}_{k(\chi)}$ with $\mathfrak{P}|\mathfrak{p}$. Since $\mathfrak{P}^\omega=\mathfrak{P}$ and $\mathfrak{p}\in\mathscr{V}_1$, $1\equiv t_g(\omega)$ mod g by (2.9), therefore $\omega=1$; $\mathfrak{p}$ is completely decomposed in $k(\chi)/k$. Since $\mathscr{U}=\mathscr{V}_1$, we can define a square free ideal C of $\mathfrak{o}_{k(\chi)}(S)$ by $C:=\prod_{\mathfrak{p}\in\mathscr{U}}\mathfrak{P}^\omega$, where $\mathfrak{P}$ is some prime ideal of $\mathfrak{o}_{k(\chi)}$ with $\mathfrak{P}|\mathfrak{p}$ and $\mathrm{ord}_{\mathfrak{P}}(A_\chi)=1$. Then (2.9) and the assumption that ι is surjective imply $A_\chi=C^\theta$. Thus the assertion (ii) is proved. □

3. Decomposition of prime ideals.

In this section, suppose that k is a totally real number field or a CM-field. Let l be an odd prime or $l=4$, and $\mathfrak{p}$ a prime ideal of $\mathfrak{o}_k$ such that $\mathfrak{p}\nmid l$. We assume that

$$k/\mathbf{Q} \text{ is Galois and } F:=k\cap\mathbf{Q}(\zeta_l)\subset k^+\,, \tag{3.1}$$

so that k/F is Galois and F is totally real. Since l is an odd prime or $l=4$, $Gal(\mathbf{Q}(\zeta_l)/F)$ is cyclic. By $\mathfrak{p}\nmid l$, $\mathfrak{p}\cap\mathfrak{o}_F$ is unramified in $\mathbf{Q}(\zeta_l)/F$. Now we wish to discuss the following problem:

(♯): For any prime ideal $\mathfrak{P}$ of $\mathfrak{o}_{k(\zeta_l)}$ with $\mathfrak{P}|\mathfrak{p}$, $\mathfrak{P}$ is not decomposed in $k(\zeta_l)/k(\zeta_l)^+$?

So we need the following proposition:

PROPOSITION 3.1. *Let F be a totally real number field and K_i/F $(i=1,2)$ a finite Galois extension with Galois group G_i such that $K_1\cap K_2=F$. Assume that K_1 is a totally real number field or a CM-field, and K_2 is a CM-field, so that $|G_2|>1$. Suppose that G_2 has only an element of order two (For example, this is true when G_2 is cyclic). Put $L:=K_1K_2$ which is a CM-field. Let $\mathfrak{P}$ be a prime ideal of $\mathfrak{o}_L$, $\mathfrak{p}_i:=\mathfrak{P}\cap\mathfrak{o}_{K_i}$ $(i=1,2)$ and $p:=\mathfrak{P}\cap\mathfrak{o}_F$. Suppose that p is unramified in K_2/F. f_i $(i=1,2)$ denotes the residue degree of p in K_i/F. Then we have the following*:

(I) *The case where K_1 is totally real.*

$\mathfrak{P}$ is not decomposed in $L/L^+\Leftrightarrow \mathrm{ord}_2(f_1)+1\leq\mathrm{ord}_2(f_2)$.

(II) *The case where K_1 is a CM-field.*

(i) *If $\mathfrak{p}_1$ is decomposed in K_1/K_1^+, then $\mathfrak{P}$ is decomposed in L/L^+.*

(ii) *If $\mathfrak{p}_1$ is ramified in K_1/K_1^+, then $\mathfrak{P}$ is not decomposed in $L/L^+\Leftrightarrow \mathrm{ord}_2(f_1)+1\leq$*

$\mathrm{ord}_2(f_2)$.

(iii) *If* $\mathfrak{p}_1$ *is inert in* K_1/K_1^+, *then* $\mathfrak{P}$ *is not decomposed in* $L/L^+ \Leftrightarrow \mathrm{ord}_2(f_1)=\mathrm{ord}_2(f_2)$ (>0).

PROOF. Let σ_i $(i=1,2)$ be a Frobenius automorphism of $\mathfrak{p}_i$ in K_i/F, and T_i and Z_i the inertia and decomposition groups of $\mathfrak{p}_i$ in K_i/F, respectively. Let θ be a Frobenius automorphism of $\mathfrak{P}$ in L/F, and T and Z the inertia and decomposition groups of $\mathfrak{P}$ in L/F, respectively. As $K_1 \cap K_2=F$, $Gal(L/F)$ is identified with $G_1 \times G_2$. Since $|T|=|T_1|$ by $T_2=\{1\}$, $T \subset T_1 \times T_2$ implies $T=T_1 \times \{1\}$. If θ_i $(i=1,2)$ is the restriction of θ to K_i, then $\theta=(\theta_1, \theta_2)$ and θ_i is a Frobenius automorphism of $\mathfrak{p}_i$ in K_i/F. Therefore $\theta_1 T_1=\sigma_1 T_1$ and furthermore $\theta_2=\sigma_2$ by $T_2=\{1\}$. Hence

$$Z=\bigcup_m \theta^m T=\bigcup_m (\sigma_1, \sigma_2)^m \cdot (T_1 \times \{1\}), \tag{3.2}$$

where m ranges over all integers. Let ρ_i $(i=1,2)$ be the restriction of the complex conjugation to K_i. Since F is real, $\rho_i \in G_i$ and furthermore the order of ρ_2 in G_2 is two since K_2 is a CM-field. Let $H:=\langle(\rho_1, \rho_2)\rangle$, where note that $\rho_1=1$ when K_1 is real. Then L^+ is the fixed field of H in L/F. So,

$$\mathfrak{P} \text{ is not decomposed in } L/L^+ \Longleftrightarrow H \subset Z, \tag{3.3}$$

because $H \cap Z$ is the decomposition group of $\mathfrak{P}$ in L/L^+. If $\mathfrak{P}$ is not decomposed in L/L^+, then $\rho_1 \in Z_1$ from (3.3) and $Z \subset Z_1 \times Z_2$, so that $\langle\rho_1\rangle \cap Z_1=\langle\rho_1\rangle$, hence $\mathfrak{p}_1$ is not decomposed in K_1/K_1^+. This proves the assertion (II-i). For each $i=1,2$, let $t_i:=\mathrm{ord}_2(f_i)$.

The cases (I) and (II-ii). Since $\langle\rho_1\rangle \cap T_1$ is the inertia group of $\mathfrak{p}_1$ in K_1/K_1^+, $\mathfrak{p}_1$ is ramified in $K_1/K_1^+ \Leftrightarrow \rho_1 \in T_1$. So $\rho_1 T_1=T_1$ by the assumptions. By (3.2) and (3.3), we may show that $t_1+1 \leq t_2 \Leftrightarrow$ there exists an integer m such that $T_1=\sigma_1^m T_1$ and $\rho_2=\sigma_2^m$. If such m exists, then we have $f_1|m$, f_2 is even, $(f_2/2)|m$ and $m/(f_2/2)$ is odd, because f_1 is the order of $\sigma_1 T_1$ in Z_1/T_1 and f_2 is the order of σ_2 in G_2. Let a be the least common multiple of f_1 and $f_2/2$. Since $a|m$, we have

$$\mathrm{Max}(t_1, t_2-1)=\mathrm{ord}_2(a) \leq \mathrm{ord}_2(m)=\mathrm{ord}_2(f_2/2)=t_2-1\,.$$

Therefore $t_1+1 \leq t_2$. Conversely, assume that this holds. So f_2 is even. Let a be the same meaning as above. Then $T_1=\sigma_1^a T_1$. Since $t_1 \leq t_2-1$, $\mathrm{ord}_2(a)=\mathrm{ord}_2(f_2/2)$ so that the order of σ_2^a is two. Since G_2 has only an element of order two, we have $\rho_2=\sigma_2^a$. This proves the assertions.

