Journal de Théorie des Nombres
de Bordeaux **8** *(1996)*,

Relative Galois module structure of integers of abelian fields

par Nigel P. BYOTT & Günter LETTL

Abstract. Let L/K be an extension of algebraic number fields, where L is abelian over $\mathbb{Q}$. In this paper we give an explicit description of the associated order $\mathcal{A}_{L/K}$ of this extension when K is a cyclotomic field, and prove that $\mathfrak{o}_L$, the ring of integers of L, is then isomorphic to $\mathcal{A}_{L/K}$. This generalizes previous results of Leopoldt, Chan & Lim and Bley. Furthermore we show that $\mathcal{A}_{L/K}$ is the maximal order if L/K is a cyclic and totally wildly ramified extension which is linearly disjoint to $\mathbb{Q}^{(m')}/K$, where m' is the conductor of K.

1. Introduction.

Let L/K be a finite Galois extension of algebraic number fields with Galois group Γ and denote the ring of integers of any number field M by $\mathfrak{o}_M$. The associated order $\mathcal{A}_{L/K}$ of the extension L/K is given by

$$\mathcal{A}_{L/K} = \{\alpha \in K\Gamma \mid \alpha\mathfrak{o}_L \subset \mathfrak{o}_L\} ,$$

where $K\Gamma$ operates on the additive structure of L. In studying the Galois module structure of $\mathfrak{o}_L$ over K one seeks to determine the associated order $\mathcal{A}_{L/K}$ and the structure of $\mathfrak{o}_L$ as an $\mathcal{A}_{L/K}$-module. For more about this problem we refer the reader to [4], [10] and the second part of [9].

Now let us assume that L is an abelian extension of $\mathbb{Q}$ with conductor $n \in \mathbb{N}$. For any integer $t \in \mathbb{N}$ let ζ_t denote a root of unity of order t and $\mathbb{Q}^{(t)} = \mathbb{Q}(\zeta_t)$ the t-th cyclotomic field.

If $K = \mathbb{Q}$, the Galois module structure of $\mathfrak{o}_L$ was determined by Leopoldt (see [6], [7]). Quite recently, this problem was also solved for $K = \mathbb{Q}^{(m')}$ and $L = \mathbb{Q}^{(n)}$ (see [3]) as well as for $K = \mathbb{Q}^{(m')}$ and L such that $\mathbb{Q}^{(n)}/L$ is at most tamely ramified (see [1]). In all these cases $\mathfrak{o}_L \simeq \mathcal{A}_{L/K}$ holds.

Manuscrit reçu le 27 décembre 1994

We will show that this result also holds for $K = \mathbb{Q}^{(m')}$ and arbitrary L, i.e. we also cover the situation where $\mathbb{Q}^{(n)}/L$ is wildly ramified (only wild ramification at 2 is possible). In [3] and [1], the proof involves splitting the extension $\mathbb{Q}^{(n)}/\mathbb{Q}^{(m')}$ into parts whose conductors are prime powers. The result is proved for a wildly ramified extension whose conductor is a prime power, and then Leopoldt's theorem and lemma 3 below are used to obtain the general result. In contrast to this, we will look at the whole extension from the beginning. Although this looks more clumsy at the first glance, we obtain a very explicit description of $\mathcal{A}_{L/K}$ and of a generating element $T_{L/K} \in \mathfrak{o}_L$ with $\mathfrak{o}_L = \mathcal{A}_{L/K}\, T_{L/K}$, while keeping the problems arising with the prime 2 to a minimum. Our proof does not depend on Leopoldt's result. It even covers Leopoldt's theorem, which occurs as the special case $m' = 1$.

2. Notations and auxiliary results.

Let G be a finite abelian group of exponent n, K a field with $\mathrm{char}(K) \nmid n$, $\overline{K}$ its algebraic closure and $G^* = \mathrm{Hom}(G, \overline{K}^{\times})$ the dual group of G. First we will assume that K contains all n-th roots of unity, which constitute the group μ_n. For any character $\chi \in G^*$ let

$$\varepsilon_{\chi,G} = \frac{1}{|G|} \sum_{\gamma \in G} \chi(\gamma^{-1})\, \gamma \in K\,G$$

be the corresponding idempotent in the group ring $K\,G$.

Now let $H \leq G$ be a subgroup and put $H^{\perp} = \{\chi \in G^* \mid \chi|H = 1\}$. It is well known that $H^* \simeq G^*/H^{\perp}$ and $(G/H)^* \simeq H^{\perp}$, and we will frequently identify under these natural isomorphisms. Let $\pi\colon K\,G \to K[G/H]$ be the K-linear map induced by the canonical projection. The following lemma describes how the idempotents behave when we change to a subgroup or a factor group of G:

LEMMA 1.

a) *Let* $\overline{\psi} = \psi H^{\perp} \in H^* = G^*/H^{\perp}$. *Then* $\varepsilon_{\overline{\psi},H} = \sum_{\chi \in H^{\perp}} \varepsilon_{\psi\chi,G} \in K\,H$.

b) *For* $\psi \in G^* \backslash H^{\perp}$ *we have* $\pi(\varepsilon_{\psi,G}) = 0$

c) *For* $\psi \in H^\perp$ *we have* $\varepsilon_{\psi,G} = \frac{1}{|G|} \sum_{i\in I} \psi(\rho_i^{-1})\, \rho_i \sum_{\gamma \in H} \gamma$ *and* $\pi(\varepsilon_{\psi,G}) = \varepsilon_{\psi,G/H}$ *, where* $\{\rho_i \mid i \in I\} \subset G$ *is a set of representatives for* G/H *.*

Proof.

a) Let $1 \in \{\rho_i \mid i \in I\} \subset G$ be a set of representatives for G/H . Then we obtain

$$\begin{aligned}\sum_{\chi \in H^\perp} \varepsilon_{\psi\chi,G} &= \frac{1}{|G|} \sum_{\gamma \in H} \sum_{i \in I} \sum_{\chi \in H^\perp} \psi(\rho_i\gamma)^{-1} \chi(\rho_i\gamma)^{-1}\, \rho_i\gamma = \\ &= \frac{1}{|G|} \sum_{\gamma \in H} \psi(\gamma)^{-1}\gamma \sum_{i \in I} \psi(\rho_i)^{-1}\rho_i \sum_{\chi \in H^\perp} \chi(\rho_i)^{-1} = \\ &= \frac{1}{|G|} \sum_{\gamma \in H} \psi(\gamma)^{-1}\, \gamma\, \psi(1)^{-1}\, |G/H| = \varepsilon_{\overline{\psi},H}\ .\end{aligned}$$

b), c) clear.

