ACTA ARITHMETICA
LXXXV.3 (1998)

Relative Galois module structure of integers of local abelian fields

by

Günter Lettl (Graz)

1. Introduction. Let K denote the quotient field of some Dedekind ring $\mathfrak{o}_K$ and N/K a finite Galois extension with Galois group Γ. Considering the action of the group algebra $K\Gamma$ on the additive structure of N, the Normal Basis Theorem tells us that $N \simeq K\Gamma$, i.e. there exist $t \in N$ with $N = K\Gamma t = \bigoplus_{\gamma\in\Gamma} K\gamma(t)$.

A more delicate problem is the study of the Galois module structure of $\mathfrak{o}_N$, the integral closure of $\mathfrak{o}_K$ in N. $\mathfrak{o}_N$ is a module over the so-called *associated order*

$$\mathcal{A}_{N/K} := \{\alpha \in K\Gamma \mid \alpha\mathfrak{o}_N \subset \mathfrak{o}_N\}, \tag{1}$$

and one is interested in an explicit description of $\mathcal{A}_{N/K}$ and the structure of $\mathfrak{o}_N$ over it, especially whether or not $\mathfrak{o}_N \simeq \mathcal{A}_{N/K}$. For more references and details we refer the reader to [11], the second part of [16] or [8].

If N/K is at most tamely ramified, a theorem of Noether shows that $\mathcal{A}_{N/K} = \mathfrak{o}_K\Gamma$, and if furthermore K is a local field (i.e. complete with respect to a discrete valuation and with finite residue class field) and $\mathfrak{o}_K$ its valuation ring then $\mathfrak{o}_N \simeq \mathcal{A}_{N/K}$.

If N is a finite abelian extension of $\mathbb{Q}$ and $\mathfrak{o}_N$ its ring of algebraic integers, then $\mathfrak{o}_N \simeq \mathcal{A}_{N/K}$ holds in the cases $K = \mathbb{Q}$ ([12], [13]) and $K = \mathbb{Q}(\zeta)$ with ζ a root of unity ([6], [2], [5]), but there are examples for K, even with N/K unramified, where $\mathfrak{o}_N \not\simeq \mathcal{A}_{N/K}$ (see [3]). Up to now it has not even been known whether for abelian fields N, $\mathfrak{o}_N$ is always a locally free $\mathcal{A}_{N/K}$-module, i.e. whether $\mathfrak{o}_{N,\mathfrak{p}} \simeq \mathcal{A}_{N/K,\mathfrak{p}}$ for each prime $\mathfrak{p} \in \operatorname{spec}(\mathfrak{o}_K)$. If $\mathcal{A}_{N/K}$

1991 *Mathematics Subject Classification*: 11R33, 11S20.

This paper was written while visiting the University of Exeter (GB), financially supported by the British Council (grant no. VIE/891/7) and the University of Exeter. Many thanks to the department of mathematics for their kind hospitality and to N. P. Byott for useful conversations.

is a Hopf order and Γ is abelian, it was proved in [7] that $\mathfrak{o}_N$ is locally free over $\mathcal{A}_{N/K}$. Unfortunately, $\mathcal{A}_{N/K}$ is not a Hopf order in general. The present paper gives an affirmative answer to this question for absolutely abelian number fields.

THEOREM 1. *Let* $\mathbb{Q}_p \subset K \subset N$ *be finite field extensions with* $N/\mathbb{Q}_p$ *abelian. Then*

$$\mathfrak{o}_N \simeq \mathcal{A}_{N/K}.$$

Let N_0 *be the inertia field of* N/K *and put* $\Gamma_0 = \mathrm{Gal}(N/N_0) \le \Gamma$. *If* $p \ge 3$ *we have, more explicitly,*

$$\mathfrak{o}_N \simeq \mathcal{A}_{N/K} \simeq \mathfrak{o}_K\Gamma \underset{\mathfrak{o}_K\Gamma_0}{\otimes} \mathcal{M}_0,$$

where $\mathcal{M}_0 \subset K\Gamma_0$ *is the maximal* $\mathfrak{o}_K$*-order of* $K\Gamma_0$.

Following the proof of this theorem, also for $p = 2$ an explicit description of $\mathcal{A}_{N/K}$ can be obtained, starting with the result of Proposition 3(a). In the same way, one can obtain an explicit generator $T_{N/K} \in \mathfrak{o}_N$ with $\mathcal{A}_{N/K}T_{N/K} = \mathfrak{o}_N$, as long as Proposition 1(b) is not needed for "going down".

If N is abelian only over K, but not over $\mathbb{Q}_p$, $\mathfrak{o}_N \simeq \mathcal{A}_{N/K}$ does not hold in general (see Corollary 1 of [1] or Theorem 5.1 of [4]).

From Theorem 1 we immediately deduce the following

COROLLARY. *If* $\mathbb{Q} \subset K \subset N$ *are algebraic number fields with* $N/\mathbb{Q}$ *finite and abelian, then* $\mathfrak{o}_N$ *is locally free over* $\mathcal{A}_{N/K}$.

2. Galois module structure for abelian extensions of local fields. Some results in Section 2 of [5] describe how the Galois module structures of different field extensions are related in some special cases. For local fields we will obtain stronger results. Throughout this section, K will be a local field and N/K a finite abelian extension with Galois group Γ.

PROPOSITION 1. *Let* $\overline{N}/K$ *be a finite abelian extension with* $\overline{N} = N\overline{K}$, *where* N/K *is totally ramified and* $\overline{K}/K$ *is unramified. Put* $\Gamma = \mathrm{Gal}(\overline{N}/\overline{K}) = \mathrm{Gal}(N/K)$ *and* $\Delta = \mathrm{Gal}(\overline{N}/N) = \mathrm{Gal}(\overline{K}/K)$. *Then we have*

(a) $\mathcal{A}_{\overline{N}/\overline{K}} = \mathcal{A}_{N/K} \underset{\mathfrak{o}_K}{\otimes} \mathfrak{o}_{\overline{K}}$ *and* $\mathcal{A}_{N/K} = \mathcal{A}_{\overline{N}/\overline{K}} \cap K\Gamma$.

(b) $\mathfrak{o}_N \simeq \mathcal{A}_{N/K}$ *as* $\mathcal{A}_{N/K}$*-modules if and only if* $\mathfrak{o}_{\overline{N}} \simeq \mathcal{A}_{\overline{N}/\overline{K}}$ *as* $\mathcal{A}_{\overline{N}/\overline{K}}$*-modules. If this holds and* $T \in \mathfrak{o}_N$ *with* $\mathfrak{o}_N = \mathcal{A}_{N/K}T$, *then one also has* $\mathfrak{o}_{\overline{N}} = \mathcal{A}_{\overline{N}/\overline{K}}T$.

Note that Proposition 1(a) also holds for global fields if we only assume that N and $\overline{K}$ are arithmetically disjoint over K.

P r o o f (of Proposition 1). Since N and $\overline{K}$ are arithmetically disjoint over K (i.e. $\mathfrak{o}_{\overline{N}} = \mathfrak{o}_N \underset{\mathfrak{o}_K}{\otimes} \mathfrak{o}_{\overline{K}}$), Lemma 5 of [5] applies, showing some parts of the above statements.