The case (II-iii). Now the order of ρ_1 in G_1 is two. Since $\mathfrak{p}_1$ is inert in K_1/K_1^+, $t_1>0$, $\langle\rho_1\rangle \cap Z_1=\langle\rho_1\rangle$ and $\langle\rho_1\rangle \cap T_1=\{1\}$. So $\rho_1 \in Z_1$ and $\rho_1 \notin T_1$. Therefore $\rho_1 T_1$ is the element of order two in the cyclic group Z_1/T_1. By (3.2) and (3.3), we may show that $t_1=t_2 \Leftrightarrow$ there exists an integer m such that $\rho_1 T_1=\sigma_1^m T_1$ and $\rho_2=\sigma_2^m$. This is similarly proved as in the above cases (e.g., let a be the least common multiple of $f_1/2$

and $f_2/2$ in this case). $\square$

Return to the situation as before Proposition 3.1. Considering (II-i) of its proposition, we distinguish two cases:

(C1) k is totally real or "k is a CM-field and $\mathfrak{p}$ is ramified in k/k^+".

(C2) k is a CM-field and $\mathfrak{p}$ is inert in k/k^+.

Let $p:=\mathfrak{p}\cap\mathbf{Z}$. We denote by a and b the residue degrees of p in $k/\mathbf{Q}$ and $\mathbf{Q}(\zeta_l)/\mathbf{Q}$, respectively. Let f, f_1 and f_2 be the residue degrees of $\mathfrak{p}\cap\mathfrak{o}_F$ in $F/\mathbf{Q}$, k/F and $\mathbf{Q}(\zeta_l)/F$, respectively. So $a=ff_1$, $b=ff_2$, therefore

$$\mathrm{ord}_2(a)=\mathrm{ord}_2(f)+\mathrm{ord}_2(f_1)\,, \qquad \mathrm{ord}_2(b)=\mathrm{ord}_2(f)+\mathrm{ord}_2(f_2)\,. \tag{3.4}$$

Note that $F=\mathbf{Q}$, $a=f_1$ and $b=f_2$ hold under the assumption (3.1) when $l=4$.

LEMMA 3.2. *Let l be an odd prime or $l=4$, and $\mathfrak{p}$ a prime ideal of $\mathfrak{o}_k$ such that $\mathfrak{p}\nmid l$. Put* $N\mathfrak{p}:=|\mathfrak{o}_k/\mathfrak{p}|$. *Then under the assumption* (3.1) *and the above notations, we have*

(i) *If l is an odd prime and $l\,|\,(N\mathfrak{p}-1)$, then* (#) *does not hold in the case* (C1).

(ii) *When $l=4$,* (#) *holds*$\Leftrightarrow N\mathfrak{p}\equiv 3 \bmod 4$ *in the case* (C1), *and* "$\mathrm{ord}_2(a)=1$ *and* $p\equiv 3 \bmod 4$" *in the case* (C2).

PROOF. (i) By $l|(N\mathfrak{p}-1)$, $p^a=N\mathfrak{p}\equiv 1 \bmod l$. Since b is the order of $p \bmod l$, we have $b|a$ so that $\mathrm{ord}_2(b)\le\mathrm{ord}_2(a)$. It follows from (3.4) that $\mathrm{ord}_2(f_2)\le\mathrm{ord}_2(f_1)<\mathrm{ord}_2(f_1)+1$. Hence (#) does not hold by Proposition 3.1, (I), (II-ii) (more precisely, any prime ideal $\mathfrak{P}$ of $\mathfrak{o}_{k(\zeta_l)}$ with $\mathfrak{P}|\mathfrak{p}$ is decomposed in $k(\zeta_l)/k(\zeta_l)^+$).

(ii) Now $\mathbf{Q}(\zeta_l)=\mathbf{Q}(\sqrt{-1})$ and p is an odd prime. So,

$$p\equiv 1 \bmod 4 \Leftrightarrow p \text{ is decomposed in } \mathbf{Q}(\zeta_l)/\mathbf{Q} \Leftrightarrow b=1 \Leftrightarrow \mathrm{ord}_2(b)=0\,,$$
$$p\equiv 3 \bmod 4 \Leftrightarrow p \text{ is inert in } \mathbf{Q}(\zeta_l)/\mathbf{Q} \Leftrightarrow b=2 \Leftrightarrow \mathrm{ord}_2(b)=1\,.$$

Hence $\mathrm{ord}_2(a)+1=(\le)\mathrm{ord}_2(b)\Leftrightarrow$"$p\equiv 3 \bmod 4$ and $\mathrm{ord}_2(a)=0$"$\Leftrightarrow N\mathfrak{p}=p^a\equiv 3 \bmod 4$. In (C2), we have $\mathrm{ord}_2(a)>0$. Since $\mathrm{ord}_2(b)\le 1$, $\mathrm{ord}_2(a)=\mathrm{ord}_2(b)\Leftrightarrow\mathrm{ord}_2(a)=1$ and $p\equiv 3 \bmod 4$. Now the assertions follow from Proposition 3.1. $\square$

For a prime ideal $\mathfrak{p}$ of $\mathfrak{o}_k$ with $\mathfrak{p}\nmid l$, putting $p:=\mathfrak{p}\cap\mathbf{Z}$, let $a_\mathfrak{p}$ (resp. $b_\mathfrak{p}$) be the residue degree of p in $k/\mathbf{Q}$ (resp. $\mathbf{Q}(\zeta_l)/\mathbf{Q}$). When l is an odd prime (resp. $l=4$), we define the sets of prime ideals of $\mathfrak{o}_k$ as follows.

$$\mathfrak{S}_{1,l}:=\{\mathfrak{p}\mid\mathfrak{p}\nmid l \text{ and } \mathrm{ord}_2(a_\mathfrak{p})+1\le\mathrm{ord}_2(b_\mathfrak{p}) \text{ (resp. } N\mathfrak{p}\equiv 3 \bmod 4)\}\,,$$

if k is totally real, and

$$\mathfrak{S}_{21,l}:=\{\mathfrak{p}\mid\mathfrak{p}\nmid l,\ \mathfrak{p} \text{ is ramified in } k/k^+ \text{ and } \mathrm{ord}_2(a_\mathfrak{p})+1\le\mathrm{ord}_2(b_\mathfrak{p}) \text{ (resp. } N\mathfrak{p}\equiv 3 \bmod 4)\}\,,$$

$$\mathfrak{S}_{22,l}:=\{\mathfrak{p}\mid\mathfrak{p}\nmid l,\ \mathfrak{p} \text{ is inert in } k/k^+ \text{ and } \mathrm{ord}_2(a_\mathfrak{p})=\mathrm{ord}_2(b_\mathfrak{p}) \text{ (resp. } \mathrm{ord}_2(a_\mathfrak{p})=1 \text{ and } p\equiv 3 \bmod 4)\}\,,$$

if k is a CM-field. Then Proposition 3.1 and Lemma 3.2, (ii) yield:

PROPOSITION 3.3. *Let l be an odd prime or $l=4$. Under the above notations and the assumption* (3.1), *suppose that S is a subset of the set $\mathfrak{S}_{1,l}$ (resp. $\mathfrak{S}_{21,l} \cup \mathfrak{S}_{22,l}$), if k is totally real (resp. a CM-field). Then for any prime ideal $\mathfrak{P}$ of $\mathfrak{o}_{k(\zeta_l)}$ lying above S, $\mathfrak{P}$ is not decomposed in $k(\zeta_l)/k(\zeta_l)^+$.*

Now we discuss the cardinal of sets $\mathfrak{S}_{1,l}$ and $\mathfrak{S}_{22,l}$.