In the next lemma we describe a special behaviour of the idempotents for cyclic Kummer extensions. Let K be given as above, $L = K(\alpha)$ with $\alpha^n = a \in K$ such that $[L : K] = n$, and denote the (cyclic) Galois group of L/K by Γ. The Kummer character $\chi_a \in \Gamma^*$ belonging to a is defined by

$$\chi_a \colon \Gamma \to \mu_n$$
$$\gamma \mapsto \frac{\gamma(\alpha)}{\alpha}$$

and $\Gamma^* = \langle \chi_a \rangle$ is generated by χ_a.

LEMMA 2. *For* $\psi \in \Gamma^*$ *we have* $\varepsilon_{\psi,\Gamma}\, \alpha = \begin{cases} \alpha & \textit{if } \psi = \chi_a \\ 0 & \textit{if } \psi \neq \chi_a \end{cases}$.

Proof. Let $\psi = \chi_a^r$ with $1 \le r \le n$. Then

$$\varepsilon_{\psi,\Gamma}\, \alpha = \frac{1}{n} \sum_{\gamma \in \Gamma} \chi_a(\gamma)^{-r} \gamma(\alpha) = \frac{\alpha^r}{n} \sum_{\gamma \in \Gamma} \gamma(\alpha^{1-r}) = \begin{cases} \alpha & \text{for } r = 1 \\ 0 & \text{for } 2 \le r \le n \end{cases} .$$

Let G and K be given as at the beginning of this section, but now we no longer assume that K contains μ_n. For any character $\chi \in G^*$, put $l = \mathrm{ord}(\chi)$, $K^{(l)} = K(\mu_l)$ and $\mathfrak{G} = \mathrm{Gal}\,(K^{(l)}/K)$. Thus the characters which are conjugate to χ over K are the χ^σ for $\sigma \in \mathfrak{G}$. Then $\varepsilon_{\chi,G} \in K^{(l)}G$ and

$$\mathcal{E}_\chi = \sum_{\sigma \in \mathfrak{G}} \varepsilon_{\chi^\sigma, G} \in KG$$

is a primitive idempotent of the group ring KG. Occasionally, we will write $\mathcal{E}_{\chi,KG}$ instead of $\mathcal{E}_\chi$ to indicate the group ring, if this is not clear from the context. Let $G_K^* \subset G^*$ be a set of representatives for the classes of characters which are conjugate over K. Then it is well known that

$$KG = \bigoplus_{\chi \in G_K^*} KG\, \mathcal{E}_\chi$$

is the decomposition of KG into simple K-algebras, where each summand is isomorphic to a field; more precisely, $KG\, \mathcal{E}_\chi \simeq K^{(\mathrm{ord}(\chi))}$.

Up to the end of this section we will now assume that K is the quotient field of a Dedekind domain $\mathfrak{o}_K$. For any field extension L/K let $\mathfrak{o}_L$ be the integral closure of $\mathfrak{o}_K$ in L. Since G is abelian, KG contains a unique maximal $\mathfrak{o}_K$-order $\mathcal{M}$, which is the integral closure of $\mathfrak{o}_K$ in KG. We have the decomposition

$$\mathcal{M} = \bigoplus_{\chi \in G_K^*} \mathcal{M}_\chi ,$$

where $\mathcal{M}_\chi$ is the maximal order of $KG\,\mathcal{E}_\chi$.

Lemma 3. *Let $\chi \in G^*$ be of order l and $d = [K^{(l)} : K]$.*

a) *Let $\gamma \in G$ with $\chi(\gamma) = \zeta$ a root of unity of order l. Then we have*

$$\mathcal{M}_\chi = \left\{ \sum_{i=0}^{d-1} a_i \gamma^i \,\mathcal{E}_\chi \;\middle|\; a_i \in K \ \text{ such that } \sum_{i=0}^{d-1} a_i \zeta^i \in \mathfrak{o}_{K^{(l)}} \right\} .$$

In particular,

$$\mathcal{M}_\chi = \mathfrak{o}_K G\,\mathcal{E}_\chi \ \text{ if and only if } \ \mathfrak{o}_{K^{(l)}} = \mathfrak{o}_K[\zeta] .$$

b) *Let K be a finite extension of $F \in \{\mathbb{Q}, \mathbb{Q}_p \mid p \in \mathbb{P}\}$ and $\mathfrak{o}_K$ its ring of integers. Then we have $\mathfrak{o}_{K^{(l)}} = \mathfrak{o}_K[\zeta]$ if and only if $\mathfrak{o}_{K^{(l)}} = \mathfrak{o}_K \underset{\mathfrak{o}_{K_l}}{\otimes} \mathfrak{o}_{F^{(l)}}$, where $K_l = K \cap F^{(l)}$. Thus $\mathcal{M} = \bigoplus_{\chi \in G_K^*} \mathfrak{o}_K G\,\mathcal{E}_\chi$ if and only if $\mathfrak{o}_{K^{(l)}} = \mathfrak{o}_K \underset{\mathfrak{o}_{K_l}}{\otimes} \mathfrak{o}_{F^{(l)}}$ holds for all $l \in \mathbb{N}$ with $l \mid n$.*

In particular, this condition is fulfilled when K is a cyclotomic field.

Remark. In the case of **b)**, where K is a local or global number field,

$$\mathfrak{o}_{K^{(l)}} = \mathfrak{o}_K \underset{\mathfrak{o}_{K_l}}{\otimes} \mathfrak{o}_{F^{(l)}}$$

is the same as saying that K and $F^{(l)}$ are arithmetically disjoint over their intersection field K_l (see [5], p. 125; in this case, (2.13) in [5] is an equivalence).

Proof. **a)** There existsa K-linear isomorphism $\varphi : KG\,\mathcal{E}_\chi \to K^{(l)}$ with $\varphi(\gamma\,\mathcal{E}_\chi) = \zeta$. Thus $\mathcal{M}_\chi = \varphi^{-1}(\mathfrak{o}_{K^{(l)}})$ is the maximal order of $KG\,\mathcal{E}_\chi$, and all claims are obvious.

b) We have $\mathfrak{o}_{F^{(l)}} = \mathfrak{o}_{K_l}[\zeta]$, which implies the first claim. The others are also easily verified.

LEMMA 4.

a) *Let* L/K *be a finite field extension and* $\mathcal{M} \subset LG$ *be the maximal* $\mathfrak{o}_L$*-order. Then* $\mathcal{M} \cap KG$ *is the maximal* $\mathfrak{o}_K$*-order of* KG *.*

b) *Let* $H \leq G$ *be a subgroup,* $\mathcal{M} \subset KG$ *be the maximal* $\mathfrak{o}_K$*-order and* $\pi : KG \to K[G/H]$ *be induced by the projection. Then* $\pi(\mathcal{M})$ *is the maximal* $\mathfrak{o}_K$*-order of* $K[G/H]$ *.*

Proof.

a) Immediate.

b) By lemma 1.b)c) either $\pi(\mathcal{E}_{\chi,KG}) = 0$ or $\pi(\mathcal{E}_{\chi,KG}) = \mathcal{E}_{\chi,K[G/H]}$. Using e.g. lemma 3.a, the claim follows.

