ACTA ARITHMETICA
122.1 (2006)

On the trace map between absolutely abelian number fields of equal conductor

by

Henri Johnston (Ithaca, NY)

1. Introduction. Let L/K be an extension of absolutely abelian number fields of equal conductor, n. If $T_{L/K} : L \to K$ denotes the trace map, then $T_{L/K}(\mathcal{O}_L)$ is an ideal in $\mathcal{O}_K$. Let $I(L/K)$ denote the norm of $T_{L/K}(\mathcal{O}_L)$ over $\mathbb{Q}$, i.e. $[\mathcal{O}_K : T_{L/K}(\mathcal{O}_L)]$. Sharpening the main result of Girstmair in [6], we determine $I(L/K)$ exactly for any such L/K: if $e = v_2(n)$ and $m = n/2^e$, then

$$I(L/K) = \begin{cases} 2^{[K\cap\mathbb{Q}^{(m)}:\mathbb{Q}]} = 2^{[K:\mathbb{Q}]/2^{e-2}} & \text{if } L/K \text{ is wildly ramified,} \\ 1 & \text{otherwise.} \end{cases}$$

After first determining criteria for wild ramification of L/K (which can only happen at primes above 2), the above result is obtained for $n = 2^e$ ($e \geq 3$) by computing $T_{L/K}(\mathcal{O}_L)$ explicitly, and is then extended to the general case. This approach does not rely on Leopoldt's Theorem, in contrast to the techniques used in [6].

The explicit nature of the calculations used to compute $I(L/K)$ leads to the definition of an "adjusted trace map" $\widehat{T}_{\mathbb{Q}^{(n)}/K}$ with the property that $\widehat{T}_{\mathbb{Q}^{(n)}/K}(\mathcal{O}^{(n)}) = \mathcal{O}_K$ (here $\mathbb{Q}^{(n)}$ denotes the nth cyclotomic field and $\mathcal{O}^{(n)}$ its ring of integers). Using this map, we restate Leopoldt's Theorem and show that its proof can be reduced to the (easier) cyclotomic case.

2. Dirichlet characters. We first recall some basic facts about Dirichlet characters. For more details, see Chapter 3 of [12] and Section 2 of [10].

Definition 2.1. For $n \in \mathbb{N}$, let ζ_n be a primitive nth root of unity and $\mathbb{Q}^{(n)} = \mathbb{Q}(\zeta_n)$ the nth cyclotomic field. Let $\mathcal{O}^{(n)} = \mathcal{O}_{\mathbb{Q}^{(n)}} = \mathbb{Z}[\zeta_n]$ denote the ring of integers of $\mathbb{Q}^{(n)}$, and $X^{(n)}$ denote the group of Dirichlet characters of conductor dividing n.

2000 *Mathematics Subject Classification*: Primary 11R04; Secondary 11R33.
Partially supported by the States of Jersey Education, Sport and Culture Committee through the Jersey Scholarship.

Let $\mathbb{P}$ denote the set of rational primes. Define $p^* = 4$ if $p = 2$, and $p^* = p$ if $p \in \mathbb{P}$, $p \neq 2$.

PROPOSITION 2.2. *Let $p \in \mathbb{P}$ and $e \in \mathbb{N}$, with $e \geq 2$ if $p = 2$. Then there exists a natural decomposition*

$$(\mathbb{Z}/p^e\mathbb{Z})^\times = (\mathbb{Z}/p^*\mathbb{Z})^\times \times (1 + p^*\mathbb{Z})/(1 + p^e\mathbb{Z})$$

where both factors are considered as subgroups of $(\mathbb{Z}/p^e\mathbb{Z})^\times$. Note that we take $(\mathbb{Z}/4\mathbb{Z})^\times = \{\pm 1\}$.

Proof. Straightforward. ∎

DEFINITION 2.3. Let $p \in \mathbb{P}$ and $e \in \mathbb{N}$ with $e \geq 2$ if $p = 2$. Then dualizing the decomposition of Proposition 2.2 yields the decomposition

$$X^{(p^e)} = \langle \omega_p \rangle \times \langle \psi_{p^e} \rangle$$

with $\langle \omega_p \rangle = X^{(p^*)}$ and $\langle \psi_{p^e} \rangle$ the group of Dirichlet characters whose conductors divide p^e and which are trivial on the factor $(\mathbb{Z}/p^*\mathbb{Z})^\times$.