(a) From definition (1) we immediately obtain $\mathcal{A}_{\overline{N}/\overline{K}} \cap K\Gamma \subset \mathcal{A}_{N/K}$. On the other hand, we have $\mathcal{A}_{N/K} \subset \mathcal{A}_{N/K} \underset{\mathfrak{o}_K}{\otimes} \mathfrak{o}_{\overline{K}} = \mathcal{A}_{\overline{N}/\overline{K}}$, thus proving $\mathcal{A}_{N/K} = \mathcal{A}_{\overline{N}/\overline{K}} \cap K\Gamma$.

(b) This is a specialization of Exercise 6.3 on p. 139 of [9]. Suppose that $\mathfrak{o}_{\overline{N}} \simeq \mathcal{A}_{\overline{N}/\overline{K}}$, i.e. $\mathfrak{o}_N \underset{\mathfrak{o}_K}{\otimes} \mathfrak{o}_{\overline{K}} \simeq \mathcal{A}_{N/K} \underset{\mathfrak{o}_K}{\otimes} \mathfrak{o}_{\overline{K}}$. Considering this as an isomorphism of $\mathcal{A}_{N/K}$-modules and using the fact that $\mathfrak{o}_{\overline{K}}$ is free over $\mathfrak{o}_K$ of rank $d = |\Delta|$, we obtain $\mathfrak{o}_N^{(d)} \simeq \mathcal{A}_{N/K}^{(d)}$ as $\mathcal{A}_{N/K}$-modules. Using now the theorem of Krull–Schmidt–Azumaya yields $\mathfrak{o}_N \simeq \mathcal{A}_{N/K}$.

The following lemma together with Lemma 6 of [5] enables us to obtain the Galois module structure for any abelian extension of a local field K as soon as we know this structure for all totally ramified, abelian extensions of K.

LEMMA 1. *Let $\overline{K}/K$ be the unramified extension of K with $[\overline{K} : K] = [N : K]$. Then there exists a totally ramified abelian extension N'/K such that for $\overline{N} = N'\overline{K}$ we have*: *$\overline{N}/K$ is abelian*, *$N \subset \overline{N}$ and $\overline{N}/N$ is unramified.*

If there exists some intermediate field $K \subset K' \subset N$ such that K'/K is totally ramified, it suffices to take for $\overline{K}$ the unramified extension of K of degree $[\overline{K} : K] = [N : K']$.

Lemma 1 can also be proved by using class field theory and analysing the norm groups, but we offer a more elementary proof.

P r o o f (of Lemma 1.) We put $\overline{N} = N\overline{K}$ and will show that this field has all the required properties. Since both N and $\overline{K}$ are abelian over K, so is $\overline{N}/K$. Obviously, $\overline{N}/N$ is unramified. It only remains to show the existence of a field N' as stated in the lemma. Consider the exact sequence

$$1 \to \mathrm{Gal}(\overline{N}/\overline{K}) \hookrightarrow \mathrm{Gal}(\overline{N}/K) \xrightarrow{\pi} \mathrm{Gal}(\overline{K}/K) \to 1.$$

Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$ be a generator of this cyclic group and take any $\tau \in \mathrm{Gal}(\overline{N}/K)$ with $\pi(\tau) = \sigma$. Since τ^d, where $d = [\overline{K} : K] = [N : K]$, is the identity on both N and $\overline{K}$, we have $\tau^d = \mathrm{id}_{\overline{N}}$. Therefore $\varphi : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(\overline{N}/K)$, defined by $\varphi(\sigma) = \tau$, is a splitting homomorphism for the above sequence. Thus we have $\mathrm{Gal}(\overline{N}/K) = \mathrm{Gal}(\overline{N}/\overline{K}) \oplus G'$ with some subgroup $G' \le \mathrm{Gal}(\overline{N}/K)$. If we take $N' = \overline{N}^{G'}$, the field fixed by G', the remaining claims immediately follow.

Since it will be of general interest, we also include the following result, which can be used to deduce Theorem 1 for $p \geq 3$ from Proposition 3 or from the global result of [2] or [5]. Alas, it does not apply to non-maximal orders and gives no information about Galois generators. I would like to thank M. J. Taylor for many useful discussions leading to this result.

PROPOSITION 2. *Let N_0 be an intermediate field $K \subset N_0 \subset N$, which is unramified over K; put $\Gamma_0 = \mathrm{Gal}(N/N_0)$ and $\mathcal{A}' = \mathcal{A}_{N/N_0} \cap K\Gamma_0$. Then*:

(a) *$\mathcal{A}_{N/N_0}$ is the maximal $\mathfrak{o}_{N_0}$-order in $N_0\Gamma_0$ if and only if $\mathcal{A}'$ is the maximal $\mathfrak{o}_K$-order in $K\Gamma_0$.*

(b) *If $\mathcal{A}_{N/N_0}$ is maximal then $\mathfrak{o}_N$ is free over $\mathcal{A}'$ and over $\mathcal{A}' \otimes_{\mathfrak{o}_K\Gamma_0} \mathfrak{o}_K\Gamma$; in particular*,

$$\mathfrak{o}_N \simeq \mathcal{A}_{N/K} = \mathcal{A}' \otimes_{\mathfrak{o}_K\Gamma_0} \mathfrak{o}_K\Gamma.$$

(c) *Assume that $\Gamma \geq \Gamma_0 \geq \Gamma_1$ are the inertia group and the first ramification group*, *resp.*, *and put $N_1 = N^{\Gamma_1}$*, *the maximal at most tamely ramified extension of K inside N. If $\mathcal{A}_{N/N_1}$ is the maximal $\mathfrak{o}_{N_1}$-order of $N_1\Gamma_1$*, *then $\mathcal{A}_{N/N_0}$ is also maximal and*

$$\mathfrak{o}_N \simeq \mathcal{A}_{N/K} = \mathcal{A}'' \otimes_{\mathfrak{o}_K\Gamma_1} \mathfrak{o}_K\Gamma \quad \textit{with} \quad \mathcal{A}'' = \mathcal{A}_{N/N_1} \cap K\Gamma_1.$$

Proof. (a) Since Γ_0 is abelian, the maximal orders are the integral closures of $\mathfrak{o}_K$ in the group algebras $K\Gamma_0$, resp. $N_0\Gamma_0$. So $\mathcal{A}'$ is maximal whenever $\mathcal{A}_{N/N_0}$ is maximal.

Now suppose that $\mathcal{A}'$ is maximal. Obviously, we have $\mathcal{A}_{N/N_0} \supset \mathcal{A}' \otimes_{\mathfrak{o}_K} \mathfrak{o}_{N_0}$. Since N_0/K is unramified, $\mathcal{A}' \otimes_{\mathfrak{o}_K} \mathfrak{o}_{N_0}$ is maximal by Corollary 26.27 of [9].