The next two lemmas will show how the associated orders of composite fields and of subfields can be determined under certain additional assumptions. Still, K will be the quotient field of a Dedekind domain $\mathfrak{o}_K$. If L/K is a finite Galois extension we define the associated order $\mathcal{A}_{L/K}$ in the same way as in the introduction. In a more special setting, lemmas 5 and 6 can be found in [3] and [1], respectively.

Lemma 5. *For* $i \in \{1,2\}$ *let* L_i/K *be finite Galois extensions with* $\Gamma_i = \mathrm{Gal}\ (L_i/K)$ *, put* $L = L_1 L_2$ *and suppose that* $\mathfrak{o}_L = \mathfrak{o}_{L_1} \underset{\mathfrak{o}_K}{\otimes} \mathfrak{o}_{L_2}$.

a) *We have* $\mathcal{A}_{L/L_2} \simeq \mathcal{A}_{L_1/K} \underset{\mathfrak{o}_K}{\otimes} \mathfrak{o}_{L_2}$ *and* $\mathcal{A}_{L/K} \simeq \mathcal{A}_{L_1/K} \underset{\mathfrak{o}_K}{\otimes} \mathcal{A}_{L_2/K}$.

b) *If there exists some* $T_1 \in \mathfrak{o}_{L_1}$ *with* $\mathfrak{o}_{L_1} = \mathcal{A}_{L_1/K} T_1$ *, then* $\mathfrak{o}_L = \mathcal{A}_{L/L_2}(T_1 \otimes 1)$.
If there also exists $T_2 \in \mathfrak{o}_{L_2}$ *with* $\mathfrak{o}_{L_2} = \mathcal{A}_{L_2/K} T_2$ *, then* $\mathfrak{o}_L = \mathcal{A}_{L/K}\,(T_1 \otimes T_2)$.

Proof. The proofs are immediate.

Now suppose that we have finite Galois extensions L/K and L'/K with $K \subset L \subset L'$, and put $\Delta = \mathrm{Gal}\ (L'/K)$ and $\Gamma = \mathrm{Gal}\ (L/K)$. Let $\pi \colon K\Delta \to K\Gamma$ denote the K -linear map induced by the projection $\pi : \Delta \to \Gamma$.

Lemma 6. *Suppose that* L'/L *is at most tamely ramified and that* $\mathfrak{o}_{L'} = \mathcal{A}_{L'/K} T'$ *with some* $T' \in \mathfrak{o}_{L'}$ *. Then* $\mathcal{A}_{L/K} = \pi(\mathcal{A}_{L'/K})$ *and* $\mathfrak{o}_L = \mathcal{A}_{L/K} T$ *with* $T = \mathrm{tr}_{L'/L}(T')$ *, where* $\mathrm{tr}_{L'/L}$ *denotes the trace from* L' *to* L .

Proof. Since L'/L is at most tamely ramified, $\mathrm{tr}_{L'/L}(\mathfrak{o}_{L'}) = \mathfrak{o}_L$. Thus we obtain $\mathfrak{o}_L = \mathrm{tr}_{L'/L}(\mathcal{A}_{L'/K} T') = \mathcal{A}_{L'/K}(\mathrm{tr}_{L'/L} T') = \pi(\mathcal{A}_{L'/K})\,T$.

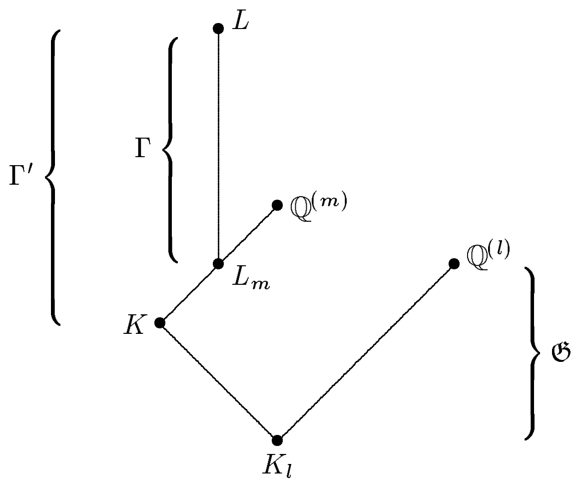
3. Statement of results.

For the rest of this paper, L will always denote an absolutely abelian number field with conductor $n \in \mathbb{N}$, so $L \subset \mathbb{Q}^{(n)}$, and K some subfield of L with conductor $m'|n$. For any integer $t \in \mathbb{N}$ let $\mathfrak{o}^{(t)} = \mathfrak{o}_{\mathbb{Q}^{(t)}}$ denote the ring of integers of $\mathbb{Q}^{(t)}$, $G^{(t)} = \mathrm{Gal}\ (\mathbb{Q}^{(t)}/\mathbb{Q})$ and $M_t = M \cap \mathbb{Q}^{(t)}$

for any number field M . We put

$$m = m' \prod_{\substack{p \in \mathbb{P} \\ p \mid n \text{ and } p \nmid m'}} p \ .$$

Note that we admit $m \equiv 2 \mod (4)$, in which case $\mathbb{Q}^{(m)}$ has conductor $\frac{m}{2}$. Our notation allows a uniform treatment for all primes including 2 ; e.g. the extension $\mathbb{Q}^{(n)}/\mathbb{Q}^{(m)}$ is always of degree $\frac{n}{m}$. Let $\Gamma = \mathrm{Gal}\ (L/L_m) \leq \mathrm{Gal}\ (L/K) = \Gamma'$.



Let $\psi \in \Gamma^*$ be a character of Γ of order l , $\mathfrak{G} = \mathrm{Gal}\ (\mathbb{Q}^{(l)}/K_l)$ and

$$\mathcal{E}_\psi = \sum_{\sigma \in \mathfrak{G}} \varepsilon_{\psi^\sigma, \Gamma} \in K_l \Gamma \subset K \Gamma$$

be the corresponding primitive idempotent of $K\Gamma$.

Γ is not a cyclic group if and only if $m \equiv 2 \mod (4)$, $8 \mid n$ and $L\mathbb{Q}^{(m)} = \mathbb{Q}^{(n)}$. In this case L_{2m} is a quadratic extension of L_m and L/L_{2m} is cyclic; so let $\omega_2 \in \Gamma^*$ denote the unique nontrivial character, which is trivial on $\mathrm{Gal}\ (L/L_{2m})$.