THEOREM 2.4. *Let $n \in \mathbb{N}$. There is an order preserving one-to-one correspondence between subgroups of $X^{(n)}$ and subfields of $\mathbb{Q}^{(n)}$. Let X_i be the subgroup corresponding to the subfield K_i. Then $|X_i| = [K_i : \mathbb{Q}]$ and the compositum K_1K_2 corresponds to $\langle X_1, X_2 \rangle$.*

Proof. See Chapter 3 of [12]. ∎

DEFINITION 2.5. Let $p \in \mathbb{P}$, $X \subseteq X^{(n)}$ and $e = v_p(n)$. Then X_p denotes the image of X under the natural projection $\pi_p : X^{(n)} \to X^{(p^e)}$.

THEOREM 2.6. *Let X be a group of Dirichlet characters and let K be the associated abelian number field. Then $p \in \mathbb{P}$ has ramification index $|X_p|$ in K.*

Proof. This is Theorem 3.5 of [12]. ∎

REMARK 2.7. When p is odd, $\langle \omega_p \rangle$ and $\langle \psi_{p^e} \rangle$ have orders $p-1$ and p^{e-1} respectively. So by considering the decomposition $X^{(p^e)} = \langle \omega_p \rangle \times \langle \psi_{p^e} \rangle$, the field corresponding to $\langle \omega_p \rangle$ can be thought of as the "tame part" of $\mathbb{Q}^{(p^e)}$, and that corresponding to $\langle \psi_{p^e} \rangle$ as the "wild part".

When $p = 2$, $\langle \omega_2 \rangle$ and $\langle \psi_{2^e} \rangle$ have orders 2 and 2^{e-2} respectively, and therefore both correspond to wildly ramified extensions of $\mathbb{Q}$ (namely $\mathbb{Q}(i)$ and the maximal totally real subfield $\mathbb{Q}(\zeta_{2^e} + \zeta_{2^e}^{-1})$, respectively). In other words, $\mathbb{Q}^{(2^e)}$ has no "tame part".

PROPOSITION 2.8. *Let $K/\mathbb{Q}$ be an abelian extension of conductor $n = p_1^{e_1} \cdots p_t^{e_t}$ where $p_1 = 2$, and let $X \subseteq X^{(n)}$ be its associated group of Dirichlet characters.*

(a) *The natural projection* $\pi_\psi : X \to \prod_{i=1}^{t} \langle \psi_{p_i^{e_i}} \rangle$ *is surjective.*

(b) *Let* $e = e_1 = v_2(n)$. *Then* X_2 *is either* $X^{(2^e)} = \langle \omega_2 \rangle \times \langle \psi_{2^e} \rangle$, $\langle \psi_{2^e} \rangle$, *or* $\langle \omega_2 \psi_{2^e} \rangle$. *Note that* ψ_{2^e} *is trivial if* $e \leq 2$.

(c) $\langle X, \prod_{i=2}^{t} \langle \omega_{p_i} \rangle \rangle = X_2 \times \prod_{i=2}^{t} \langle \omega_{p_i} \rangle \times \prod_{j=2}^{t} \langle \psi_{p_j^{e_j}} \rangle = X_2 \times X^{(m)}$ *where* $m = n/2^e$.

Proof. Part (a) is essentially Lemma 1(a) in [10]. Part (b) follows from the fact that the natural projection $X \to \langle \psi_{2^e} \rangle$ and thus $X_2 \to \langle \psi_{2^e} \rangle$ must be surjective. By part (a), $\langle X, \prod_{i=2}^{t} \langle \omega_{p_i} \rangle \rangle$ contains all the Sylow-p subgroups of $X^{(n)} = \prod_{i=1}^{t} \langle \omega_{p_i} \rangle \times \prod_{j=1}^{t} \langle \psi_{p_j^{e_j}} \rangle$ for p odd; in particular, it contains $\prod_{j=2}^{t} \langle \psi_{p_j^{e_j}} \rangle$. Thus $\prod_{i=2}^{t} \langle \omega_{p_i} \rangle \times \prod_{j=2}^{t} \langle \psi_{p_j^{e_j}} \rangle \subseteq \langle X, \prod_{i=2}^{t} \langle \omega_{p_i} \rangle \rangle$. Part (c) now follows by noting that the image of the natural projection $\langle X, \prod_{i=2}^{t} \langle \omega_{p_i} \rangle \rangle \to X^{(2^e)}$ is X_2. ∎

3. Ramification

Definition 3.1. Throughout this paper, we take "tamely ramified" to mean "at most tamely ramified", i.e. "not wildly ramified".

Theorem 3.2. *Let* L/K *be an extension of number fields. Then* $T_{L/K}(\mathcal{O}_L)$ *is an ideal of* $\mathcal{O}_K$. *Suppose further that* L/K *is Galois, and let* $\mathfrak{p}$ *be a (non-zero) prime of* $\mathcal{O}_K$. *Then* $\mathfrak{p} \mid T_{L/K}(\mathcal{O}_L)$ *if and only if* $\mathfrak{p}$ *is wildly ramified in* L/K.