LEMMA 3.4. *Let l be an odd prime and $e := \mathrm{ord}_2(l-1)(\geq 1)$. For a prime p such that $p \nmid l$, let b_p be the residue degree of p in $\mathbf{Q}(\zeta_l)/\mathbf{Q}$. Then for each i $(1 \leq i \leq e)$, there are infinitely many primes p such that $i = \mathrm{ord}_2(b_p)$ and $p \nmid l$.*

PROOF. Let r be a primitive root mod l and c a divisor of $(l-1)/2^e$. By Dirichlet's density theorem, there are infinitely many primes p such that

$$p \equiv r^{2^{e-i}c} \bmod l\,. \tag{3.5}$$

For such primes p, we have $b_p = (l-1)/(2^{e-i}c)$, therefore $i = \mathrm{ord}_2(b_p)$. This proves our lemma. □

LEMMA 3.5. *Let l be an odd prime or $l=4$. Assume that $k/\mathbf{Q}$ is an abelian extension with the discriminant d. Then under the above notations, we have*

(i) *$[k:\mathbf{Q}]$ is not a power of 2 and $(d, l) = 1 \Rightarrow |\mathfrak{S}_{1,l}| = \infty$.*

(ii) *$l \equiv 1 \bmod 4$ and $(d, l) = 1 \Rightarrow |\mathfrak{S}_{1,l}| = \infty$.*

(iii) *Let k be a CM-field. If we put*

$$\mathfrak{S}_{2,l} := \{\mathfrak{p} \mid \mathfrak{p} \text{ is inert in } k/k^+ \text{ and } p^{a_\mathfrak{p}/2} \equiv -1 \bmod l\}\,,$$

then $\mathfrak{S}_{2,l} \subset \mathfrak{S}_{22,l}$ and $|\mathfrak{S}_{2,l}| = \infty$.

PROOF. (i) Since $[k:\mathbf{Q}]$ is not a power of 2, there is an element σ of $Gal(k/\mathbf{Q})$ of odd prime order. By Tchebotarev's density theorem, there are infinitely many primes p_0 with $p_0 \nmid d$, whose Frobenius automorphism in $k/\mathbf{Q}$ is equal to σ. Take such a prime p_0. Let $m (\in \mathbf{Z})$ be the conductor of $k/\mathbf{Q}$ so that $Gal(k/\mathbf{Q})$ is isomorphic to the quotient group of $(\mathbf{Z}/m\mathbf{Z})^\times$. Since $(d, l) = 1$, $(m, l) = 1$. By Dirichlet's density theorem, there are infinitely many primes p such that $p \equiv p_0 \bmod m$, and (3.5) for $i=1$ (resp. $p \equiv 3 \bmod 4$) holds if l is odd (resp. $l=4$). Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}_k$ lying above such a prime p. Then $\mathrm{ord}_2(b_\mathfrak{p}) = 1$ by Lemma 3.4 and the proof of Lemma 3.2, (ii). Furthermore $\mathrm{ord}_2(a_\mathfrak{p}) = 0$, because σ is also the Frobenius automorphism of p in $k/\mathbf{Q}$ and $a_\mathfrak{p}$ is the order of σ. Hence $\mathfrak{p} \in \mathfrak{S}_{1,l}$. This proves the assertion.

(ii) Now l is odd and, by (i), we may assume that $[k:\mathbf{Q}]$ is a power of 2. So there is an element σ of $Gal(k/\mathbf{Q})$ of order two. Then the same argument as in (i) proves the assertion. (Since $l \equiv 1 \bmod 4$, use (3.5) for $i=2$. Then we obtain $\mathrm{ord}_2(b_\mathfrak{p}) = 2$, $\mathrm{ord}_2(a_\mathfrak{p}) = 1$.)

(iii) Let $\mathfrak{p} \in \mathfrak{S}_{2,l}$. Since $b_\mathfrak{p}$ is the order of p mod l and $p^{a_\mathfrak{p}/2} \equiv -1 \bmod l$, we have

$\mathrm{ord}_2(a_\mathfrak{p})=\mathrm{ord}_2(b_\mathfrak{p})$ (resp. $\mathrm{ord}_2(a_\mathfrak{p})=1$ and $p\equiv 3 \bmod 4$) when l is odd (resp. $l=4$). Hence $\mathfrak{p}\in\mathfrak{S}_{22,l}$ so that $\mathfrak{S}_{2,l}\subset\mathfrak{S}_{22,l}$. By Dirichlet's density theorem, there are infinitely many primes p such that $p\equiv -1 \bmod ml$. Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}_k$ lying above such a prime p. Since $p\equiv -1 \bmod m$, the complex conjugation ρ $(\neq 1)$ on k is the Frobenius automorphism of p in $k/\mathbf{Q}$. So $a_\mathfrak{p}=2$ and $\mathfrak{p}$ is inert in k/k^+. Hence $\mathfrak{p}\in\mathfrak{S}_{2,l}$. This proves our lemma. □

4. A sufficient condition for the non-existence.

We assume that $k/\mathbf{Q}$ is a Galois extension of even degree and K/k is a finite abelian extension with conductor $\mathfrak{m}$. And we write the finite component $\mathfrak{m}_0$ of $\mathfrak{m}$ as the form $\mathfrak{m}_0=\mathfrak{m}_1\mathfrak{m}_2$, satisfying that "$\mathfrak{p}\,|\,\mathfrak{m}_1\Rightarrow\mathrm{ord}_\mathfrak{p}(\mathfrak{m}_0)=1$" and "$\mathfrak{p}\,|\,\mathfrak{m}_2\Rightarrow\mathrm{ord}_\mathfrak{p}(\mathfrak{m}_0)\geq 2$". Let l be a fixed odd prime such that $k\cap\mathbf{Q}(\zeta_l)=\mathbf{Q}$. Put $\mathfrak{S}_l:=\mathfrak{S}_{1,l}$ (resp. $\mathfrak{S}_{21,l}\cup\mathfrak{S}_{22,l}$), when k is totally real (resp. a CM-field), where the set $\mathfrak{S}_{*,l}$ is defined before Proposition 3.3. Suppose that $S=S_l$ is a finite subset of $\mathfrak{S}_l$ such that $\{\mathfrak{p}\ ;\ \mathfrak{p}\,|\,\mathfrak{m}_2\}\subset S$. So S contains all prime ideals of $\mathfrak{o}_k$ which are wildly ramified in K/k, by the conductor-discriminant theorem. For a prime ideal $\mathfrak{p}$ of $\mathfrak{o}_k$, $e_\mathfrak{p}$ denotes the ramification index of $\mathfrak{p}$ in $k/\mathbf{Q}$. We define the finite set of prime ideals of $\mathfrak{o}_k$ as follows.

$$\mathfrak{T}_l:=\{\mathfrak{p}\ ;\ 2\,|\,e_\mathfrak{p},\ \mathrm{ord}_2(b_\mathfrak{p})=0\}\ ,$$

where $b_\mathfrak{p}$ is the residue degree of $\mathfrak{p}\cap\mathbf{Z}$ in $\mathbf{Q}(\zeta_l)/\mathbf{Q}$. Then note that $\mathfrak{T}_l\cap\mathfrak{S}_{1,l}=\mathfrak{T}_l\cap\mathfrak{S}_{21,l}=\varnothing$.