Now define

$$E_\psi = \begin{cases} \mathcal{E}_\psi + \mathcal{E}_{\psi\omega_2} & \text{if } \Gamma \text{ is not cyclic and both } \psi \text{ and } \psi\omega_2 \text{ have even order} \\ \mathcal{E}_\psi & \text{in all other cases} \end{cases}$$

and put

$$\mathcal{B}_{L/K} = \mathfrak{o}_K \, \Gamma' \, [\, E_\psi \mid \psi \in \overline{\Gamma^*} \,] = \bigoplus_{\psi \in \overline{\Gamma^*}} \mathfrak{o}_K \Gamma' E_\psi \quad ,$$

where $\overline{\Gamma^*} \subset \Gamma^*$ is a set of representatives for the classes into which Γ^* is divided by the definition of the pairwise orthogonal idempotents E_ψ .

Let $\mathcal{D}(m,n)$ denote the set $\{d \in \mathbb{N} \mid \; m|d \;$ and $\; d|n\}$. For $t \in \mathcal{D}(m,n)$ let $\mathcal{R}_t \subset G^{(n)}$ be a set of representatives for $\mathrm{Gal}\,(K_{\frac{t}{m}}/\mathbb{Q})$ and define

$$T_{L/K} = \sum_{t \in \mathcal{D}(m,n)} \; \sum_{\sigma \in \mathcal{R}_t} \mathrm{tr}_{\mathbb{Q}^{(t)}/L_t} \, \sigma(\zeta_t) \; .$$

Theorem. *Let L be an abelian number field containing $K = \mathbb{Q}^{(m')}$. Then, with the above notations, the associated order of $L/\mathbb{Q}^{(m')}$ is given by*

$$\mathcal{A}_{L/\mathbb{Q}^{(m')}} = \mathcal{B}_{L/\mathbb{Q}^{(m')}} = \bigoplus_{\psi \in \overline{\Gamma^*}} \mathfrak{o}^{(m')}\Gamma' E_\psi ,$$

and $T_{L/\mathbb{Q}^{(m')}}$ generates $\mathfrak{o}_L$ as a free, rank one module over $\mathcal{A}_{L/\mathbb{Q}^{(m')}}$. More explicitly, we have

$$\mathfrak{o}_L = \mathcal{B}_{L/\mathbb{Q}^{(m')}} T_{L/\mathbb{Q}^{(m')}} = \bigoplus_{t \in \mathcal{D}(m,n)} \bigoplus_{\sigma \in \mathcal{R}_t} \mathfrak{o}^{(m')}\Gamma' \operatorname{tr}_{\mathbb{Q}^{(t)}/L_t} \sigma(\zeta_t) .$$

We call an extension of numberfields N/M *totally wildly ramified* if each intermediate field different from M is wildly ramified above M.

Corollary. *Let L/K be a cyclic and totally wildly ramified extension which is linearly disjoint to the extension $\mathbb{Q}^{(m')}/K$, where m' denotes the conductor of K. Then $\mathcal{A}_{L/K}$ is the maximal order of $K\Gamma$.*

Proof of the Corollary. For $K = \mathbb{Q}^{(m')}$, we have $\mathcal{A}_{L/\mathbb{Q}^{(m')}} = \mathcal{B}_{L/\mathbb{Q}^{(m')}}$ by the theorem. If $L/\mathbb{Q}^{(m')}$ is cyclic and totally wildly ramified, $\mathcal{B}_{L/\mathbb{Q}^{(m')}} = \bigoplus_{\psi\in\overline{\Gamma^*}} \mathfrak{o}_{\mathbb{Q}^{(m')}}\Gamma\,\mathcal{E}_\psi$ is the maximal order of $\mathbb{Q}^{(m')}\Gamma$ by lemma 3.b.

In the general case, put $L' = L\mathbb{Q}^{(m')}$ and $\Delta = \mathrm{Gal}\,(L'/\mathbb{Q}^{(m')})$. Since L/K and $\mathbb{Q}^{(m')}/K$ are linearly disjoint, we have the canonical isomorphism $\pi : \mathbb{Q}^{(m')}\Delta \to \mathbb{Q}^{(m')}\Gamma$. Since $\mathcal{A}_{L'/\mathbb{Q}^{(m')}}$ is the maximal order of $\mathbb{Q}^{(m')}\Delta$, $\pi(\mathcal{A}_{L'/\mathbb{Q}^{(m')}}) \cap K\Gamma$ is the maximal order of $K\Gamma$ by lemma 4.a. On the other hand $\pi(\mathcal{A}_{L'/\mathbb{Q}^{(m')}}) \cap K\Gamma \subset \mathcal{A}_{L/K}$, which concludes the proof.

Remarks.

1. The assumption of the linear disjointness is crucial in the above corollary. For $k \geq 3$, let $L = \mathbb{Q}^{(2^k)}$ and $K = \mathbb{Q}(\zeta_{2^k} \pm \zeta_{2^k}^{-1})$. Then L/K is cyclic of degree 2 and totally wildly ramified, but $\mathcal{A}_{L/K}$ is not the maximal order (see [8]).
2. In the situation occurring in the corollary, we only know the associated order, but we do not know the structure of $\mathfrak{o}_L$ as a module over $\mathcal{A}_{L/K}$ if $K \subsetneq \mathbb{Q}^{(m')}$.

3. In the general case, one cannot expect that $\mathfrak{o}_L$ is free over $\mathcal{A}_{L/K}$ (e.g. see [2]).

4. Proof of the Theorem.

Throughout this section, we have $K = \mathbb{Q}^{(m')}$. Therefore, for any $t \in \mathcal{D}(m,n)$ we have $K_{\frac{t}{m}} = \mathbb{Q}^{(t_0)}$ with $t_0 = (\frac{t}{m}, m')$ and $\mathcal{R}_t$ is a set of representatives for $G^{(t_0)}$. First we will show that for $\mathbb{Q}^{(n)}/\mathbb{Q}^{(m')}$ the roots of unity in the theorem indeed generate $\mathfrak{o}^{(n)}$ as module over $\mathfrak{o}^{(m')}\Gamma'$. We use the same notations as introduced above.

Lemma 7.

$$\mathfrak{o}^{(n)} = \sum_{t \in \mathcal{D}(m,n)} \sum_{\sigma \in \mathcal{R}_t} \mathfrak{o}^{(m')}\Gamma' \, \sigma(\zeta_t) \ .$$

Proof. Obviously, $\mathfrak{o}^{(n)} = \sum_{t' \in \mathcal{D}(m',n)} \sum_{\tau \in G^{(t')}} \mathfrak{o}^{(m')} \, \tau(\zeta_{t'})$. For $t' \in \mathcal{D}(m',n)$ put

$$t = \ t' \prod_{\substack{p \in \mathbb{P} \\ p \mid n \text{ and } p \nmid t'}} p \ \in \mathcal{D}(m,n) \ .$$