Proof. See [7]. Alternatively, this follows Lemma 2 in Section 5 of [4] and the fact that the extension of residue fields in question is separable. ∎

Corollary 3.3. *If* L/K *is a Galois extension of number fields, then* L/K *is tamely ramified if and only if* $T_{L/K}(\mathcal{O}_L) = \mathcal{O}_K$.

Proposition 3.4. *Let* K *be an abelian number field of conductor* n. *Then* $\mathbb{Q}^{(n)}/K$ *is tamely ramified at each prime lying above an odd rational prime.*

Proof. Let X be the group of Dirichlet characters associated to K and write $n = \prod_{i=1}^{t} p_i^{e_i}$ where $p_1 = 2$. Let M be the field corresponding to $\prod_{i=2}^{t} \langle \omega_{p_i} \rangle$. The extension MK/K is tamely ramified since the same is true of $M/\mathbb{Q}$. By Proposition 2.8(b) and (c) we have $[\mathbb{Q}^{(n)} : MK] = 1$ or 2, and so the result follows. ∎

Corollary 3.5. *Let* K *be an abelian number field of conductor* n. *Then wild ramification in* $\mathbb{Q}^{(n)}/K$ *can only occur in a degree* 2 *sub-extension (at primes above* 2).

Remark 3.6. The result of Proposition 3.4 appears to be well known (it is noted in [3], for example), but its proof and corollary are not easily found in the literature.

PROPOSITION 3.7. *Let K be an abelian number field of conductor $n = \prod_{i=1}^{t} p_i^{e_i}$ with associated character group X. Let $e = e_1 = v_2(n)$. Then the following are equivalent*:

(a) $X_2 = X^{(2^e)}$.
(b) $X^{(n)} = \langle X, \prod_{i=2}^{t} \langle \omega_{p_i} \rangle \rangle$.
(c) $\mathbb{Q}^{(n)}/K$ *is tamely ramified.*
(d) $T_{\mathbb{Q}^{(n)}/K}(\mathcal{O}^{(n)}) = \mathcal{O}_K$, *i.e.* $I(\mathbb{Q}^{(n)}/K) = 1$.

Proof. (a)⇔(b) follows from Proposition 2.8(c).
(c)⇔(d) follows from Corollary 3.3.
(a)⇔(c) follows from Proposition 3.4 and Theorem 2.6. ∎

REMARK 3.8. In particular, the equivalent conditions of Proposition 3.7 hold when $e \leq 2$. Furthermore, it can be shown that they also hold if there exists $d \in \mathbb{Z}$ with $d \equiv 3 \pmod 4$ and d square-free such that $\mathbb{Q}[\sqrt{d}] \subseteq K$.

PROPOSITION 3.9. *Let K be an abelian number field of conductor $n = \prod_{i=1}^{t} p_i^{e_i}$ with associated character group X and let K_2 be the field corresponding to X_2. Let $e = e_1 = v_2(n)$ and $m = n/2^e$. Define L to be the compositum $K_2\mathbb{Q}^{(m)}$, i.e. the field corresponding to $X_2 \times X^{(m)} \subseteq X^{(n)}$. When the equivalent conditions of Proposition* 3.7 *do* not *hold, the following statements are true*:

(a) X_2 *is either* $\langle \psi_{2^e} \rangle$ *or* $\langle \omega_2 \psi_{2^e} \rangle$.
(b) L/K *is tamely ramified.*
(c) $\mathbb{Q}^{(n)} = L[i]$, *i.e.* $\mathbb{Q}^{(n)}$ *is the field generated by adjoining a root of* $x^2 + 1$ *to* L.
(d) $[\mathbb{Q}^{(n)} : L] = [L[i] : L] = 2$.
(e) $\mathbb{Q}^{(n)}/L$ *is wildly ramified at the primes above* 2.
(f) $T_{L/K}(\mathcal{O}_L) = \mathcal{O}_K$.
(g) $\mathcal{O}_L = \mathcal{O}_{K_2} \otimes_{\mathbb{Z}} \mathcal{O}^{(m)}$.
(h) $I(\mathbb{Q}^{(n)}/L) = 2^r$ *for some* $r \geq 1$.

The situation is partially illustrated by the field diagram on p. 67.

Proof. (a) This follows from Proposition 2.8(b) and the hypothesis that Proposition 3.7(a) does not hold.