THEOREM 4.1. *Under the above assumptions and notations, suppose that $Gal(K\cap\tilde{k}/k)$ is a 2-group and that there exists some $\mathfrak{p}$ with $\mathfrak{p}\nmid 2$ in $\mathfrak{T}_l$, not belonging to S, such that $l\mid[K\cap k(\mathfrak{p}):k]$. Then $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ does not have a normal basis.*

REMARK 4.2. As seen below, note that $\mathfrak{p}\nmid l$. And note that $l\mid[k(\mathfrak{p}):k]=(N\mathfrak{p}-1)h_k/w_\mathfrak{p}$, where $w_\mathfrak{p}:=|(\mathfrak{o}_k^\times+\mathfrak{p})/\mathfrak{p}|$ and $h_k:=[\tilde{k}:k]$.

PROOF OF THEOREM 4.1. Let $L:=K\cap k(\mathfrak{p})$. Since $l\mid[L:k]$, there exists some χ in $Gal(L/k)^\wedge$ such that $g_\chi=l$. Let k_χ be the fixed field of $\mathrm{Ker}\,\chi$ in L/k. Then $\mathfrak{p}$ is ramified in k_χ/k. If not so, then $k_\chi\subset\tilde{k}$ so that $k_\chi\subset K\cap\tilde{k}$. This contradicts that $Gal(K\cap\tilde{k}/k)$ is a 2-group. Consequently since $k_\chi\subset k(\mathfrak{p})$, $\mathfrak{p}$ is tamely ramified in k_χ/k so that $\mathfrak{p}\nmid g_\chi$.

Assume that $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ has a normal basis; therefore so does $\mathfrak{o}_L(S)/\mathfrak{o}_k(S)$. By the assumed tameness in K/k outside S, there is some γ in $\mathfrak{o}_L(S)$ such that $\mathrm{Tr}_{L/k}(\gamma)=\langle\gamma,1\rangle_{L/k}=1$. This yields that there is some α in $\mathfrak{o}_L(S)$ such that α is a generator of normal basis of $\mathfrak{o}_L(S)/\mathfrak{o}_k(S)$ with $\langle\alpha,1\rangle=1$. If $\mathfrak{b}(\chi)$ is the fractional ideal of $\mathfrak{o}_{k(\chi)}(S)$ depending on α as in (2.1), then we have $\mathfrak{b}(\chi)=(1)$ by [8, Lemma 2.8, (ii)]. Furthermore $\mathfrak{p}$ is totally ramified in k_χ/k and $k\cap\mathbf{Q}(\chi)=\mathbf{Q}$ by the assumption. So by Proposition 2.3, (ii),

$$(4.1)\qquad (\langle\alpha,\chi\rangle^{g_\chi})\,\mathfrak{o}_{k(\chi)}(S)=\mathfrak{P}^\theta\ ,$$

where θ is defined in (2.8) and $\mathfrak{P}$ is some prime ideal of $\mathfrak{o}_{k(\chi)}$ lying above $\mathfrak{p}$. Put $p:=\mathfrak{p}\cap\mathbf{Q}$ and $P:=\mathfrak{P}\cap\mathbf{Q}(\chi)$. Let $b:=b_{\mathfrak{p}}$ and q be the cardinal of $\mathfrak{o}_{\mathbf{Q}(\chi)}/P$ so that $q=p^b$ and $\mathfrak{o}_{\mathbf{Q}(\chi)}/P$ is identified with the field $\mathbf{F}_q$ of q elements. Let T be the trace map from $\mathbf{F}_q$ to $\mathbf{F}_p$. Define

$$\psi:\mathbf{F}_q\longrightarrow\mathbf{C}^\times\,,\qquad \psi(x)=\zeta_p^{\mathrm{T}(x)}\,.$$

Let $\left(\frac{x}{P}\right)_{g_\chi}$ be the g_χth power residue symbol mod P in $\mathbf{Q}(\chi)$. Define the Gauss sum

$$\tau:=-\sum_{x\in\mathbf{F}_q^\times}\left(\frac{x}{P}\right)_{g_\chi}^{-1}\psi(x)\,.$$

Let $\Omega:=Gal(k(\chi)/k)$. Since $p\nmid g_\chi$, note that there is a canonical isomorphism:

$$\Omega\cong Gal(\mathbf{Q}(\chi)/\mathbf{Q})\cong Gal(\mathbf{Q}(\zeta_p)(\chi)/\mathbf{Q}(\zeta_p))\,.$$

By Stickelberger's theorem,

$$(\tau^{g_\chi})\mathfrak{o}_{\mathbf{Q}(\chi)}=P^\theta\,. \tag{4.2}$$

Now we establish some relation between Gauss sum τ and the resolvent $\langle\alpha,\chi\rangle$. As $p\nmid g_\chi$, p is unramified in $\mathbf{Q}(\chi)/\mathbf{Q}$. So $e:=e_{\mathfrak{p}}$ is the ramification index of $\mathfrak{P}$ in $k(\chi)/\mathbf{Q}(\chi)$. Let Z be the decomposition group of $\mathfrak{P}$ in $k(\chi)/\mathbf{Q}(\chi)$ and put $\mathscr{G}:=Gal(k(\chi)/\mathbf{Q}(\chi))$. Then elements of Ω and $\mathscr{G}$ are commutative. So by (4.2) and (4.1),

$$\begin{aligned}(\tau^{g_\chi})\mathfrak{o}_{k(\chi)}(S)&=\Big(\prod_{\sigma\in\mathscr{G}/Z}\mathfrak{P}^\sigma\Big)^{\theta e}=\prod_{\sigma\in\mathscr{G}/Z}(\mathfrak{P}^\theta)^{e\sigma}\\&=\Big(\prod_{\sigma\in\mathscr{G}/Z}\langle\alpha,\chi\rangle^{g_\chi e\sigma}\Big)\mathfrak{o}_{k(\chi)}(S)\,.\end{aligned} \tag{4.3}$$

As g_χ is odd, there is some ω in Ω such that $\zeta^\omega=\zeta^2$, where ζ is a primitive g_χth root of unity. Let $J:=\tau^{2-\omega}$ (Jacobi sum) in $\mathbf{Q}(\chi)$. Then we have

$$J\bar{J}=q\,,\qquad J\equiv-1 \bmod (\zeta-1)\,,$$

where the bar denotes the complex conjugation. Let $A:=\langle\alpha,\chi\rangle^{2-\tilde{\omega}}$ in $k(\chi)$ where $\tilde{\omega}$ is an extension of ω to $L(\chi)$, and put $B:=\prod_{\sigma\in\mathscr{G}/Z}A^\sigma$. Then since $\langle\alpha,\chi\rangle\equiv\langle\alpha,1\rangle=1 \bmod (\zeta-1)$, we have $B\equiv1 \bmod (\zeta-1)$. Furthermore it follows from (4.3) that $(J)\mathfrak{o}_{k(\chi)}(S)=(B^e)\mathfrak{o}_{k(\chi)}(S)$. Hence there exists some ε in $\mathfrak{o}_{k(\chi)}(S)^\times$ such that