(b) Suppose that $\mathcal{A}_{N/N_0}$ is maximal in $N_0\Gamma_0$; thus by (a), $\mathcal{A}'$ is the maximal order of $K\Gamma_0$ and both orders are hereditary (see Theorem 18.1 of [15]). Therefore $\mathfrak{o}_N$ is projective over each of these orders, and by Theorem 18.10 of [15], even free over them. So $\mathfrak{o}_N \otimes_{\mathbb{Z}\Gamma_0} \mathbb{Z}\Gamma$ is free over $\mathcal{A}' \otimes_{\mathbb{Z}\Gamma_0} \mathbb{Z}\Gamma$.

Now we use an idea from the proof of Proposition 2.1 of [17]. Consider the exact sequence

$$\mathfrak{o}_N \otimes_{\mathbb{Z}\Gamma_0} \mathbb{Z}\Gamma \xrightarrow{\pi} \mathfrak{o}_N \to 0,$$

where π is defined by $\pi(y \otimes \gamma) = y^\gamma$. Since N_0/K is unramified, there exists some $t \in \mathfrak{o}_{N_0}$ with $\mathrm{tr}_{N_0/K}\, t = 1$, where tr denotes the trace. Using such a t, define $i : \mathfrak{o}_N \to \mathfrak{o}_N \otimes_{\mathbb{Z}\Gamma_0} \mathbb{Z}\Gamma$ by

$$i(x) = \sum_{\gamma \in \Gamma/\Gamma_0} tx^\gamma \otimes \gamma^{-1},$$

where γ runs through a set of representatives for Γ/Γ_0. One easily checks that i and π are Γ-equivariant, thus $\mathcal{A}' \otimes_{\mathbb{Z}\Gamma_0} \mathbb{Z}\Gamma$-module homomorphisms. Now $\pi \circ i = \mathrm{id}_{\mathfrak{o}_N}$ shows that the exact sequence above splits and $\mathfrak{o}_N$ is a projective module over $\mathcal{A}' \otimes_{\mathbb{Z}\Gamma_0} \mathbb{Z}\Gamma$. Using A.4 on p. 230 of [10], we conclude that $\mathfrak{o}_N$ is free over $\mathcal{A}' \otimes_{\mathbb{Z}\Gamma_0} \mathbb{Z}\Gamma$, which yields all our assertions.

(c) Γ_0 is abelian, thus we have $\Gamma_0 = \Gamma_t \times \Gamma_1$ with $|\Gamma_t| = e \mid (q-1)$ and Γ_1 the p-Sylow group of Γ_0, where q is the cardinality and p the characteristic of the residue class field of N_0. Put $N_2 = N^{\Gamma_t}$.

Since $\mathcal{A}_{N/N_1}$ is maximal, $\mathcal{A}_{N/N_1} \cap N_0\Gamma_1$ is maximal in $N_0\Gamma_1$, thus equals $\mathcal{A}_{N_2/N_0}$. Since N_1/N_0 is tame, $\mathcal{A}_{N_1/N_0} = \mathfrak{o}_{N_0}\Gamma_t$ by Noether's theorem, and this is the maximal order, because the roots of unity of order e are contained in N_0.

Thus $\mathcal{A}_{N_1/N_0} \otimes_{\mathfrak{o}_{N_0}} \mathcal{A}_{N_2/N_0} \subset N_0[\Gamma_t \times \Gamma_1]$ is the maximal order, and it equals $\mathcal{A}_{N/N_0}$ because its elements obviously map $\mathfrak{o}_N$ into itself. So we obtain

$$\begin{aligned}\mathcal{A}' &= \mathcal{A}_{N/N_0} \cap K\Gamma_0 = (\mathfrak{o}_{N_0}\Gamma_t \otimes_{\mathfrak{o}_{N_0}} \mathcal{A}_{N_2/N_0}) \cap K\Gamma_0 \\ &= \mathfrak{o}_K\Gamma_t \otimes_{\mathfrak{o}_K} (\mathcal{A}_{N_2/N_0} \cap K\Gamma_1) = \mathfrak{o}_K\Gamma_0 \otimes_{\mathfrak{o}_K\Gamma_1} \mathcal{A}'',\end{aligned}$$

which together with part (b) completes the proof.

3. The result for fields contained in $\mathbb{Q}_p(\zeta_{p^n})$. Let us agree on the following notations: for any $p \in \mathbb{P}$ and $k \in \mathbb{N}$ let $\zeta_{p^k} \in \overline{\mathbb{Q}}_p$ be a root of unity of order p^k, put $\mathbb{Q}_p^{(k)} = \mathbb{Q}_p(\zeta_{p^k})$ and $\mathbb{Q}_p^{(k)\pm} = \mathbb{Q}_p(\zeta_{p^k} \pm \zeta_{p^k}^{-1})$. For any field $L \supset \mathbb{Q}_p$ we put $L_k = L \cap \mathbb{Q}_p^{(k)}$ and $L^{(k)} = L\mathbb{Q}_p^{(k)}$.

For a finite abelian group G, let $\widehat{G} = \{\chi \mid \chi : G \to \overline{\mathbb{Q}}_p^\times\}$ be its dual group of characters χ with values in $\overline{\mathbb{Q}}_p^\times$ and

$$\varepsilon_{\chi,G} = \frac{1}{|G|} \sum_{\gamma \in G} \chi(\gamma^{-1})\gamma \in \overline{\mathbb{Q}}_p G$$

the absolutely irreducible idempotents. Put $\mathbb{Q}_p(\chi) = \mathbb{Q}_p(\{\chi(\gamma) \mid \gamma \in G\})$, the field obtained by adjoining the values of χ. For any field $L \supset \mathbb{Q}_p$ let $L_\chi = L \cap \mathbb{Q}_p(\chi)$. Then

$$\mathcal{E}_{\chi,LG} = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}_p(\chi)/L_\chi)} \varepsilon_{\chi^\sigma,G}$$

are the primitive idempotents of the group algebra

$$LG = \bigoplus_{\chi \in \widehat{\Gamma}_L} LG\mathcal{E}_{\chi,LG},$$

where $\widehat{\Gamma}_L \subset \widehat{\Gamma}$ denotes a set of representatives for the classes of characters which are conjugated over L.

Throughout this section, we will fix the following situation: let $\mathbb{Q}_p \subset K \subset N \subset \mathbb{Q}_p^{(n)}$ and $K \subset \mathbb{Q}_p^{(m)}$, where m, n are chosen minimal with $1 \le m \le n$ ($2 \le m \le n$ if $p = 2$, resp.). Put $\Gamma = \mathrm{Gal}(N/K)$ and let $\zeta \in \mathbb{Q}_p^{(n)}$ denote a root of unity of order p^n. For any $t \in \mathbb{N}$, let

$$\mathcal{R}_t \subset \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$$

denote a set of automorphisms representing $\mathrm{Gal}(K_t/\mathbb{Q}_p)$. Then we have the following result:

PROPOSITION 3. (a) *$\mathcal{A}_{N/K}$ is the maximal $\mathfrak{o}_K$-order of $K\Gamma$ except for the case $N = \mathbb{Q}_2^{(n)}$ and $K = \mathbb{Q}_2^{(m)\pm}$, where $\mathcal{A}_{N/K} = \mathfrak{o}_K\Gamma\big[\frac{2}{t}\varepsilon_{\omega,\Gamma}\big] \underset{\mathfrak{o}_K\Gamma_1}{\otimes} \mathcal{M}_1$. Here ω denotes the quadratic character belonging to $\mathbb{Q}_2^{(m)}/K$, $t \in \mathfrak{o}_K$ is a prime dividing 2, $\Gamma_1 = \mathrm{Gal}(\mathbb{Q}_2^{(n)}/\mathbb{Q}_2^{(m)})$ and $\mathcal{M}_1$ is the maximal order of $K\Gamma_1$.*

(b) *$\mathfrak{o}_N$ is a free $\mathcal{A}_{N/K}$-module. Explicitly we have $\mathfrak{o}_N = \mathcal{A}_{N/K}T_{N/K}$ with*

$$T_{N/K} = \sum_{j=0}^{n-m} \sum_{\sigma\in\mathcal{R}_{n-m-j}} \mathrm{tr}_{\mathbb{Q}_p^{(n-j)}/N_{n-j}}\, \sigma(\zeta^{p^j})$$

except for the case $N = \mathbb{Q}_2^{(n)\pm}$ and $K = \mathbb{Q}_2^{(m)+}$, where

$$T_{N/K} = 1 + \sum_{j=0}^{n-m-1} \sum_{\sigma\in\mathcal{R}_{n-m-j}} \mathrm{tr}_{\mathbb{Q}_2^{(n-j)}/N_{n-j}}\, \sigma(\zeta^{2^j}).$$

First we consider a special situation:

LEMMA 2. *Suppose that $N = \mathbb{Q}_p^{(n)}$ and $K = \mathbb{Q}_p^{(m)}$ and put $\Gamma_1 = \mathrm{Gal}(N/K)$. Let ψ be a generator of the character group $\widehat{\Gamma}_1$, let $1 \le r \le p^{n-m}$ and put $\nu = v_p(r)$.*

(a) *For any $x \in \mathbb{Z}$ with $\nu \ne v_p(x) \le n-m$ we have*

$$\varepsilon_{\psi^r,\Gamma_1}\zeta^x = 0.$$

(b) *There exists $\tau_r \in \mathcal{R}_{n-m-\nu}$ such that for all $\sigma \in \mathcal{R}_{n-m-\nu}$,*

$$\mathcal{E}_{\psi^r,K\Gamma_1}\sigma(\zeta^{p^\nu}) = \begin{cases} \tau_r(\zeta^{p^\nu}) & \text{if } \sigma = \tau_r, \\ 0 & \text{if } \sigma \ne \tau_r. \end{cases}$$

(c) *If $1 \le r' \le p^{n-m}$ with $v_p(r') = \nu$ such that $\mathcal{E}_{\psi^r,K\Gamma_1} \ne \mathcal{E}_{\psi^{r'},K\Gamma_1}$ then $\tau_r \ne \tau_{r'}$.*

Proof. If $m = n$, we have $K = N$, $\nu = 0$, $\Gamma_1 = \mathcal{R}_0 = \{\mathrm{id}\}$ and the lemma reduces to trivialities. So assume that $m < n$.

(a) Let $M_1 = \mathbb{Q}_p^{(n-\nu)}$ be the subfield of N which is fixed by $\langle\psi^r\rangle^\perp = \{\gamma \in \Gamma_1 \mid \psi^r(\gamma) = 1\}$ and $M_2 = \mathbb{Q}_p(\zeta^x) = \mathbb{Q}_p^{(n-v_p(x))}$; so $K \subset M_i \subset N$.

If $v_p(x) < \nu$ then $M_1 \subsetneqq M_2$ and $\varepsilon_{\psi^r,\Gamma_1}$ contains the trace from N to M_1 as a factor, which annihilates ζ^x (here the lower bounds for m are vital!).

If $v_p(x) > \nu$ then $M_2 \subsetneqq M_1$ and the restriction of $\varepsilon_{\psi^r,\Gamma_1}$ to M_2 is 0 by Lemma 1(b) of [5].

(b) Let $x \in \mathbb{Z}$ with $v_p(x) = \nu$. The automorphism $\sigma_{1+p^m} : \zeta \mapsto \zeta^{1+p^m}$ generates Γ_1, and without restriction we may assume that $\psi(\sigma_{1+p^m}) = \zeta^{p^m}$.

First we consider the case $\nu \geq n-2m$. We have $K_{n-m-\nu} = \mathbb{Q}_p^{(n-m-\nu)} \subset K$, $\mathcal{R}_{n-m-\nu}$ corresponds to $\mathrm{Gal}(\mathbb{Q}_p^{(n-m-\nu)}/\mathbb{Q}_p)$ and for any $k \in \mathbb{N}$,

$$x(1+p^m)^k \equiv x(1+kp^m) \bmod p^n.$$

So we obtain

$$\mathcal{E}_{\psi^r,K\Gamma_1}\zeta^x = \varepsilon_{\psi^r,\Gamma_1}\zeta^x = \frac{1}{p^{n-m}} \sum_{0\leq k<p^{n-m}} \zeta^{-rp^m k}\zeta^{x(1+p^m)^k}$$
$$= \frac{1}{p^{n-m}}\zeta^x \sum_{0\leq k<p^{n-m}} \zeta^{(x-r)p^m k} = \begin{cases} \zeta^x & \text{if } x \equiv r \bmod p^{n-m}, \\ 0 & \text{else.} \end{cases}$$

If σ runs through $\mathcal{R}_{n-m-\nu}$, we have $\sigma(\zeta^{p^\nu}) = \zeta^{p^\nu t}$ with t running through $\mathbb{Z}/(p^{n-m-\nu})^\times$. Thus the above calculation yields Lemma 2(b) in this case.

Now we consider the case $0 \leq \nu < n-2m$, which yields $K_{n-m-\nu} = K$ and $\mathcal{R}_{n-m-\nu}$ corresponding to $\mathrm{Gal}(K/\mathbb{Q}_p)$. For any $k \in \mathbb{N}$ with $v_p(k) \geq n-2m-\nu$ one has

$$\text{(2)} \qquad x(1+p^m)^k \equiv \begin{cases} x(1+kp^m) \bmod p^n & \text{if } p \geq 3, \\ x(1+kp^m+kp^{2m-1}) \bmod p^n & \text{if } p = 2. \end{cases}$$

Put $\mathfrak{G} = \mathrm{Gal}(\mathbb{Q}_p^{(n-m-\nu)}/K)$. For $j \in \mathbb{Z}$ we have

$$\sum_{\sigma\in\mathfrak{G}} \sigma(\zeta^j) = \begin{cases} 0 & \text{if } \zeta^j \notin K, \\ p^{n-2m-\nu}\zeta^j & \text{if } \zeta^j \in K. \end{cases}$$