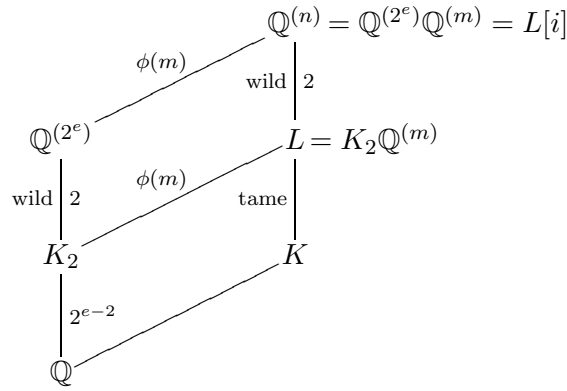
(b) Since $X_2 \times X^{(m)} = \langle X, \prod_{i=2}^{t} \langle \omega_{p_i} \rangle \rangle$ (Proposition 2.8(c)), the result follows by noting that $L = KM$ in the proof of Proposition 3.4.

(c) Since $\langle \omega_2 \rangle$ corresponds to $\mathbb{Q}[i]$, this follows from part (a).

(d) $[\mathbb{Q}^{(n)} : L] = [X^{(n)} : X_2 \times X^{(m)}] = [X^{(2^e)} : X_2] = 2$.

(e) This follows from part (b) and the hypothesis that Proposition 3.7(c) does not hold (i.e. $\mathbb{Q}^{(n)}/K$ is wildly ramified).

(f) By Corollary 3.3, this is equivalent to part (b).



(g) Since the discriminants of $\mathcal{O}_{K_2}$ and $\mathcal{O}^{(m)}$ are coprime, this follows from III.2.13 in [5].

(h) This follows from part (e) and Theorem 3.2. ∎

PROPOSITION 3.10. *Let L/K be an extension of absolutely abelian number fields of equal conductor, n. Then each prime above an odd rational prime is tamely ramified in L/K. Furthermore, L/K is wildly ramified at primes above* 2 *if and only if*

(a) *the equivalent conditions of Proposition* 3.7 *applied to L hold*;

(b) *the equivalent conditions of Proposition* 3.7 *applied to K do* not *hold.*

Proof. Since L/K is a sub-extension of $\mathbb{Q}^{(n)}/K$, the first statement follows from Proposition 3.4. The second statement holds because wild ramification in $\mathbb{Q}^{(n)}/K$ can only occur in a degree 2 sub-extension (Corollary 3.5), so L/K is wildly ramified (at primes above 2) if and only if $\mathbb{Q}^{(n)}/L$ is tamely ramified and $\mathbb{Q}^{(n)}/K$ is wildly ramified. ∎

4. Abelian number fields of conductor 2^e, $e \geq 3$. In this section, let $e \geq 3$, let ζ denote a primitive 2^eth root of unity and let $i = \zeta^{2^{e-2}}$.

PROPOSITION 4.1. *The cyclotomic field $\mathbb{Q}^{(2^e)}$ has precisely two proper fields of conductor 2^e:*

(a) $\mathbb{Q}(\zeta + \zeta^{-1})$, *with ring of integers* $\mathbb{Z}[\zeta + \zeta^{-1}]$;

(b) $\mathbb{Q}(i(\zeta + \zeta^{-1}))$, *with ring of integers* $\mathbb{Z}[i(\zeta + \zeta^{-1})]$.

Proof. Proposition 2.8(b) implies that any proper subfield of $\mathbb{Q}^{(2^e)}$ of conductor 2^e has associated character group either $\langle \psi_{2^e} \rangle$ or $\langle \omega_2 \psi_{2^e} \rangle$. It is straightforward to check that these correspond to $\mathbb{Q}(\zeta + \zeta^{-1})$ and $\mathbb{Q}(i(\zeta + \zeta^{-1}))$.

The ring of integers of $\mathbb{Q}(\zeta + \zeta^{-1})$ is $\mathbb{Z}[\zeta + \zeta^{-1}]$ by Proposition 2.16 of [12]. A slightly modified version of this argument, keeping track of real and imaginary parts, shows that $\mathbb{Q}(i(\zeta+\zeta^{-1}))$ has ring of integers $\mathbb{Z}[i(\zeta+\zeta^{-1})]$. ∎

PROPOSITION 4.2. *Let K_2 be a proper subfield of $\mathbb{Q}^{(2^e)}$ of conductor 2^e. Let $T = T_{\mathbb{Q}^{(2^e)}/K_2}$. In the cases of Proposition* 4.1,

(a) $T(\mathbb{Z}[\zeta]) = 2\mathbb{Z} \oplus (\zeta + \zeta^{-1}) \cdot \mathcal{O}_{K_2} = 2\mathbb{Z} \oplus (\zeta + \zeta^{-1}) \cdot \mathbb{Z}[\zeta + \zeta^{-1}]$;
(b) $T(\mathbb{Z}[\zeta]) = 2\mathbb{Z} \oplus i(\zeta + \zeta^{-1}) \cdot \mathcal{O}_{K_2} = 2\mathbb{Z} \oplus i(\zeta + \zeta^{-1}) \cdot \mathbb{Z}[i(\zeta + \zeta^{-1})]$.