$$B^e=\varepsilon J\,. \tag{4.4}$$

By the definition of S and Proposition 3.3, the complex conjugation acts trivially on S; therefore $\varepsilon\in\mathfrak{o}_{k(\chi)}(S)^\times$ implies $\bar{\varepsilon}\in\mathfrak{o}_{k(\chi)}(S)^\times$ and $\mathrm{ord}_{\mathfrak{P}}(\varepsilon/\bar{\varepsilon})=0$ for any prime ideal $\mathfrak{P}$ of $\mathfrak{o}_{k(\chi)}$ lying above S. Since k is a totally real number field or a CM-field, $k(\chi)$ is a CM-field. Hence $\varepsilon/\bar{\varepsilon}$ is a root of unity by the generalized Dirichlet's unit theorem. Let $2^a w$ be the number of roots of unity in $k(\chi)$ where w is odd. Since $J/\bar{J}=J^2/q$, it follows from (4.4) that

$$(B/\bar{B})^{we}=(J^w/q^{w/2})^2\cdot(\varepsilon/\bar{\varepsilon})^w.$$

Since e is even, there is some 2-power root of unity ξ such that

$$(B/\bar{B})^{we/2}=\pm J^w/(q^{w/2}\xi).$$

It follows from $B\equiv 1$, $J\equiv -1 \bmod (\zeta-1)$ and $(q, g_\chi)=1$ that

$$q^{w/2}\xi\equiv\pm 1 \bmod (\zeta-1). \tag{4.5}$$

Let $F:=\mathbf{Q}(\chi)(q^{1/2}, \xi)$. As b is odd, we have $q^{1/2}\notin\mathbf{Q}$. Since $(2q, g_\chi)=1$, $Gal(\mathbf{Q}(q^{1/2}, \xi)/\mathbf{Q})$ is identified with $Gal(F/\mathbf{Q}(\chi))$. Therefore by $(2, q)=1$, there is an isomorphism φ of $F/\mathbf{Q}(\chi)$ such that $\varphi(\xi)=\xi$ and $\varphi(q^{1/2})=-q^{1/2}$. Applying φ to (4.5), since w is odd, we have $1\equiv -1 \bmod (\zeta-1)$, hence $l=g_\chi=2$. This is a contradiction. Thus our theorem is proved. $\square$

PROPOSITION 4.3. *Assume that $\mathbf{Q}\subset k\subset K\subset\mathbf{Q}(\zeta_p)$, p being an odd prime, and $[k:\mathbf{Q}]$ is even. Suppose that there exists an odd prime l such that $l\mid[K:k]$. Then for any finite subset S (or $S=\varnothing$) of $\mathfrak{S}_l$, $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ does not have a normal basis.*

REMARK 4.4. If we assume that $l\equiv 1 \bmod 4$ in the case where k is totally real and $[k:\mathbf{Q}]$ is a power of 2, then the set $\mathfrak{S}_l$ is always infinite by Lemma 3.5.

PROOF OF PROPOSITION 4.3. By $(p, l)=1$, we have $k\cap\mathbf{Q}(\zeta_l)=\mathbf{Q}$. Let $\mathfrak{p}$ be the unique prime ideal of $\mathfrak{o}_k$ lying above p. Since $\mathfrak{p}$ is totally ramified in K/k, we have $K\cap\tilde{k}=k$. Furthermore since $\mathfrak{p}$ is tamely ramified and only a prime ideal of $\mathfrak{o}_k$ which is ramified in K/k, the conductor of K/k is of the form $\mathfrak{p}\mathfrak{m}_\infty$ (therefore $\mathfrak{m}_2=1$). So $l\mid[K\cap k(\mathfrak{p}):k]$, because $[k(\mathfrak{p}\mathfrak{m}_\infty):k(\mathfrak{p})]$ is a power of 2 by class field theory. Now $e_\mathfrak{p}=[k:\mathbf{Q}]\Rightarrow 2\mid e_\mathfrak{p}$ and $p\equiv 1 \bmod l\Rightarrow b_\mathfrak{p}=1$; therefore $\mathrm{ord}_2(b_\mathfrak{p})=0$, so that $\mathfrak{p}\in\mathfrak{T}_l$. Claim that $\mathfrak{p}\notin S$. This follows from $\mathfrak{T}_l\cap\mathfrak{S}_{1,l}=\varnothing$ when k is totally real. When k is a CM-field, if $\mathfrak{p}\in S$, then we have $\mathfrak{p}\in\mathfrak{S}_{22,l}$ ($\because\mathfrak{T}_l\cap\mathfrak{S}_{21,l}=\varnothing$), so that $\mathfrak{p}$ is inert in k/k^+. This contradicts that $\mathfrak{p}$ is totally ramified in $k/\mathbf{Q}$. Hence $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ does not have a normal basis by Theorem 4.1. $\square$

PROPOSITION 4.5. *Let k be a quadratic field such that $[\tilde{k}:k]$ is a power of 2 and $\mathfrak{p}$ a prime ideal of $\mathfrak{o}_k$ which is ramified in $k/\mathbf{Q}$. Put $p:=\mathfrak{p}\cap\mathbf{Z}$. Suppose that there exists an odd prime l such that $l\,|\,((p-1)/w_\mathfrak{p})$, where $w_\mathfrak{p}$ is defined in Remark 4.2. Then for any finite subset S (or $S=\varnothing$) of $\mathfrak{S}_l$, $\mathfrak{o}_{k(\mathfrak{p})}(S)/\mathfrak{o}_k(S)$ does not have a normal basis.*

REMARK 4.6. By Lemma 3.5, the set $\mathfrak{S}_l$ is always infinite, if we assume that $l\equiv 1 \bmod 4$ and l is prime to the discriminant of $k/\mathbf{Q}$ when k is a real quadratic field.

PROOF OF PROPOSITION 4.5. Now $e_\mathfrak{p}=2$, $\mathrm{N}\mathfrak{p}=p$ and $b_p=1$ hold. Since $p\neq l$, $k\cap\mathbf{Q}(\zeta_l)=\mathbf{Q}$. And we have $\mathfrak{p}\notin S$ by the same reason as in the proof of Proposition 4.3.

Hence Theorem 4.1 implies our assertion. □

5. Normal integral bases in abelian fields with prime conductors.

Let p be an odd prime. In this section, we let K be a subfield of the pth cyclotomic field $\mathbf{Q}(\zeta_p)$, and k a subfield of K. Let $n:=[K:k](>1)$ and $m:=[k:\mathbf{Q}]$. If $m=1$, then it is well known that $\mathfrak{o}_K/\mathfrak{o}_k$ has a normal basis. So we assume that $m>1$ throughout this section. Our goal is Theorem 5.3.

Let $\Gamma:=Gal(K/\mathbf{Q})$. Since Γ is cyclic, so is the group $\hat{\Gamma}$ of its characters; let ψ_0 be a fixed generator of $\hat{\Gamma}$. There exists a natural surjective group homomorphism:

$$\hat{\Gamma} \longrightarrow \hat{G}, \qquad \psi \longmapsto \psi|_G .$$

For a positive integer i, we put $\psi_i:=\psi_0^i$ and $\chi_i:=\psi_i|_G$. Let $l_i:=(i/d, m)$ where $d=d_i$ is the greatest common divisor of i and n. Then

$$g_{\psi_i}=\frac{m}{l_i}g_{\chi_i}, \tag{5.1}$$

where g_{ψ_i} (resp. g_{χ_i}) is the order of ψ_i (resp. χ) in $\hat{\Gamma}$ (resp. $\hat{G}$). For a number field N and each $\psi\in\hat{\Gamma}$, $N(\psi)$ denotes the field generated by the value of ψ on Γ over N. Let $\Omega_i:=Gal(k(\psi_i)/k)$ and ξ_i be a fixed primitive g_{ψ_i}th root of unity. Since $k\cap\mathbf{Q}(\psi_i)=\mathbf{Q}$ by $(p, g_{\psi_i})=1$, there exists a group isomorphism ι_i of Ω_i into $(\mathbf{Z}/g_{\psi_i}\mathbf{Z})^\times$ such that $\xi_i^\omega=\xi_i^{\iota_i(\omega)}$ for all $\omega\in\Omega_i$. For each $\omega\in\Omega_{\psi_i}$, let $t_i(\omega)$ be the integer satisfying $\iota_i(\omega)=t_i(\omega) \bmod g_{\psi_i}$, $0<t_i(\omega)<g_{\psi_i}$ and put