Since $\mathbb{Q}^{(t)}/\mathbb{Q}^{(t')}$ is only tamely ramified, $\tau(\zeta_{t'})$ can be written as $\pm \operatorname{tr}_{\mathbb{Q}^{(t)}/\mathbb{Q}^{(t')}} \zeta_t$ for a suitably chosen root of unity of order t (see e.g. lemma 3 in [7]). Thus we have $\mathfrak{o}^{(n)} = \sum_{t \in \mathcal{D}(m,n)} \sum_{\tau \in G^{(t)}} \mathfrak{o}^{(m')} \, \tau(\zeta_t)$. To prove the lemma, we will show that for any $\tau \in G^{(t)}$ there exist some $\sigma \in \mathcal{R}_t$, $\gamma \in \Gamma'$ and $k \in \mathbb{Z}$ such that

$$\tau(\zeta_t) = \zeta_{m'}^k \ \gamma\sigma(\zeta_t) \ , \quad \text{where} \ \ \zeta_{m'} = \zeta_t^{\frac{t}{m'}} \in \mathfrak{o}^{(m')} \ .$$

For $l \in \mathbb{N}$ let σ_l denote the Galois automorphism with $\sigma_l(\zeta) = \zeta^l$ for all roots of unity ζ of order prime to l . Now choose some $j \in \mathbb{Z}$ with $(j,t) = 1$ and $\tau = \sigma_j$. Furthermore, Γ' consists of the automorphisms $\sigma_{1+am'}$ for $a \in \mathbb{Z}$. First we can find some $\sigma = \sigma_{j_0} \in \mathcal{R}_t$ with $j_0 \equiv j \mod (t_0)$. Now we have to look for some $a, k \in \mathbb{Z}$ such that $j \equiv k\dfrac{t}{m'} + j_0\,(1 + am') \mod (t)$. This reduces to

$$\frac{j - j_0}{t_0} \equiv k\frac{t}{m' t_0} + a j_0 \frac{m'}{t_0} \quad \mod \left(\frac{t}{t_0}\right) \ .$$

Since $\frac{m}{m'}$ has only prime factors, which do not divide m' , we obtain $(\frac{t}{m'}, m') = t_0$ and $(\frac{t}{m' t_0}, \frac{m'}{t_0}) = 1$. Since $(j_0, n) = 1$, we obviously can find $a, k \in \mathbb{Z}$ satisfying the above congruence. This concludes the proof of lemma 7.

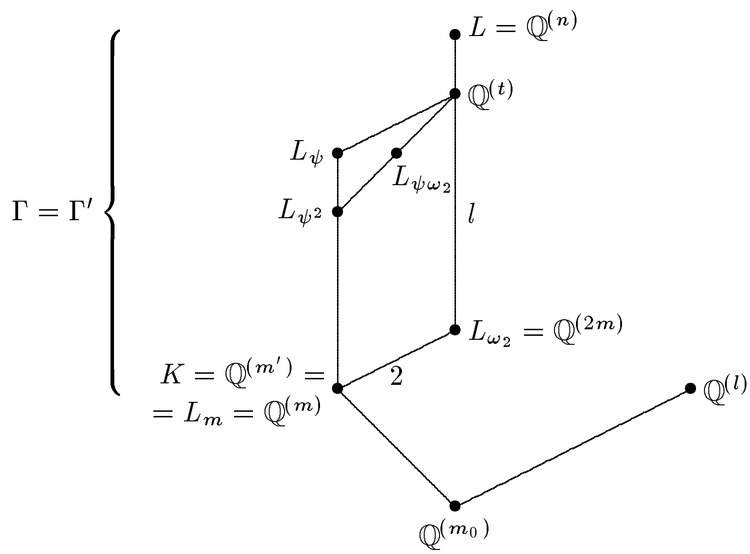
I. Proof for the totally wildly ramified cyclotomic case ($\mathbb{Q}^{(n)}/\mathbb{Q}^{(m)}$).

We will first prove the theorem for the totally wildly ramified case; thus we have $m = 2m'$ if m' is odd and n is even, and $m = m'$ otherwise.

For $\chi \in \Gamma^*$, let L_χ be the subfield of $\mathbb{Q}^{(n)}$ belonging to χ , i.e. the field fixed by $\{\gamma \in \Gamma \mid \chi(\gamma) = 1\}$.

Now let $\psi \in \Gamma^*$ be of order l , $t \in \mathcal{D}(m,n)$ be minimal with $L_\psi \subset \mathbb{Q}^{(t)}$, and put $m_0 = (m,l)$.

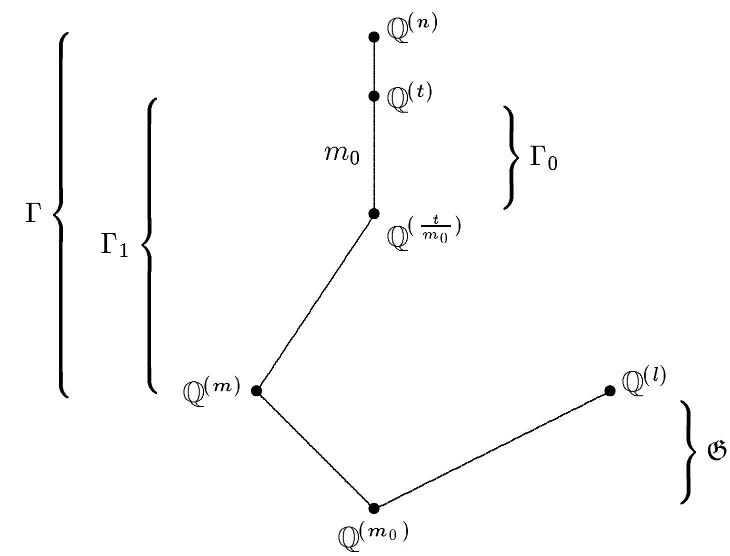
If $m \equiv 2 \mod (4)$ and $8|t$ then $t = 2lm$, $\mathbb{Q}^{(t)}/K$ is not cyclic and L_ψ is a quadratic subfield of $\mathbb{Q}^{(t)}$. In this case ψ and $\psi\omega_2$ both have even order and both characters induce the same character, say ψ' , of order l for the cyclic extension $\mathbb{Q}^{(t)}/\mathbb{Q}^{(2m)}$ of degree l . The following diagram illustrates this situation:



In all other cases $t = lm$ and $L_\psi = \mathbb{Q}^{(t)}$ is cyclic over $\mathbb{Q}^{(m)}$.

The conductor of L_ψ equals t except for the case that $m \equiv 2 \mod (4)$ and l is odd. In this latter case it equals $\frac{t}{2}$, but nevertheless $\mathbb{Q}^{(t)} = \mathbb{Q}^{(\frac{t}{2})}$.

Now consider the cyclic Kummer extension $\mathbb{Q}^{(t)}/\mathbb{Q}^{(\frac{t}{m_0})}$ and denote its Galois group by Γ_0 .