In both cases, $I(\mathbb{Q}^{(2^e)}/K_2) = 2$.

Proof. (a) In this case, $K_2 = \mathbb{Q}(\zeta + \zeta^{-1})$, $\mathcal{O}_{K_2} = \mathbb{Z}[\zeta + \zeta^{-1}]$ and $\{1, \zeta\}$ is a basis for $\mathbb{Q}^{(2^e)}$ over K_2. The only non-trivial automorphism of $\mathbb{Q}^{(2^e)}$ over K_2 is induced by complex conjugation, and so for $a, b \in K_2$,

$$T(a + \zeta b) = (a + \zeta b) + (a + \zeta^{-1} b) = 2a + (\zeta + \zeta^{-1})b\,.$$

Since $\mathbb{Z} + \zeta \cdot \mathbb{Z}[\zeta + \zeta^{-1}] \subseteq \mathbb{Z}[\zeta]$, we therefore have $2\mathbb{Z} \oplus (\zeta + \zeta^{-1}) \cdot \mathbb{Z}[\zeta + \zeta^{-1}] \subseteq T(\mathbb{Z}[\zeta])$. However, $\mathbb{Z}[\zeta + \zeta^{-1}] = \mathbb{Z} \oplus (\zeta + \zeta^{-1}) \cdot \mathbb{Z}[\zeta + \zeta^{-1}]$, so

$$[\mathbb{Z}[\zeta + \zeta^{-1}] : 2\mathbb{Z} \oplus (\zeta + \zeta^{-1}) \cdot \mathbb{Z}[\zeta + \zeta^{-1}]] = 2$$

and by Proposition 3.9(h),

$$[\mathbb{Z}[\zeta + \zeta^{-1}] : T(\mathbb{Z}[\zeta])] = 2^r$$

for some $r \geq 1$. Hence $2\mathbb{Z} \oplus (\zeta + \zeta^{-1}) \cdot \mathbb{Z}[\zeta + \zeta^{-1}] = T(\mathbb{Z}[\zeta])$ (and in fact $r = 1$).

(b) In this case, $K_2 = \mathbb{Q}(i(\zeta + \zeta^{-1}))$ and $\mathcal{O}_{K_2} = \mathbb{Z}[i(\zeta + \zeta^{-1})]$. The proof is essentially the same as in part (a), noting that $\{1, i\zeta^{-1} = \zeta^{2^{e-2}-1}\}$ is a basis for $\mathbb{Q}^{(2^e)}$ over K_2 and that the non-trivial Galois conjugate of $i\zeta^{-1} = \zeta^{2^{e-2}-1}$ over K_2 is $i\zeta = \zeta^{2^{e-2}+1}$. ∎

PROPOSITION 4.3. *Consider the cases of Proposition* 4.1.

(a) *Let* $A = \{\zeta + \zeta^{-1}, \zeta^2 + \zeta^{-2}, \ldots, \zeta^{2^{e-2}-1} + \zeta^{-2^{e-2}+1}\}$. *Then* $T(\mathbb{Z}[\zeta]) = \mathrm{Span}_{\mathbb{Z}}(A \cup \{2\})$, $\mathcal{O}_{K_2} = \mathrm{Span}_{\mathbb{Z}}(A \cup \{1\})$ *and* $\mathrm{Gal}(K_2/\mathbb{Q})(A) \subseteq \pm A$.
(b) *Let* $B = \{i(\zeta + \zeta^{-1}), \zeta^2 + \zeta^{-2}, \ldots, i(\zeta^{2^{e-2}-1} + \zeta^{-2^{e-2}+1})\}$. *Then* $T(\mathbb{Z}[\zeta]) = \mathrm{Span}_{\mathbb{Z}}(B \cup \{2\})$, $\mathcal{O}_{K_2} = \mathrm{Span}_{\mathbb{Z}}(B \cup \{1\})$ *and* $\mathrm{Gal}(K_2/\mathbb{Q})(B) \subseteq \pm B$.