$$\eta_i:=\sum_{\omega\in\Omega_i}[l_it_i(\omega)/g_{\chi_i}]\omega^{-1},$$

where $[x]$ denotes the greatest integer $\leq x$ as usual for a real number x. For each $\psi\in\hat{\Gamma}$, we define the group homomorphism $\det_\psi$ by

$$\det_\psi : k\Gamma^\times \longrightarrow k(\psi)^\times, \qquad \sum_{s\in\Gamma}a_s s \longmapsto \sum_{s\in\Gamma}\psi(s)a_s .$$

PROPOSITION 5.1. *Let $\beta\in\mathfrak{o}_K$ be a free generator of K over kG. Then there exists some λ in $k\Gamma^\times$ such that for any positive integer i with $i\not\equiv 0 \bmod n$, we have*

$$\mathfrak{b}(\chi_i)^{-1}=(\det_{\psi_i}(\lambda))\mathfrak{P}_i^{\eta_i}, \tag{5.2}$$

where $\mathfrak{P}_i$ is some prime ideal of $\mathfrak{o}_{k(\psi_i)}$ lying above p and, taking $S=\varnothing$, $\mathfrak{b}(\chi_i)$ is the fractional ideal of $\mathfrak{o}_{k(\chi_i)}$ depending on β as in (2.1).

PROOF. Let $\alpha:=\mathrm{Tr}_{\mathbf{Q}(\zeta_p)/K}(\zeta_p)$. Since α is a free generator of K over $\mathbf{Q}\Gamma$, we can prove the following in the same way as in Fröhlich [7, Lemma 6.2 and Theorem 25, (ii) of Chapter III]: there exists some λ in $k\Gamma^\times$ such that

(5.3) $$\langle \beta, \psi|_G \rangle_{K/k} = \det_\psi(\lambda) \langle \alpha, \psi \rangle_{k/\mathbf{Q}},$$

for all $\psi \in \hat{\Gamma}$. Let $\tilde{\psi}_i$ be the character of $Gal(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ of order g_{ψ_i}, defined by $\tilde{\psi}_i(s) := \psi_i(s|_K)$ for all $s \in Gal(\mathbf{Q}(\zeta_p)/\mathbf{Q})$. Then it follows from the definition of α that

$$\langle \alpha, \psi_i \rangle_{K/\mathbf{Q}} = \sum_{s \in Gal(\mathbf{Q}(\zeta_p)/\mathbf{Q})} \tilde{\psi}_i(s^{-1}) \zeta_p^s .$$

Let P be any prime ideal of $\mathfrak{o}_{\mathbf{Q}(\psi_i)}$ lying above p. Since $p \equiv 1 \mod g_{\psi_i}$, p is completely decomposed in $\mathbf{Q}(\psi_i)/\mathbf{Q}$ so that $\mathfrak{o}_{\mathbf{Q}(\psi_i)}/P$ is identified with the field $\mathbf{F}_p$ of p elements. Since $i \not\equiv 0 \mod n$, $g_{\chi_i} > 1$ so that $g_{\psi_i} > 1$. Let $\left(\frac{x}{P}\right)_{g_{\psi_i}}$ be the g_{ψ_i}th power residue symbol mod P in $\mathbf{Q}(\psi_i)$ which can be regarded as a character of $\mathbf{F}_p^\times$ of order g_{ψ_i}. Since $Gal(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ is identified with $\mathbf{F}_p^\times$, $\tilde{\psi}_i$ is also a character of $\mathbf{F}_p^\times$ of order g_{ψ_i}. Consequently there is some δ in $\Omega_i \cong (\mathbf{Z}/g_{\psi_i}\mathbf{Z})^\times$ such that $\tilde{\psi}_i = \left(\frac{\ }{P}\right)_{g_{\psi_i}}^\delta$. Define the Gauss sum

$$\tau := -\sum_{x \in \mathbf{F}_p^\times} \left(\frac{x}{P}\right)_{g_{\psi_i}}^{-1} \zeta_p^x .$$

As $(p, g_{\psi_i}) = 1$, Ω_i can be identified with $Gal(\mathbf{Q}(\zeta_p)(\psi_i)/\mathbf{Q}(\zeta_p))$. Hence we have $\langle \alpha, \psi_i \rangle_{K/\mathbf{Q}} = -\tau^\delta$. Since P is totally ramified in $k(\psi_i)/\mathbf{Q}(\psi_i)$, $P = \mathfrak{P}^m$ with some prime ideal $\mathfrak{P}$ of $\mathfrak{o}_{k(\psi_i)}$. Let $\mathfrak{P}_i := \mathfrak{P}^\delta$. Then we have by Stickelberger's theorem

$$(\langle \alpha, \psi_i \rangle_{K/\mathbf{Q}}^{g_{\psi_i}}) = \mathfrak{P}_i^{m\theta_i} ,$$

where we put $\theta_i := \sum_{\omega \in \Omega_i} t_i(\omega) \omega^{-1}$. Hence it follows from (5.3) that

(5.4) $$(\langle \beta, \chi_i \rangle_{K/k}^{g_{\psi_i}}) = (\det_{\psi_i}(\lambda)^{g_{\psi_i}}) \mathfrak{P}_i^{m\theta_i} .$$

Let $\mathfrak{p}$ be the unique prime ideal of $\mathfrak{o}_k$ lying above p. Since $\mathfrak{p} \nmid g_{\chi_i}$, we have by (2.3) and Proposition 2.3, (i),

(5.5) $$(\langle \beta, \chi_i \rangle_{K/k}^{g_{\chi_i}}) = \mathfrak{a}(\chi_i) \mathfrak{b}(\chi_i)^{-g_{\chi_i}}$$

and $\mathfrak{a}(\chi_i)$ is a g_{χ_i}-power free ideal of $\mathfrak{o}_{k(\chi_i)}$. Hence (5.2) follows from (5.1), (5.4), (5.5) and the definition of η_i. This proves our proposition. □

PROPOSITION 5.2. *Let i be a positive integer with $i \not\equiv 0 \mod n$ and β, $\mathfrak{b}(\chi_i)$ as in Proposition 5.1. Under the above notations, assume that $(l_i, g_{\psi_i}) = 1$, $l_i > 1$ and one of the following conditions is satisfied*:

(i) *l_i is odd and $g_{\chi_i} > 2$,*
(ii) *l_i is even, $l_i \geq 4$ and "$l_i \neq 6$ or $g_{\chi_i} \neq 5$".*

Then $\mathfrak{b}(\chi_i)$ is not a principal ideal of $\mathfrak{o}_{k(\chi_i)}$.