Now we can calculate

$$\begin{aligned} \mathcal{E}_{\psi^r,K\Gamma_1}\zeta^x &= \sum_{\sigma\in\mathfrak{G}} \varepsilon_{(\psi^r)^\sigma,\Gamma_1}\zeta^x \\ &= \frac{1}{p^{n-m}} \sum_{0\leq k<p^{n-m}} \zeta^{x(1+p^m)^k} \sum_{\sigma\in\mathfrak{G}} \sigma(\zeta^{-rp^m k}) \\ &= \frac{1}{p^{n-m}} \sum_{\substack{0\leq k<p^{n-m} \\ v_p(k)\geq n-2m-\nu}} \zeta^{x(1+p^m)^k} p^{n-2m-\nu}\zeta^{-rp^m k} \\ &= \frac{1}{p^{m+\nu}} \sum_{0\leq j<p^{m+\nu}} \zeta^{x(1+p^m)^{jp^{n-2m-\nu}}} \zeta^{-rjp^{n-m-\nu}}. \end{aligned}$$

Using (2), we obtain for $p \geq 3$,

$$\mathcal{E}_{\psi^r,K\Gamma_1}\zeta^x = \frac{1}{p^{m+\nu}}\zeta^x \sum_{0\leq j<p^{m+\nu}} \zeta^{(x-r)jp^{n-m-\nu}} = \begin{cases} \zeta^x & \text{if } x \equiv r \bmod p^{m+\nu}, \\ 0 & \text{else.} \end{cases}$$

For $p = 2$ we arrive at

$$\begin{aligned}\mathcal{E}_{\psi^r,K\Gamma_1}\zeta^x &= \frac{1}{2^{m+\nu}} \sum_{0\leq j<2^{m+\nu}} \zeta^{x(1+j2^{n-m-\nu}+j2^{n-\nu-1})}\zeta^{-rj2^{n-m-\nu}} \\ &= \frac{1}{2^{m+\nu}}\zeta^x \sum_{0\leq j<2^{m+\nu}} (-\zeta^{(x-r)2^{n-m-\nu}})^j \\ &= \begin{cases} \zeta^x & \text{if } x \equiv r \bmod 2^{m+\nu}, \\ 0 & \text{else.} \end{cases}\end{aligned}$$

The proof now concludes as in the first case.

(c) There is some $\varrho \in \mathcal{R}_{n-m-\nu}$ which does not induce the identity on $K_{n-m-\nu}$, such that $\mathcal{E}_{\psi^{r'},K\Gamma_1} = \mathcal{E}_{(\psi^r)^\varrho,K\Gamma_1}$. Applying ϱ to the result of part (b) we see that $\tau_{r'} \neq \tau_r$.

Now we consider the situation where K is an arbitrary subfield of $N = \mathbb{Q}_p^{(n)}$ and $\Gamma = \mathrm{Gal}(N/K)$ can be written as $\Gamma = \Delta \times \Gamma_1$ with $\Gamma_1 = \mathrm{Gal}(\mathbb{Q}_p^{(n)}/\mathbb{Q}_p^{(m)})$ and $|\Delta| = e$, where $e \mid (p-1)$ for $p \geq 3$ and $e \leq 2$ for $p = 2$. Choosing generators, we write the character groups as $\widehat{\Gamma} = \widehat{\Delta} \times \widehat{\Gamma}_1 = \langle\omega\rangle \times \langle\psi\rangle$.

Lemma 3. *Let $\chi = \omega^s\psi^r \in \widehat{\Gamma}$ with $1 \leq r \leq p^{n-m}$, $1 \leq s \leq e$ and put $\nu = v_p(r)$.*

(a) *For any $x \in \mathbb{Z}$ with $\nu \neq v_p(x) \leq n - m$ we have*

$$\varepsilon_{\chi,\Gamma}\zeta^x = 0.$$

(b) *There exists $\tau_r \in \mathcal{R}_{n-m-\nu}$ such that for all $\sigma \in \mathcal{R}_{n-m-\nu}$ and for all s with $1 \leq s \leq e$ we have*

$$\mathcal{E}_{\chi,K\Gamma}\sigma(\zeta^{p^\nu}) = \begin{cases} \varepsilon_{\omega^s,\Delta}\tau_r(\zeta^{p^\nu}) & \text{if } \sigma = \tau_r, \\ 0 & \text{if } \sigma \neq \tau_r. \end{cases}$$

(c) *If $1 \leq r' \leq p^{n-m}$ with $v_p(r') = \nu$ such that ψ^r and $\psi^{r'}$ are not conjugated over K then $\tau_r \neq \tau_{r'}$.*

Proof. (a) With $\varepsilon_{\chi,\Gamma} = \varepsilon_{\omega^s,\Delta}\varepsilon_{\psi^r,\Gamma_1}$, this follows from Lemma 2(a).

(b) We have $\mathcal{E}_{\chi,K\Gamma} = \varepsilon_{\omega^s,\Delta}\mathcal{E}_{\psi^r,K\Gamma_1} = \varepsilon_{\omega^s,\Delta}\sum_{\delta\in\Delta}\mathcal{E}_{(\psi^r)^\delta,\mathbb{Q}_p^{(m)}\Gamma_1}$. Since $\varepsilon_{\omega^s,\Delta} \in \mathbb{Q}_p\Delta$, we obtain for any $\xi \in N$,

$$\mathcal{E}_{\chi,K\Gamma}\xi = \sum_{\delta\in\Delta}\mathcal{E}_{(\psi^r)^\delta,\mathbb{Q}_p^{(m)}\Gamma_1}\biggl(\frac{1}{e}\sum_{\delta'\in\Delta}\omega^{-s}(\delta')\delta'(\xi)\biggr).$$

There is a one-to-one-correspondence between $\mathcal{R}_{n-m-\nu}\times\Delta$ and the set $\mathcal{R}_{n-m-\nu}$ which we considered in Lemma 2(b). Thus there exist uniquely determined $\theta_r\in\Delta$ and $\tau_r\in\mathcal{R}_{n-m-\nu}$ such that for all $\sigma\in\mathcal{R}_{n-m-\nu}\times\Delta$ we have

$$\mathcal{E}_{\psi^r,\mathbb{Q}_p^{(m)}\Gamma_1}\sigma(\zeta^{p^\nu}) = \begin{cases}\theta_r\tau_r(\zeta^{p^\nu}) & \text{if } \sigma=\theta_r\tau_r,\\ 0 & \text{if } \sigma\ne\theta_r\tau_r.\end{cases}$$

Now an easy calculation yields the claim of part (b).

(c) The same argument as for Lemma 2(c) applies.

After these preliminary results we now prove Proposition 3.