Proof. (a) $T(\mathbb{Z}[\zeta]) = \mathrm{Span}_{\mathbb{Z}}(A \cup \{2\})$ by Proposition 4.2 and a straightforward induction argument; that $\mathcal{O}_{K_2} = \mathrm{Span}_{\mathbb{Z}}(A \cup \{1\})$ follows easily. For any $\sigma \in \mathrm{Gal}(K_2/\mathbb{Q})$ and any $j \in \{1, \ldots, 2^{e-2} - 1\}$, $\sigma(\zeta^j + \zeta^{-j}) = \zeta^{jk} + \zeta^{-jk}$ for some $k \in (\mathbb{Z}/2^e\mathbb{Z})^\times$. However, any such $\zeta^{jk} + \zeta^{-jk}$ can be rewritten as $\pm(\zeta^r + \zeta^{-r})$ for some $r \in \{1, \ldots, 2^{e-2} - 1\}$ (note $\zeta^{2^{e-1}} = -1$). Part (b) is similar, noting that $\sigma(i) = \pm i$. ∎

5. Computing $I(L/K)$

PROPOSITION 5.1. *Let $L \subseteq M \subseteq N$ be a tower of Galois number fields such that N/M is tamely ramified. Then $I(N/L) = I(M/L)$.*

Proof. Since $T_{N/L}(\mathcal{O}_N) = T_{M/L}(T_{N/M}(\mathcal{O}_N))$ and $T_{N/M}(\mathcal{O}_N) = \mathcal{O}_M$ (by Corollary 3.3), we have that $T_{N/L}(\mathcal{O}_N) = T_{M/L}(\mathcal{O}_M)$ and so the result follows from the definition of I. ∎

COROLLARY 5.2. *Let L/K be a wildly ramified extension of absolutely abelian number fields of equal conductor, n. Then $I(L/K) = I(\mathbb{Q}^{(n)}/K)$.*

Proof. $\mathbb{Q}^{(n)}/L$ is tamely ramified since wild ramification in $\mathbb{Q}^{(n)}/K$ only occurs in a degree 2 sub-extension (Corollary 3.5) and L/K is wildly ramified. ∎

LEMMA 5.3. *Let K and M be abelian number fields of conductors k and m respectively. Suppose that k and m are relatively prime. Then*

$$T_{\mathbb{Q}^{(k)}M/KM}(\mathcal{O}_{\mathbb{Q}^{(k)}M}) = T_{\mathbb{Q}^{(k)}/K}(\mathcal{O}^{(k)}) \otimes_{\mathbb{Z}} \mathcal{O}_M.$$

Proof. The proof is straightforward once one observes that by III.2.13 in [5], we have $\mathcal{O}_{KM} = \mathcal{O}_K \otimes_{\mathbb{Z}} \mathcal{O}_M$ and $\mathcal{O}_{\mathbb{Q}^{(k)}M} = \mathcal{O}^{(k)} \otimes_{\mathbb{Z}} \mathcal{O}_M$. ∎

PROPOSITION 5.4. *Let K be an abelian number field of conductor n such that $\mathbb{Q}^{(n)}/K$ is wildly ramified. Let $m = n/2^e$ where $e = v_2(n)$ and let $L = K_2 \otimes_{\mathbb{Q}} \mathbb{Q}^{(m)} = K_2\mathbb{Q}^{(m)}$ (as in Proposition 3.9). Let $C = A$ or B from Proposition 4.3, as appropriate. Define*

$$D = T_{L/K}(\mathcal{O}^{(m)}) \quad \textit{and} \quad E = T_{L/K}(\mathrm{Span}_{\mathbb{Z}}(C) \otimes_{\mathbb{Z}} \mathcal{O}^{(m)}).$$

Then

$$\mathcal{O}_K = D \oplus E \quad \textit{and} \quad T_{\mathbb{Q}^{(n)}/K}(\mathcal{O}^{(n)}) = 2D \oplus E.$$

Proof. Note that $D \subseteq \mathcal{O}^{(m)} = \mathbb{Z} \otimes_{\mathbb{Z}} \mathcal{O}^{(m)}$ and $E \subseteq \mathrm{Span}_{\mathbb{Z}}(C) \otimes_{\mathbb{Z}} \mathcal{O}^{(m)}$, with the last containment following from Proposition 4.3 (note $\mathrm{Gal}(L/K)(C) \subseteq \mathrm{Gal}(K_2/\mathbb{Q})(C) \subseteq \pm C$). Since $\mathbb{Z} \cap \mathrm{Span}_{\mathbb{Z}}(C) = \{0\}$, we have $D \cap E = \{0\}$, which gives the last equality of