PROOF. Since $l_i | m$, there exists the unique subfield F of k with $[k : F] = l_i$. Let $\mathcal{G} := Gal(k(\psi_i)/F(\psi_i))$ and $\mathfrak{P}_i$ be as in Proposition 5.1. Assume that $\mathfrak{b}(\chi_i)$ is a principal ideal of $\mathfrak{o}_{k(\chi_i)}$. So by Proposition 5.1, there is some A in $k(\psi_i)^\times$ such that $\mathfrak{P}_i^{\eta_i}=(A)$. Let $\omega_0\in\Omega_i$ such that $\xi_i^{\omega_0}=\xi_i^{-1}$. Since $\mathfrak{P}_i$ is totally ramified in $k(\psi_i)/\mathbf{Q}(\psi_i)$, we have $\overline{\mathfrak{P}_i}=\mathfrak{P}_i^{\omega_0}$ so that $\overline{\mathfrak{P}_i^{\eta_i}}=\mathfrak{P}_i^{\eta_i\omega_0}$, since $k(\psi_i)/\mathbf{Q}$ is abelian, where the bar denotes the complex conjugation. It is easy to see that $\eta_i-\eta_i\omega_0=\sum_{\omega\in\Omega_i}\{2[l_it_i(\omega)/g_{\chi_i}]+1-m\}\omega^{-1}$. Hence we have

$$\operatorname{ord}_{\mathfrak{P}_i}(A/\bar{A})=2[l_i/g_{\chi_i}]+1-m\,. \tag{5.6}$$

For a Dedekind domain $\mathfrak{o}$, we denote by $P(\mathfrak{o})$ the group of principal ideals of $\mathfrak{o}$. The group $P(\mathfrak{o}_{F(\psi_i)})$ can be regarded as a subgroup of $P(\mathfrak{o}_{k(\psi_i)})$ by the extension of ideals. Then $P(\mathfrak{o}_{k(\psi_i)})^{\mathscr{G}}/P(\mathfrak{o}_{F(\psi_i)})$ is isomorphic to the cohomology group $\mathrm{H}^1(\mathscr{G},\mathfrak{o}_{k(\psi_i)}^\times)$, where $P(\mathfrak{o}_{k(\psi_i)})^{\mathscr{G}}$ denotes the group of elements of $P(\mathfrak{o}_{k(\psi_i)})$, fixed by $\mathscr{G}$. Furthermore since $\mathscr{G}$ is cyclic, this cohomology group is isomorphic to ${}_{\mathrm{N}}(\mathfrak{o}_{k(\psi_i)}^\times)/(\mathfrak{o}_{k(\psi_i)}^\times)^{\sigma-1}$, where σ is a generator of $\mathscr{G}$, ${}_{\mathrm{N}}(\mathfrak{o}_{k(\psi_i)}^\times):=\{u\in\mathfrak{o}_{k(\psi_i)}^\times\mid \mathrm{N}(u)=1\}$ and N is the norm map from $k(\psi_i)$ to $F(\psi_i)$. Let $(x)\in P(\mathfrak{o}_{k(\psi_i)})^{\mathscr{G}}$. Then under this group isomorphism, the class of (x) corresponds to the class of $x^{\sigma-1}$, and the class of $(x/\bar{x})$ corresponds to the class of $x^{\sigma-1}/\overline{x^{\sigma-1}}$, since $k(\psi_i)$ is a CM-field.

Since $\mathfrak{P}_i$ is totally ramified in $k(\psi_i)/F(\psi_i)$ and $k(\psi_i)/F$ is abelian, $\mathfrak{P}_i^{\eta_i}$ is now fixed by $\mathscr{G}$. So $(A)\in P(\mathfrak{o}_{k(\psi_i)})^{\mathscr{G}}$. We claim that $(A/\bar{A})$ belongs to $P(\mathfrak{o}_{F(\psi_i)})$ if l_i is odd, and to $\langle(\sqrt{a})\bmod P(\mathfrak{o}_{F(\psi_i)})\rangle$ if l_i is even, where $\sqrt{a}$ $(a\in F(\psi_i)^\times)$ is a primitive element of the quadratic subextension of $k(\psi_i)/F(\psi_i)$. Put indeed $u:=A^{\sigma-1}$. Since $k(\psi_i)$ is a CM-field, $u/\bar{u}$ is a root of unity by Dirichlet's unit theorem. As $k\subsetneq\mathbf{Q}(\zeta_p)$, the group of roots of unity in $k(\psi_i)$ is generated by $\pm\xi_i$. So $u/\bar{u}=(-\xi_i)^v$ with some integer v. Taking the norm N, we see $1=(-\xi_i)^{vl_i}$, therefore $2g_{\psi_i}\mid vl_i$. Since $(l_i, g_{\psi_i})=1$, we have $2g_{\psi_i}\mid v$ (resp. $g_{\psi_i}\mid v$), hence $u/\bar{u}=1$ (resp. ± 1) when l_i is odd (resp. even). Thus our claim is proved since $\sqrt{a}^{\,\sigma-1}=-1$. Hence there are some ε in $\mathfrak{o}_{k(\psi_i)}^\times$ and some b in $F(\psi_i)^\times$ such that $A/\bar{A}=\sqrt{a}^{\,j}b\varepsilon$, where $j=0$ or 1, and if l_i is odd, then we put $j=0$. So

$$\operatorname{ord}_{\mathfrak{P}_i}(A/\bar{A})\equiv j\frac{l_i}{2}\operatorname{ord}_{P_i}(a)\quad \operatorname{mod} l_i\,,$$

where let $P_i:=\mathfrak{P}_i\cap F(\psi_i)$. It follows from (5.6) that

$$2[l_i/g_{\chi_i}]+1\equiv j\frac{l_i}{2}\operatorname{ord}_{P_i}(a)\quad \operatorname{mod} l_i\,. \tag{5.7}$$

(i) The case where l_i is odd. As $g_{\chi_i}>2$, $2[l_i/g_{\chi_i}]+1\le 2(l_i-1)/2+1=l_i$. So it follows from $j=0$ and (5.7) that $2[l_i/g_{\chi_i}]+1=l_i$. Since $(l_i, g_{\chi_i})=1$, we can write $l_i=g_{\chi_i}q+r$ with some non-negative integer q and $0<r<g_{\chi_i}$. Therefore $(2-g_{\chi_i})q=r-1$, so $q=0$, $r=1$. Hence we have $l_i=1$. This is a contradiction.

(ii) The case where l_i is even. Then it follows from (5.7) that j $(=1)$, $l_i/2$ and $\operatorname{ord}_{P_i}(a)$ are all odd. So we have $2[l_i/g_{\chi_i}]+1\equiv l_i/2 \bmod l_i$. Since $(l_i, g_{\chi_i})=1$ and $g_{\chi_i}>1$, we have $g_{\chi_i}>2$, hence $2[l_i/g_{\chi_i}]+1=l_i/2$. We write $l_i=g_{\chi_i}q+r$ with some non-negative integer q and $0<r<g_{\chi_i}$. Then

(5.8) $$(4-g_{\chi_i})q=r-2\,.$$

If $r>2$, then $g_{\chi_i}<4$ from (5.8). Since g_{χ_i} is odd, $g_{\chi_i}=3$ so that $2<r<3$. This is a contradiction. Therefore $r=1$ or 2. If $r=2$, then $q=0$ by (5.8) so that $l_i=2$. This contradicts $l_i\geq 4$. If $r=1$, then $g_{\chi_i}=5$ and $l_i=6$ from (5.8). This is a contradiction. Thus our proposition is proved. □

THEOREM 5.3. *Under the above notations, we have the following*:

(I) $\mathfrak{o}_K/\mathfrak{o}_k$ *does not have a normal basis, except for the following four cases*:

(i) *m is even and not a power of* 2, *and* $n=2$.

(ii) *m and n are both powers of* 2.

(iii) *m is a power of q and n is a power of q or* $2\times$(*a power of q*), *with some odd prime q*.