Proof of Proposition 3

Case I: $p\ge 3$. Since $\mathbb{Q}_p^{(n)}/N$ is tamely ramified, we can apply Lemmas 4(b) and 6 of [5] to deduce the results for N/K from those for $\mathbb{Q}_p^{(n)}/K$. Thus it suffices to consider $N=\mathbb{Q}_p^{(n)}$, the situation dealt with in Lemma 3, and we take over the notations used there. Let $\mathcal{M}$ be the maximal order of $K\Gamma$, which decomposes as

$$\mathcal{M} = \bigoplus_{\chi\in\widehat{\Gamma}_K}\mathcal{M}_\chi = \bigoplus_{\substack{1\le s\le e\\ 0\le\nu\le n-m}}\ \bigoplus_{\sigma\in\mathcal{R}_{n-m-\nu}}\mathcal{M}_{(\omega^s\psi^{p^\nu})^\sigma}.$$

It suffices to show that

$$\mathcal{M}T_{N/K} = \mathfrak{o}_N \quad\text{with}\quad T_{N/K} = \sum_{j=0}^{n-m}\sum_{\sigma\in\mathcal{R}_{n-m-j}}\sigma(\zeta^{p^j}).$$

If $\nu\le n-2m$ we use Lemma 3(a) in [5] to obtain for any $\tau\in\mathcal{R}_{n-m-\nu}$,

$$\mathcal{M}_{(\omega^s\psi^{p^\nu})^\tau} = \mathfrak{o}_K\Gamma\mathcal{E}_{\omega^s\psi^r,K\Gamma}$$

for some $1\le r\le p^{n-m}$ with $v_p(r)=\nu$. Using Lemma 3, we get

$$\begin{aligned}\bigoplus_{s=1}^{e}\mathcal{M}_{\omega^s\psi^r}T_{N/K} &= \bigoplus_{s=1}^{e}\mathfrak{o}_K\Gamma\mathcal{E}_{\omega^s\psi^r,K\Gamma}\Bigl(\sum_{\sigma\in\mathcal{R}_{n-m-\nu}}\sigma(\zeta^{p^\nu})\Bigr)\\ &= \bigoplus_{s=1}^{e}\mathfrak{o}_K\Gamma\varepsilon_{\omega^s,\Delta}\tau_r(\zeta^{p^\nu}) = \mathfrak{o}_K\Gamma\tau_r(\zeta^{p^\nu})\end{aligned}$$

and therefore

$$\bigoplus_{s=1}^{e}\bigoplus_{\tau\in\mathcal{R}_{n-m-\nu}}\mathcal{M}_{(\omega^s\psi^{p^\nu})^\tau}T_{N/K} = \bigoplus_{\sigma\in\mathcal{R}_{n-m-\nu}}\mathfrak{o}_K\Gamma\sigma(\zeta^{p^\nu}),$$

which contains all roots of unity of order $p^{n-\nu}$, since $\Gamma\mathcal{R}_{n-m-\nu} = \mathrm{Gal}(\mathbb{Q}_p^{(n)}/\mathbb{Q}_p)$.

If $n-2m < \nu < n-m$ we have for any $1 \le r \le p^{n-m}$ with $v_p(r) = \nu$,

$$\mathcal{E}_{\omega^s\psi^r,K\Gamma} T_{N/K} = \Big(\varepsilon_{\omega^s,\Delta} \sum_{\varrho\in\Delta} \varepsilon_{(\psi^r)^\varrho,\Gamma_1}\Big) T_{N/K} = \varepsilon_{\omega^s,\Delta}\varepsilon_{(\psi^r)^{\varrho_0},\Gamma_1}\tau_r(\zeta^{p^\nu})$$

for some $\varrho_0 \in \Delta$. Using Lemma 3(a) in [5] yields

$$\mathcal{M}_{\omega^s\psi^r} T_{N/K} = \mathfrak{o}_K \varepsilon_{\omega^s,\Delta}\mathfrak{o}^{(m)}\tau_r(\zeta^{p^\nu}),$$

therefore we obtain

$$\bigoplus_{s=1}^{e} \mathcal{M}_{\omega^s\psi^r} T_{N/K} = \bigoplus_{s=1}^{e} \mathfrak{o}_K \varepsilon_{\omega^s,\Delta}\mathfrak{o}^{(m)}\tau_r(\zeta^{p^\nu}) = \mathfrak{o}^{(m)}\Delta\tau_r(\zeta^{p^\nu})$$

and

$$\bigoplus_{\tau\in\mathcal{R}_{n-m-\nu}} \bigoplus_{s=1}^{e} \mathcal{M}_{(\omega^s\psi^{p^\nu})^\tau} T_{N/K} = \bigoplus_{\sigma\in\mathcal{R}_{n-m-\nu}} \mathfrak{o}^{(m)}\Delta\sigma(\zeta^{p^\nu}).$$

Since $\Delta\mathcal{R}_{n-m-\nu} = \mathrm{Gal}(\mathbb{Q}_p^{(n-m-\nu)}/\mathbb{Q}_p)$ one can check that the last sum contains all roots of unity of order $p^{n-\nu}$.

If $\nu = n-m$, a simple argument yields

$$\bigoplus_{s=1}^{e} \mathcal{M}_{\omega^s} T_{N/K} = \mathfrak{o}^{(m)}.$$

Thus we achieved

$$\begin{aligned}\mathcal{M}T_{N/K} &= \bigoplus_{\nu=0}^{n-2m} \bigoplus_{\sigma\in\mathcal{R}_{n-m-\nu}} \mathfrak{o}_K\Gamma\sigma(\zeta^{p^\nu}) \\ &\quad \oplus \bigoplus_{\max\{n-2m+1,0\}}^{n-m} \bigoplus_{\sigma\in\mathcal{R}_{n-m-\nu}} \mathfrak{o}^{(m)}\Delta\sigma(\zeta^{p^\nu}) \\ &= \mathfrak{o}_N.\end{aligned}$$

Case II: $p = 2$. 1. A simpler version (without tame characters ω^s) of the proof of Case I applies for the situation $N = \mathbb{Q}_2^{(n)}$, $K = \mathbb{Q}_2^{(m)}$ with $2 \le m \le n$ (in this case Proposition 3 also follows from the global results of [2] or [5]).

2. Now we consider the case $N = \mathbb{Q}_2^{(n)\pm}$ and $K = \mathbb{Q}_2^{(m)+}$ with $2 \le m < n$ (this includes the case $K = \mathbb{Q}_2^{(2)+} = \mathbb{Q}_2$). Let $\Delta = \mathrm{Gal}(\mathbb{Q}_2^{(n)}/N) = \langle\tau\rangle$ and $\Gamma_1 = \mathrm{Gal}(\mathbb{Q}_2^{(n)}/\mathbb{Q}_2^{(m)}) \simeq \Gamma$. Using Lemma 4(a) of [5] and the result for Case

1 above we see that $\mathcal{A}_{N/K}$ is the maximal order, thus

$$\mathcal{A}_{N/K} = \mathcal{M} = \bigoplus_{\nu=0}^{n-m} \bigoplus_{\sigma\in\mathcal{R}_{n-m-\nu}} \mathcal{M}_{(\psi^{2^\nu})^\sigma},$$

where $\langle\psi\rangle = \widehat{\Gamma} \simeq \widehat{\Gamma}_1$. For $1 \le r \le 2^{n-m}$ we put $\nu = v_2(r)$ and $\eta_\nu = \zeta^{2^\nu} + \tau(\zeta^{2^\nu}) = \mathrm{tr}_{\mathbb{Q}_2^{(n-\nu)}/N_{n-\nu}}(\zeta^{2^\nu})$.