Since $\mathbb{Q}^{(m_0)}$ is fixed by $\mathfrak{G}$, for any $\sigma \in \mathfrak{G}$ ψ and ψ^σ coincide when restricted to Γ_0 . With these notations we will prove the following

LEMMA 8. *Let* $\zeta \in \mathbb{Q}^{(t)}$ *be a root of unity of order* t . *Then*

$$E_\psi \, \zeta = \begin{cases} \zeta & \textit{if } \ \psi(\gamma) = \frac{\gamma(\zeta)}{\zeta} \ \textit{ for all } \ \gamma \in \Gamma_0 \\ 0 & \textit{otherwise} \end{cases} .$$

Proof. Since any prime divisor of l also divides m_0 , $\mathbb{Q}^{(l)}/\mathbb{Q}^{(m_0)}$ is of degree $\frac{l}{m_0}$ and has no tame subextension. Therefore for any root of unity $\xi \in \mathbb{Q}^{(l)}$,

$$\sum_{\sigma \in \mathfrak{G}} \xi^\sigma = \operatorname{tr}_{\mathbb{Q}^{(l)}/\mathbb{Q}^{(m_0)}} \xi = \begin{cases} \frac{l}{m_0}\xi & \text{if } \ \xi \in \mathbb{Q}^{(m_0)} \\ \quad 0 & \text{otherwise} \end{cases} . \tag{1}$$

Putting $\Gamma_1 = \mathrm{Gal}\,(\mathbb{Q}^{(t)}/\mathbb{Q}^{(m)})$ we obtain

$$\mathcal{E}_\psi \, \zeta = \sum_{\sigma \in \mathfrak{G}} \frac{m}{n} \sum_{\gamma \in \Gamma} \psi^\sigma(\gamma^{-1})\, \gamma(\zeta) = \sum_{\sigma \in \mathfrak{G}} \frac{m}{t} \sum_{\gamma \in \Gamma_1} \psi^\sigma(\gamma^{-1})\, \gamma(\zeta) = \frac{m}{t} \sum_{\gamma \in \Gamma_1} \sum_{\sigma \in \mathfrak{G}} \psi^\sigma(\gamma^{-1})\, \gamma(\zeta) \, .$$

If $t = lm$, Γ_1 is cyclic, and $\sum_{\sigma \in \mathfrak{G}} \psi^\sigma(\gamma^{-1})$ vanishes for all $\gamma \notin \Gamma_0$ by (1). In this case we can continue our calculation as follows:

$E_\psi\,\zeta \;=\; \mathcal{E}_\psi\,\zeta \;=\; \frac{m}{t}\sum_{\gamma\in\Gamma_0}\frac{l}{m_0}\psi(\gamma^{-1})\,\gamma(\zeta) \;=\; \frac{1}{m_0}\sum_{\gamma\in\Gamma_0}\psi(\gamma^{-1})\,\gamma(\zeta)$, and the assertion follows with lemma 2.

If $t = 2lm$, ψ and $\psi\omega_2$ induce the same character ψ' on Gal $(\mathbb{Q}^{(t)}/\mathbb{Q}^{(2m)})$ and differ by the factor -1 for the nontrivial automorphism of Gal $(\mathbb{Q}^{(t)}/L_\psi)$. In this case we have

$$E_\psi\,\zeta = (\mathcal{E}_\psi + \mathcal{E}_{\psi\omega_2})\,\zeta = \frac{m}{t}\sum_{\gamma\in\Gamma_1}\sum_{\sigma\in\mathfrak{G}}(\psi(\gamma^{-1}) + \psi\omega_2(\gamma^{-1}))^\sigma\,\gamma(\zeta) = \frac{m}{t}\sum_{\gamma\in\Gamma_0}2\frac{l}{m_0}\psi'(\gamma^{-1})\,\gamma(\zeta)$$

$= \frac{1}{m_0}\sum_{\gamma\in\Gamma_0}\psi'(\gamma^{-1})\,\gamma(\zeta)$, and again lemma 2 establishes our assertion.

After these preparations we will start the proof of the theorem. We will show that for any $\psi \in \Gamma^*$ there exist uniquely determined $t \in \mathcal{D}(m,n)$ and $\sigma \in \mathcal{R}_t$ with

$$E_\psi\,T_{\mathbb{Q}^{(n)}/\mathbb{Q}^{(m)}} = \sigma(\zeta_t)\ ,$$

and that the correspondence $E_\psi \mapsto (t,\sigma)$ is bijective. Using lemma 7, all claims of the theorem follow immediately from this.

For any $k \in \mathbb{N}$ let $q(k) \in \mathbb{N}$ denotes the powerful part of k , which we define by

$$k = q(k)\prod_{\substack{p\in\mathbb{P}\\ p\mid k \text{ and } p^2\nmid k}} p\ .$$

For any character $\chi \in G^{(n)^*}$ of conductor f and any $d \in \mathbb{N}$, lemma 2 in [7] yields

$$\varepsilon_{\chi,G^{(n)}}\zeta_d \neq 0 \iff f \mid d \text{ and } q(f) = q(d)\ .$$

Now let $\psi \in \Gamma^*$ be of order l and put $t = lm$ or $t = 2lm$, as above. Let $f \in \{t, \frac{t}{2}\}$ be the conductor of L_ψ . By lemma 1.a, $\varepsilon_{\psi,\Gamma} = \sum_{\chi\in\psi G^{(m')^*}}\varepsilon_{\chi,G^{(n)}}$, and one can easily verify that if the conductor of $\chi \in \psi G^{(m')^*}$ is divisible by m' then this conductor must equal f . For $d \in \mathcal{D}(m,n)$ we conclude that $E_\psi\,\zeta_d \neq 0$ can only hold if $d = t$, and therefore

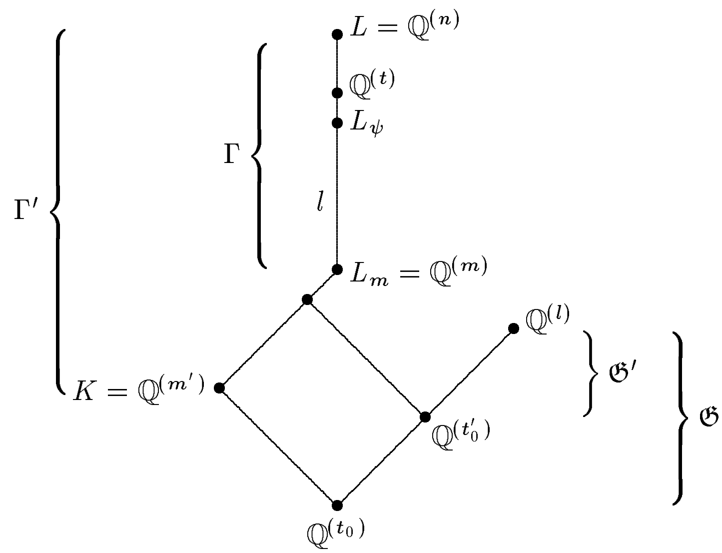
$$E_\psi\,T_{\mathbb{Q}^{(n)}/\mathbb{Q}^{(m)}} = E_\psi\sum_{\sigma\in\mathcal{R}_t}\sigma(\zeta_t)\ .$$

We have $\mathbb{Q}^{(t_0)} = \mathbb{Q}^{(m_0)}$, where $t_0 = (\frac{t}{m}, m')$ and $m_0 = (l, m')$ as above. Now we can see that there is exactly one $\sigma \in \mathcal{R}_t$ with $\psi(\gamma) = \frac{\gamma(\sigma(\zeta_t))}{\sigma(\zeta_t)}$ for all $\gamma \in \Gamma_0 = \mathrm{Gal}\ (\mathbb{Q}^{(t)}/\mathbb{Q}^{(\frac{t}{m_0})})$; so by lemma 8, $E_\psi\,T_{\mathbb{Q}^{(n)}/\mathbb{Q}^{(m)}} = \sigma(\zeta_t)$.