(iv) *m is odd and* $n=2$.

(II) *In the case* (I-iv), $\mathfrak{o}_K/\mathfrak{o}_k$ *has a normal basis.* (*For the other cases, see the remark below.*)

PROOF. Let $\beta\in\mathfrak{o}_K$ be a free generator of $\mathfrak{o}_{k_\mathfrak{p}}\otimes_{\mathfrak{o}_k}\mathfrak{o}_k$ over $\mathfrak{o}_{k_\mathfrak{p}}G$ for each prime ideal $\mathfrak{p}$ of $\mathfrak{o}_k$, dividing the order of G.

(I) By Proposition 4.3, we need prove when (A): m is even and n is a power of 2, or (B): m is odd.

The case (A). Let $v:=\mathrm{ord}_2(m)$ and $i:=m/2^v$. Then $l_i=i$, $g_{\chi_i}=n/(i,n)=n$ so that $(l_i,g_{\psi_i})=1$ by (5.1). Since we make exceptions of the cases (ii) and (i), we have $l_i>1$ so that $g_{\chi_i}>2$. Therefore it follows from Proposition 5.2, (i) that $\mathfrak{b}(\chi_i)$ is not a principal ideal of $\mathfrak{o}_{k(\chi_i)}$. Hence $\mathfrak{o}_K/\mathfrak{o}_k$ does not have a normal basis by [8, Theorem 2.10, (ii)].

The case (B). If n is not a power of 2, then there is some odd prime q with $q\,|\,n$. Let $v:=\mathrm{ord}_q(m)(\geq 0)$. When $m/q^v>1$, putting $i:=mn/q^{v+1}$, we have $l_i=m/q^v>1$, $g_{\chi_i}=q>2$, $(l_i,g_{\psi_i})=1$ so that $\mathfrak{b}(\chi_i)$ is not principal by Proposition 5.2, (i). When $m=q^v$, let $w:=\mathrm{ord}_q(n)$ and $i:=q^{v+w}$. Then $l_i=m>1$, $g_{\chi_i}=n/q^w$, $(l_i,g_{\psi_i})=1$. Since we make exception of the case (iii), $n/q^w>2$ so that $g_{\chi_i}>2$. Hence $\mathfrak{b}(\chi_i)$ is not principal by Proposition 5.2, (i). If n is a power of 2, then we put $i:=m$. So $l_i=m>1$, $g_{\chi_i}=n$, $(l_i,g_{\psi_i})=1$. Since we make exception of the case (iv), $n>2$ so that $g_{\chi_i}>2$. Hence $\mathfrak{b}(\chi_i)$ is not principal by Proposition 5.2, (i). Thus $\mathfrak{o}_K/\mathfrak{o}_k$ does not have a normal basis by [8, Theorem 2.10, (ii)].

(II) Let $i:=m$. Then $g_{\chi_i}=g_{\psi_i}=2$, $l_i=m$, $\Omega_i=\{1\}$. So $\hat{G}=\{1,\chi_i\}$. Put $\pi:=\mathrm{N}_{\mathbf{Q}(\zeta_p)/k}(1-\zeta_p)$ so that $\mathfrak{P}_i=(\pi)$. As $\eta_i=(m-1)/2$, it follows from (5.2) that

$$\mathfrak{b}(\chi_i)^{-1}=(\pi^{(m-1)/2}\det{}_{\psi_i}(\lambda))\,.$$

From (5.3), $\langle\beta,1\rangle_{K/k}=\det_1(\lambda)\,\mathrm{Tr}_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}(\zeta_p)=-\det_1(\lambda)$. Since $\mathfrak{b}(1)^{-1}=(\langle\beta,1\rangle_{K/k})$ by [8, Remark 2.12], we have

$$\mathfrak{b}(1)^{-1}=(\det{}_1(\lambda))\,.$$

It follows from the definition of β and [8, Lemma 2.8, (ii)] that any prime divisor of

$\mathfrak{d}(1)$ and $\mathfrak{d}(\chi_i)$ does not divide two. Let $u := \zeta_p + \zeta_p^{-1}$ which is a unit in $\mathbf{Q}(\zeta_p)^+$. Since m is odd, $k \subset \mathbf{Q}(\zeta_p)^+$. As $u \equiv \mathrm{N}_{\mathbf{Q}(\zeta_p)/\mathbf{Q}(\zeta_p)^+}(1-\zeta_p) \bmod 2$, we have $\mathrm{N}_{\mathbf{Q}(\zeta_p)^+/k}(u) \equiv \pi \bmod 2$. Let $\varepsilon := \mathrm{N}_{\mathbf{Q}(\zeta_p)^+/k}(u)^{-(m-1)/2} \in \mathfrak{o}_k^\times$. So we have $\varepsilon\pi^{(m-1)/2} \equiv 1 \bmod 2$. Since $\det_1(\lambda) \equiv \det_{\psi_i}(\lambda) \bmod 2$ by $g_{\psi_i} = 2$,

$$\det_1(\lambda) - \varepsilon\pi^{(m-1)/2} \det_{\psi_i}(\lambda) \equiv 0 \bmod 2 .$$

Hence by [8, Remark 2.11], $\mathfrak{o}_K/\mathfrak{o}_k$ has a normal basis. Thus our theorem is proved. □

REMARK 5.4. Let $K := \mathbf{Q}(\zeta_p)$ and $k := \mathbf{Q}(\zeta_p)^+$ with $p \equiv 1 \bmod 4$. So $n=2$ and m is even. Then it is well known that ζ_p is a generator of normal basis of $\mathfrak{o}_K/\mathfrak{o}_k$ (in the cases (I-i, ii)). In the case (I-ii), if $n=2$, then we can prove that $\mathfrak{o}_K/\mathfrak{o}_k$ has a normal basis. In the case (I-iii), $\mathfrak{o}_K/\mathfrak{o}_k$ does not have a normal basis by Brinkhuis [1, Theorem 4.1], because a sequence of Galois extension $\mathbf{Q} \subset k \subset K$ does not split and $[k : \mathbf{Q}]$ is odd. The question is still open as to other cases.

Let S be any finite set of prime ideals of $\mathfrak{o}_k$ which contains the unique prime ideal of $\mathfrak{o}_k$ lying above p and assume that $(m, n) = 1$. Then it is easy to see that $\mathfrak{o}_K(S)/\mathfrak{o}_k(S)$ has a normal basis.

References

[1] J. BRINKHUIS, Normal integral bases and embedding problems, Math. Ann. **264** (1983), 537–543.
[2] ———, Normal integral bases and complex conjugation, J. Reine Angew. Math. **375** (1987), 157–166.
[3] J. Cassels and A. Fröhlich (ed.), *Algebraic Number Theory*, Academic Press (1967).
[4] J. COUGNARD, Quelques extensions modérément ramifiées sans base normale, J. London Math. Soc. **31** (1985), 200–204.
[5] ———, Bases normales relatives dans certaines extensions cyclotomiques, J. Number Theory **23** (1986), 336–346.
[6] A. FRÖHLICH, Stickelberger without Gauss sums, *Algebraic Number Fields* (*Proceedings of The Durham Symposium 1975*), Academic Press (1977), 589–607.
[7] ———, *Galois Module Structure of Algebraic Integers*, Springer (1983).
[8] F. KAWAMOTO and K. KOMATSU, Normal bases and $\mathbf{Z}_p$-extensions, J. Algebra **163** (1994), 335–347.
[9] B. SODAÏGUI, Structure galoisienne relative des anneaux d'entiers, J. Number Theory **28** (1988), 189–204.

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