If $\nu \le n-2m$ we use Lemma 2 to obtain

$$\begin{aligned}\mathcal{E}_{\psi^r,K\Gamma}T_{N/K} &= (\mathcal{E}_{\psi^r,\mathbb{Q}_2^{(m)}\Gamma_1} + \mathcal{E}_{(\psi^r)^\tau,\mathbb{Q}_2^{(m)}\Gamma_1}) \sum_{\sigma\in\mathcal{R}_{n-m-\nu}} \sigma(\zeta^{2^\nu} + \tau(\zeta^{2^\nu}))\\ &= \tau_r(\eta_\nu)\end{aligned}$$

and

$$\bigoplus_{\sigma\in\mathcal{R}_{n-m-\nu}} \mathcal{M}_{(\psi^{2^\nu})^\sigma}T_{N/K} = \bigoplus_{\sigma\in\mathcal{R}_{n-m-\nu}} \mathfrak{o}_K\Gamma\sigma(\eta_\nu),$$

which contains all conjugates of η_ν.

If $n-2m < \nu \le n-m-2$ we have $\mathcal{E}_{\psi^r,K\Gamma} = \varepsilon_{\psi^r,\Gamma_1} + \varepsilon_{(\psi^r)^\tau,\Gamma_1}$, and again using Lemma 3(a) of [5], we can calculate

$$\mathcal{M}_{\psi^r}T_{N/K} = \mathcal{M}_{\psi^r}\tau_r(\eta_\nu) = (1+\tau)\mathfrak{o}^{(m)}\tau_r(\zeta^{2^\nu}).$$

Again, one can verify that

$$\bigoplus_{\sigma\in\mathcal{R}_{n-m-\nu}} \mathcal{M}_{(\psi^{2^\nu})^\sigma}T_{N/K} = \bigoplus_{\sigma\in\mathcal{R}_{n-m-\nu}} (1+\tau)\mathfrak{o}^{(m)}\sigma(\zeta^{2^\nu})$$

contains all conjugates of η_ν.

If $\nu = n-m-1$, i.e. $r = 2^{n-m-1}$, we have $\mathcal{M}_{\psi^r}T_{N/K} = \mathfrak{o}_K\varepsilon_{\psi^r,\Gamma}\eta_\nu = \mathfrak{o}_K\eta_\nu$; and if $\nu = n-m$, then ψ^r is the trivial character and we have $\mathcal{M}_{\psi^r}T_{N/K} = \mathfrak{o}_K\varepsilon_1 1 = \mathfrak{o}_K$ (remember that we deal with the case where $T_{N/K}$ has an exceptional form).

Combining all these results, we see that $\mathcal{M}T_{N/K}$ contains $\mathfrak{o}_K$ and all conjugates of η_ν for $0 \le \nu < n-m$, thus $\mathcal{M}T_{N/K} = \mathfrak{o}_N$.

3. The last case to consider is $N = \mathbb{Q}_2^{(n)}$ and $K = \mathbb{Q}_2^{(m)\pm}$ with $2 \le m \le n$ (and $3 \le m$ if $K = \mathbb{Q}_2^{(m)-}$). Let $\Gamma_1 = \mathrm{Gal}(\mathbb{Q}_2^{(n)}/\mathbb{Q}_2^{(m)})$. Then for $m < n$ the exact sequence $1 \to \Gamma_1 \to \Gamma \to \Delta \to 1$ splits if $K = \mathbb{Q}_2^{(m)+}$, and does not split if $K = \mathbb{Q}_2^{(m)-}$.

Put $\Delta = \langle\tau\rangle = \mathrm{Gal}(\mathbb{Q}_2^{(n)}/\mathbb{Q}_2^{(n)+})$ in the first case and $\Delta = \{1,\tau\} \subset \Gamma$, a set of representatives for $\mathrm{Gal}(\mathbb{Q}_2^{(m)}/K)$, in the latter, and denote the quadratic character belonging to $\mathbb{Q}_2^{(m)}/K$ by ω. Let $\langle\psi\rangle = \widehat{\Gamma}_1$. Then the maximal order $\mathcal{M}_1$ of $K\Gamma_1$ decomposes as

$$\mathcal{M}_1 = \bigoplus_{\nu=0}^{n-m} \bigoplus_{\sigma\in\mathcal{R}_{n-m-\nu}} \mathcal{M}'_{(\psi^{2^\nu})^\sigma},$$

where $\mathcal{M}'_{(\psi^{2^\nu})^\sigma}$ is the maximal order of the component $K\Gamma_1\mathcal{E}_{(\psi^{2^\nu})^\sigma,K\Gamma_1}$.

For any $1\le r\le 2^{n-m}$ with $0\le \nu = v_2(r)\le n-m-2$ we obtain from Lemma 1(b),

$$\mathcal{E}_{\psi^r,K\Gamma_1}T_{N/K} = (\mathcal{E}_{\psi^r,\mathbb{Q}_2^{(m)}\Gamma_1} + \mathcal{E}_{(\psi^r)^\tau,\mathbb{Q}_2^{(m)}\Gamma_1}) \sum_{\sigma\in\mathcal{R}_{n-m-\nu}} \sigma(\zeta^{2^\nu}) = \tau_r(\zeta^{2^\nu}).$$

If $0\le\nu\le n-2m$ we obtain

$$\Big(\mathfrak{o}_K\Gamma\Big[\frac{2}{t}\varepsilon_{\omega,\Gamma}\Big] \underset{\mathfrak{o}_K\Gamma_1}{\otimes} \bigoplus_{\sigma\in\mathcal{R}_{n-m-\nu}} \mathcal{M}'_{(\psi^{2^\nu})^\sigma}\Big)T_{N/K}$$
$$= \Big(\bigoplus_{\sigma\in\mathcal{R}_{n-m-\nu}} \mathfrak{o}_K\Delta\mathfrak{o}_K\Gamma_1\mathcal{E}_{(\psi^{2^\nu})^\sigma,K\Gamma_1}\Big)T_{N/K} = \bigoplus_{\sigma\in\mathcal{R}_{n-m-\nu}} \mathfrak{o}_K\Delta\Gamma_1\sigma(\zeta^{2^\nu}).$$

Since $\Delta\Gamma_1\mathcal{R}_{n-m-\nu} = \mathrm{Gal}(\mathbb{Q}_2^{(n)}/\mathbb{Q}_2)$, the last sum contains all conjugates of ζ^{2^ν}.

If $n-2m<\nu\le n-m-2$ one can calculate that $\mathcal{M}'_{\psi^r}T_{N/K} = \mathfrak{o}^{(m)}\tau_r(\zeta^{2^\nu})$. Therefore

$$\Big(\mathfrak{o}_K\Gamma\Big[\frac{2}{t}\varepsilon_{\omega,\Gamma}\Big] \underset{\mathfrak{o}_K\Gamma_1}{\otimes} \bigoplus_{\sigma\in\mathcal{R}_{n-m-\nu}} \mathcal{M}'_{(\psi^{2^\nu})^\sigma}\Big)T_{N/K} = \bigoplus_{\sigma\in\mathcal{R}_{n-m-\nu}} \mathfrak{o}^{(m)}\Delta\sigma(\zeta^{2^\nu}),$$

containing again all conjugates of ζ^{2^ν}.