On the other hand, any $\sigma \in \mathcal{R}_t$ defines by the above formula a character of Γ_0 of order m_0 , from which we can derive that the correspondence $E_\psi \mapsto (t, \sigma)$ is bijective.

II. Proof for the cyclotomic case ($\mathbb{Q}^{(n)}/\mathbb{Q}^{(m')}$).

Let again $\psi \in \Gamma^*$ be of order l and put $t = lm$ or $t = 2lm$, as above. With $t_0 = (\frac{t}{m}, m') = (l, m')$ and $t_0' = (\frac{t}{m}, m)$ we now have the following situation:



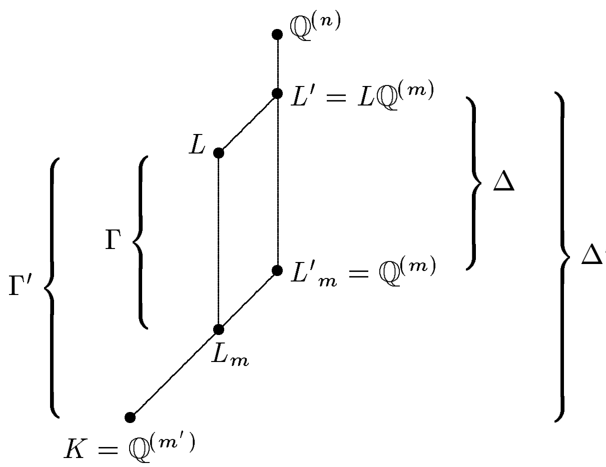
Let $\mathcal{R}'$ be a set of representatives for $\mathfrak{G}/\mathfrak{G}'$ and $\mathcal{R}_t$ a set of representatives for $G^{(t_0)}$. From now on, we will use a second subscript to indicate the group ring with respect to which the idempotents are constructed. The same arguments as in the proof of the wild case show that there exist uniquely determined $\rho \in \mathcal{R}'$ and $\sigma \in \mathcal{R}_t$ such that

$$E_{\psi, K\Gamma}\, T_{L/K} = \sum_{\delta \in \mathcal{R}'} E_{\psi^\delta, \mathbb{Q}^{(m)}\Gamma} \sum_{\tau \in \mathcal{R}_t} \tau(\zeta_t) = E_{\psi^\rho, \mathbb{Q}^{(m)}\Gamma}\, \sigma(\zeta_t) = \sigma(\zeta_t) \ ,$$

and that the correspondence $E_{\psi, K\Gamma} \mapsto (t, \sigma)$ is bijective. Using lemma 7 again, all claims of the theorem follow.

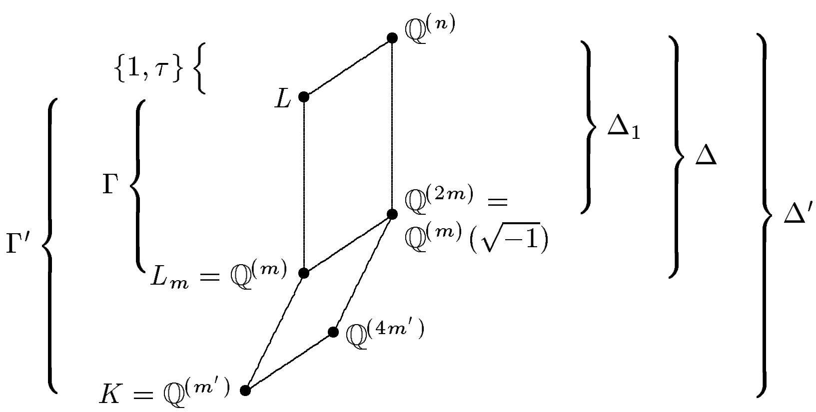
III. Proof for the general case ($L/\mathbb{Q}^{(m')}$).

Putting $L' = L\mathbb{Q}^{(m)}$ we have $[\mathbb{Q}^{(n)} : L'] \leq 2$. We denote the Galois groups as indicated in the following diagram:



Let us suppose that the theorem holds already for the extension L'/K . Since L'/L is at most tamely ramified, we will apply lemma 6. One easily checks that $\mathrm{tr}_{L'/L}(T_{L'/K}) = T_{L/K}$. The projection $\pi : \mathbb{Q}^{(m')}\Delta' \to \mathbb{Q}^{(m')}\Gamma'$ induces an isomorphism $\pi : \Delta \to \Gamma$ with dual isomorphism $\pi^* : \Gamma^* \to \Delta^*$. Since for all $\psi \in \Gamma^*$ we have $E_{\psi,K\Gamma} = \pi(E_{\pi^*(\psi),K\Delta})$, this shows $\pi(\mathcal{B}_{L'/K}) = \mathcal{B}_{L/K}$.

Thus it only remains to prove the theorem for the case where L is a quadratic subfield of $\mathbb{Q}^{(n)}$ with conductor n and $\mathbb{Q}^{(m)} \subset L$, so $m \equiv 2 \mod (4)$ and $8|n$. The following diagram shows this situation and the notations we will use.



Let $\pi : \mathbb{Q}^{(m')}\Delta' \to \mathbb{Q}^{(m')}\Gamma'$ denote the projection, put $\Delta_1 = \mathrm{Gal}\,(\mathbb{Q}^{(n)}/\mathbb{Q}^{(2m)})$ and identify Γ^* with Δ_1^* under π^*. Let $\omega_2 \in \Delta^*$ be the quadratic character belonging to $\mathbb{Q}^{(2m)}/\mathbb{Q}^{(m)}$, thus $\omega_2(\tau) = -1$, $\omega_2(\Delta_1) = 1$ and $\Delta^* = \Delta_1^* \times \{1, \omega_2\} = \Gamma^* \,\dot\cup\, \omega_2\Gamma^*$. Using lemma 1.b) c) we have for any $\psi \in \Delta^*$

$$\pi(\mathcal{E}_{\psi,K\Delta}) = \begin{cases} \mathcal{E}_{\psi,K\Gamma} & \text{if } \psi \in \Delta_1^* \\ 0 & \text{if } \psi \in \omega_2\Delta_1^* \end{cases}$$

from which we deduce that $\pi(\mathcal{B}_{\mathbb{Q}^{(n)}/K}) = \mathcal{B}_{L/K}$.