$$\begin{aligned}
\mathcal{O}_K &= T_{L/K}(\mathcal{O}_L) \quad \text{(Proposition 3.9(f))} \\
&= T_{L/K}(\mathcal{O}_{K_2} \otimes_{\mathbb{Z}} \mathcal{O}^{(m)}) \quad \text{(Proposition 3.9(g))} \\
&= T_{L/K}((\mathbb{Z} \oplus \mathrm{Span}_{\mathbb{Z}}(C)) \otimes_{\mathbb{Z}} \mathcal{O}^{(m)}) \quad \text{(Proposition 4.3)} \\
&= T_{L/K}((\mathbb{Z} \otimes_{\mathbb{Z}} \mathcal{O}^{(m)}) \oplus (\mathrm{Span}_{\mathbb{Z}}(C) \otimes_{\mathbb{Z}} \mathcal{O}^{(m)})) \\
&= D + E = D \oplus E.
\end{aligned}$$

Furthermore,

$$\begin{aligned}
T_{\mathbb{Q}^{(n)}/K}(\mathcal{O}^{(n)}) &= T_{L/K}(T_{\mathbb{Q}^{(n)}/L}(\mathcal{O}^{(n)})) = T_{L/K}(T_{\mathbb{Q}^{(n)}/L}(\mathcal{O}^{(2^e)} \otimes_{\mathbb{Z}} \mathcal{O}^{(m)})) \\
&= T_{L/K}(T_{\mathbb{Q}^{(2^e)}/K_2}(\mathcal{O}^{(2^e)}) \otimes_{\mathbb{Z}} \mathcal{O}^{(m)}) \quad \text{(Lemma 5.3)} \\
&= T_{L/K}((2\mathbb{Z} \oplus \mathrm{Span}_{\mathbb{Z}}(C)) \otimes_{\mathbb{Z}} \mathcal{O}^{(m)}) \quad \text{(Proposition 4.3)} \\
&= 2D \oplus E \quad \text{(as above).}
\end{aligned}$$

∎

REMARK 5.5. The key point in this proof is the use of Proposition 4.3 to show that $D \cap E = \{0\}$, and hence that the sums $D+E$ and $2D+E$ are direct.

THEOREM 5.6. *Under the hypotheses of Proposition* 5.4,

(a) $\mathcal{O}_K = \mathcal{O}_{K\cap\mathbb{Q}^{(m)}} \oplus T_{L/K}(\mathrm{Span}_{\mathbb{Z}}(C) \otimes_{\mathbb{Z}} \mathcal{O}^{(m)})$;

(b) $T_{\mathbb{Q}^{(n)}/K}(\mathcal{O}^{(n)}) = 2\mathcal{O}_{K\cap\mathbb{Q}^{(m)}} \oplus T_{L/K}(\mathrm{Span}_{\mathbb{Z}}(C) \otimes_{\mathbb{Z}} \mathcal{O}^{(m)})$;

(c) $I(\mathbb{Q}^{(n)}/K) = 2^{[K\cap\mathbb{Q}^{(m)}:\mathbb{Q}]}$.

Proof. Note that $\mathcal{O}_{K\cap\mathbb{Q}^{(m)}} \subseteq \mathcal{O}^{(m)} = \mathbb{Z}\otimes_{\mathbb{Z}} \mathcal{O}^{(m)}$ and, as shown in Proposition 5.4, $E \subseteq \mathrm{Span}_{\mathbb{Z}}(C) \otimes_{\mathbb{Z}} \mathcal{O}^{(m)}$. Since $\mathbb{Z} \cap \mathrm{Span}_{\mathbb{Z}}(C) = \{0\}$, we have $\mathcal{O}_{K\cap\mathbb{Q}^{(m)}} \cap E = \{0\}$ (this is essentially the same argument as that used to show $D \cap E = \{0\}$). Furthermore, $D = T_{L/K}(\mathcal{O}^{(m)}) \subseteq \mathcal{O}_{K\cap\mathbb{Q}^{(m)}}$ and $\mathcal{O}_{K\cap\mathbb{Q}^{(m)}} \subseteq \mathcal{O}_K = D \oplus E$, so $D = \mathcal{O}_{K\cap\mathbb{Q}^{(m)}}$. By Proposition 5.4, this gives parts (a) and (b). Now we have