If $\nu = n-m-1$, we have $\mathcal{E}_{\psi^r,K\Gamma_1} = \varepsilon_{\psi^r}$, thus

$$\Big(\mathfrak{o}_K\Gamma\Big[\frac{2}{t}\varepsilon_{\omega,\Gamma}\Big] \underset{\mathfrak{o}_K\Gamma_1}{\otimes} \mathcal{M}'_{\psi^r}\Big)T_{N/K} = \mathfrak{o}_K\Delta\zeta^{2^{n-m-1}} = \mathfrak{o}^{(m)}\zeta^{2^{n-m-1}}.$$

If $\nu = n-m$, we obtain

$$\Big(\mathfrak{o}_K\Gamma\Big[\frac{2}{t}\varepsilon_{\omega,\Gamma}\Big] \underset{\mathfrak{o}_K\Gamma_1}{\otimes} \mathfrak{o}_K\varepsilon_{1,\Gamma_1}\Big)T_{N/K} = \mathfrak{o}_K\Delta\Big[\frac{2}{t}\varepsilon_{\omega,\Gamma}\Big]\zeta^{2^{n-m}} = \mathfrak{o}^{(m)}$$

by Proposition 3 of [14].

Combining all these results, we again arrive at $\mathcal{A}_{N/K}T_{N/K} = \mathfrak{o}_N$.

4. Proof of Theorem 1. For $f\in\mathbb{N}$, $n\in\mathbb{N}_0$, let $\mathbb{Q}_p^{(f,n)}$ denote the field obtained by adjoining all roots of unity of orders p^n and p^f-1 to $\mathbb{Q}_p$. Then $\mathbb{Q}_p^{(f,n)}/\mathbb{Q}_p$ is the composite of the totally ramified extension $\mathbb{Q}_p^{(1,n)}$ and the unramified extension $\mathbb{Q}_p^{(f,0)}$ of degree f over $\mathbb{Q}_p$. Moreover, $\bigcup_{f\ge1,n\ge0}\mathbb{Q}_p^{(f,n)}$ is the maximal abelian extension of $\mathbb{Q}_p$.

Now let N be any finite abelian extension of $\mathbb{Q}_p$, K some subfield of N, and N_0 the inertia field of N/K. By Lemma 1 we can find a suitable $f \in \mathbb{N}$ such that $\overline{N} = N\mathbb{Q}_p^{(f,0)}$ is the composite of $\overline{K} = K\mathbb{Q}_p^{(f,0)}$ which is unramified over K, and some field N' which is totally ramified over K. Let $n \in \mathbb{N}$ be minimal with $\overline{N} \subset \mathbb{Q}_p^{(f,n)}$ and put $\widetilde{N} = \overline{N} \cap \mathbb{Q}_p^{(1,n)}$ and $\widetilde{K} = \overline{K} \cap \mathbb{Q}_p^{(1,n)}$. By Proposition 3(b), $\mathfrak{o}_{\widetilde{N}} = \mathcal{A}_{\widetilde{N}/\widetilde{K}} T_{\widetilde{N}/\widetilde{K}}$. Composition with $\mathbb{Q}_p^{(f,0)}$ yields $\mathfrak{o}_{\overline{N}} = \mathcal{A}_{\overline{N}/\overline{K}} T_{\widetilde{N}/\widetilde{K}}$ by Proposition 1(b). Since $\overline{K}/K$ is unramified, $\mathfrak{o}_{\overline{K}} \simeq \mathcal{A}_{\overline{K}/K}$, which equals the integral group ring. Applying now the other implication of Proposition 1(b) and Lemmas 5(b) and 6 of [5], we obtain $\mathfrak{o}_{N'} \simeq \mathcal{A}_{N'/K}$, $\mathfrak{o}_{\overline{N}} \simeq \mathcal{A}_{\overline{N}/K}$ and $\mathfrak{o}_N \simeq \mathcal{A}_{N/K}$.

Being aware that for $p \geq 3$, $\mathcal{A}_{\widetilde{N}/\widetilde{K}}$ is maximal, we conclude that the associated order is the maximal one for any totally ramified extension; in particular, $\mathcal{A}_{N/N_0}$ is maximal. Using now Proposition 2(b) we obtain

$$\mathfrak{o}_N \simeq \mathcal{A}_{N/K} \simeq \mathfrak{o}_K\Gamma \underset{\mathfrak{o}_K\Gamma_0}{\otimes} (\mathcal{A}_{N/N_0} \cap K\Gamma_0) = \mathfrak{o}_K\Gamma \underset{\mathfrak{o}_K\Gamma_0}{\otimes} \mathcal{M}_0.$$

References

[1] F. Bertrandias et M.-J. Ferton, *Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local*, C. R. Acad. Sci. Paris Sér. A 274 (1972), 1330–1333.

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

[3] J. Brinkhuis, *Normal integral bases and complex conjugation*, J. Reine Angew. Math. 375/376 (1987), 157–166.

[4] N. P. Byott, *Galois structure of ideals in wildly ramified abelian p-extensions of a p-adic field, and some applications*, J. Théor. Nombres Bordeaux 9 (1997), 201–219.

[5] N. P. Byott and G. Lettl, *Relative Galois module structure of integers of abelian fields*, ibid. 8 (1996), 125–141.

[6] S.-P. Chan and C.-H. Lim, *Relative Galois module structure of rings of integers of cyclotomic fields*, J. Reine Angew. Math. 434 (1993), 205–220.

[7] L. Childs, *Taming wild extensions with Hopf algebras*, Trans. Amer. Math. Soc. 304 (1987), 111–140.

[8] L. Childs and D. J. Moss, *Hopf algebras and local Galois module theory*, in: Advances in Hopf Algebras, J. Bergen and S. Montgomery (eds.), Lecture Notes in Pure and Appl. Math. 158, Dekker, Basel, 1994, 1–24.

[9] C. W. Curtis and I. Reiner, *Methods of Representation Theory*, Vol. I, Pure Appl. Math., Wiley, 1981.

[10] A. Fröhlich, *Invariants for modules over commutative separable orders*, Quart. J. Math. Oxford Ser. (2) 16 (1965), 193–232.

[11] —, *Galois module structure of algebraic integers*, Ergeb. Math. Grenzgeb. 3, Vol. 1, Springer, 1983.

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

[13] G. Lettl, *The ring of integers of an abelian number field*, ibid. 404 (1990), 162–170.

[14] G. Lettl, *Note on the Galois module structure of quadratic extensions*, Colloq. Math. 67 (1994), 15–19.
[15] I. Reiner, *Maximal Orders*, London Math. Soc. Monographs 5, Academic Press, 1975.
[16] K. W. Roggenkamp and M. J. Taylor, *Group rings and class groups*, DMV-Sem. 18, Birkhäuser, 1992.
[17] M. J. Taylor, *On the Galois module structure of rings of integers of wild*, *abelian extensions*, J. London Math. Soc. 52 (1995), 73–87.

Institut für Mathematik
Karl-Franzens-Universität
Heinrichstrasse 36
A-8010 Graz, Austria
E-mail: guenter.lettl@kfunigraz.ac.at

Received on 14.7.1997 (3214)