To finish our proof, we have to show that $\mathfrak{o}_L \subset \mathcal{B}_{L/K}T_{L/K}$. So let $y \in \mathfrak{o}_L$, which is equivalent to $y \in \mathfrak{o}^{(n)}$ and $\tau(y) = y$. Our theorem holds already for $\mathbb{Q}^{(n)}/\mathbb{Q}^{(m')}$, therefore there exists some

$$\alpha = \sum_{\psi \in \overline{\Delta^*}} a_\psi\, E_{\psi,K\Delta} \;\in\; \mathcal{B}_{\mathbb{Q}^{(n)}/K} = \bigoplus_{\psi \in \overline{\Delta^*}} \mathfrak{o}^{(m')}\Delta'\, E_{\psi,K\Delta}$$

with $a_\psi \in \mathfrak{o}^{(m')}\Delta'$ such that $y = \alpha\, T_{\mathbb{Q}^{(n)}/K}$. Since α is uniquely determined, it follows that $\tau a_\psi E_{\psi,K\Delta} = a_\psi E_{\psi,K\Delta}$ for all $\psi \in \overline{\Delta^*}$. On the other hand we have

$$\tau\, \mathcal{E}_{\psi,K\Delta} = \psi(\tau)\, \mathcal{E}_{\psi,K\Delta} = \begin{cases} \mathcal{E}_{\psi,K\Delta} & \text{if } \psi \in \Gamma^* \\ -\mathcal{E}_{\psi,K\Delta} & \text{if } \psi \in \omega_2\Gamma^* \end{cases} .$$

For $\psi \in \Gamma^*$ with odd order l, we put $t = lm$ and have $\mathbb{Q}^{(t)} = L_t$. Then we obtain

$$\begin{aligned} a_\psi E_{\psi,K\Delta}\, T_{\mathbb{Q}^{(n)}/K} &= a_\psi \mathcal{E}_{\psi,K\Delta} \sum_{\sigma \in \mathcal{R}_t} \sigma(\zeta_t) = \\ &= \pi(a_\psi)\mathcal{E}_{\psi,K\Gamma} \sum_{\sigma \in \mathcal{R}_t} \mathrm{tr}_{\mathbb{Q}^{(t)}/L_t}\, \sigma(\zeta_t) = \pi(a_\psi) E_{\psi,K\Gamma}\, T_{L/K} \end{aligned} \tag{2}$$

and $a_{\psi\omega_2} E_{\psi\omega_2,K\Delta} = 0$.

Now let $\psi \in \Gamma^*$ with even order l and put $t = 2lm$. Then $\psi\omega_2 \notin \Gamma^*$ also has even order. Let $\Delta_1' = \mathrm{Gal}\,(\mathbb{Q}^{(n)}/\mathbb{Q}^{(4m')})$. Since ψ and $\psi\omega_2$ coincide on Δ_1 and differ by the factor -1 on $\tau\Delta_1$, we see that $E_{\psi,K\Delta} \in \mathfrak{o}^{(m')}\Delta_1 \subset \mathfrak{o}^{(m')}\Delta_1'$. Decomposing $a_\psi = a' + (1+\tau)a''$ with $a', a'' \in \mathfrak{o}^{(m')}\Delta_1'$ and inserting this into $\tau a_\psi E_{\psi,K\Delta} = a_\psi E_{\psi,K\Delta}$, we can deduce that $a' E_{\psi,K\Delta} = 0$ and $a_\psi E_{\psi,K\Delta} = (1+\tau)a''\mathcal{E}_{\psi,K\Delta}$. Thus we obtain

$$a_\psi E_{\psi,K\Delta}\, T_{\mathbb{Q}^{(n)}/K} = a''\mathcal{E}_{\psi,K\Delta}(1+\tau) \sum_{\sigma\in\mathcal{R}_t} \sigma(\zeta_t) =$$

$$= a''\pi(\mathcal{E}_{\psi,K\Delta}) \sum_{\sigma\in\mathcal{R}_t} \mathrm{tr}_{\mathbb{Q}^{(t)}/L_t}\sigma(\zeta_t) = a'' E_{\psi,K\Gamma}\, T_{L/K} \ .$$

Combining this with (2) shows that

$$y \in \bigoplus_{\psi\in\overline{\Gamma^*}} \mathfrak{o}^{(m')}\Gamma'\, E_{\psi,K\Gamma}\, T_{L/K} = \mathcal{B}_{L/K}\, T_{L/K} \ ,$$

which finishes the proof.

References

[1] W. Bley, *A Leopoldt–type result for rings of integers of cyclotomic extensions*, Canad. Math. Bull. **38** (1995), 141 – 148.

[2] J. Brinkhuis, *Normal integral bases and complex conjugation*, J reine angew. Math. **375/376** (1987), 157 – 166.

[3] S.-P. Chan & C.-H. Lim, *Relative Galois module structure of rings of integers of cyclotomic fields*, J. reine angew. Math. **434** (1993), 205 – 220.

[4] A. Fröhlich, *Galois module structure of algebraic integers*, Erg. d. Math. 3, vol. 1, Springer, 1983.

[5] A. Fröhlich & M.J. Taylor, *Algebraic number theory*, Camb. Studies Adv. Math. vol. 27, Cambridge University Press, 1991.

[6] H.-W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. reine angew. Math. **201** (1959), 119 – 149.

[7] G. Lettl, *The ring of integers of an abelian number field*, J. reine angew. Math. **404** (1990), 162 – 170.

[8] G. Lettl, *Note on the Galois module structure of quadratic extensions*, Coll. Math. **67** (1994), 15 – 19.

[9] K.W. Roggenkamp & M.J. Taylor, *Group rings and class groups*, DMV-Seminar Bd. 18, Birkhäuser, 1992.

[10] M.J. Taylor, *Relative Galois module structure of rings of integers*, Orders and their applications (Proceedings of Oberwolfach 1984) (I. Reiner & K.W. Roggenkamp, eds.), Lect. Notes 1142, Springer, 1985, pp. 289–306.

Nigel P. Byott
Department of Mathematics
University of Exeter

North Park Road
Exeter, EX4 4QE
United Kingdom
e-mail: NPByott@uk.ac.exeter.maths

Günter Lettl
Institut für Mathematik
Karl-Franzens-Universität
Heinrichstraße 36
A-8010 Graz, Österreich
e-mail: guenter.lettl@kfunigraz.ac.at