$$\begin{aligned} I(\mathbb{Q}^{(n)}/K) &= [\mathcal{O}_K : T_{\mathbb{Q}^{(n)}/K}(\mathcal{O}^{(n)})] = [\mathcal{O}_{K\cap\mathbb{Q}^{(m)}} \oplus E : 2\mathcal{O}_{K\cap\mathbb{Q}^{(m)}} \oplus E] \\ &= [\mathcal{O}_{K\cap\mathbb{Q}^{(m)}} : 2\mathcal{O}_{K\cap\mathbb{Q}^{(m)}}] = 2^{\mathrm{rank}_{\mathbb{Z}}(\mathcal{O}_{K\cap\mathbb{Q}^{(m)}})} = 2^{[K\cap\mathbb{Q}^{(m)}:\mathbb{Q}]}, \end{aligned}$$

giving part (c). ∎

THEOREM 5.7. *Let L/K be an extension of absolutely abelian number fields of equal conductor, n. Let $e = v_2(n)$ and $m = n/2^e$. Then*

$$I(L/K) = \begin{cases} 2^{[K\cap\mathbb{Q}^{(m)}:\mathbb{Q}]} = 2^{[K:\mathbb{Q}]/2^{e-2}} & \text{if } L/K \text{ is wildly ramified,} \\ 1 & \text{otherwise.} \end{cases}$$

REMARK 5.8. Recall that criteria for wild ramification of L/K (which can only happen at primes above 2) are given in Proposition 3.10.

Proof. Suppose L/K is wildly ramified. Then $I(L/K) = I(\mathbb{Q}^{(n)}/K)$ by Corollary 5.2 and $I(\mathbb{Q}^{(n)}/K) = 2^{[K\cap\mathbb{Q}^{(m)}:\mathbb{Q}]}$ by Theorem 5.6. Noting that $[K_2 : \mathbb{Q}] = 2^{e-2}$ (see Proposition 3.9(a)) and that $\mathbb{Q}^{(m)}K = \mathbb{Q}^{(m)}K_2$, we have

$$\begin{aligned} [K \cap \mathbb{Q}^{(m)} : \mathbb{Q}] &= \frac{[\mathbb{Q}^{(m)} : \mathbb{Q}]}{[\mathbb{Q}^{(m)} : K \cap \mathbb{Q}^{(m)}]} = \frac{[\mathbb{Q}^{(m)} : \mathbb{Q}]}{[\mathbb{Q}^{(m)}K : K]} = \frac{[\mathbb{Q}^{(m)} : \mathbb{Q}]}{[\mathbb{Q}^{(m)}K_2 : K]} \\ &= \frac{[\mathbb{Q}^{(m)} : \mathbb{Q}][K : \mathbb{Q}]}{[\mathbb{Q}^{(m)}K_2 : \mathbb{Q}]} = \frac{[\mathbb{Q}^{(m)} : \mathbb{Q}][K : \mathbb{Q}]}{[\mathbb{Q}^{(m)} : \mathbb{Q}][K_2 : \mathbb{Q}]} = \frac{[K : \mathbb{Q}]}{[K_2 : \mathbb{Q}]} \\ &= \frac{[K : \mathbb{Q}]}{2^{e-2}}. \end{aligned}$$

In the case where L/K is tamely ramified, the result follows from Corollary 3.3. ∎

REMARK 5.9. It is clear that Theorem 5.7 agrees with the expressions for $I(L/K)$ in [6] (where $K\cap\mathbb{Q}^{(m)}$ is denoted $K_{n/2^e}$), and is in fact a sharpening

of these results since an exact value for $I(L/K)$ is given for *any* extension of abelian number fields L/K of equal conductor. Furthermore, the above result does not rely on Leopoldt's Theorem.

6. The adjusted trace map

DEFINITION 6.1. Let K be an abelian number field of conductor n. We define the *adjusted trace map*, $\widehat{T}_{\mathbb{Q}^{(n)}/K}$. If $\mathbb{Q}^{(n)}/K$ is tamely ramified, let $\widehat{T}_{\mathbb{Q}^{(n)}/K} = T_{\mathbb{Q}^{(n)}/K}$. Otherwise, let $m = n/2^e$ where $e = v_2(n)$ (recall that $e \geq 3$ in this case). Note that $\mathcal{O}^{(n)} = \mathcal{O}^{(2^e)} \otimes_{\mathbb{Z}} \mathcal{O}^{(m)}$ has $\mathbb{Z}$-basis $\{\zeta_{2^e}^i \otimes \zeta_m^j \mid 0 \leq i \leq 2^{e-1}-1,\ 0 \leq j \leq \phi(m)-1\}$. Define

$$\widehat{T}_{\mathbb{Q}^{(n)}/K}(\zeta_{2^e}^i \otimes \zeta_m^j) = \begin{cases} \frac{1}{2} T_{\mathbb{Q}^{(n)}/K}(\zeta_m^j) & \text{for } i = 0, \\ T_{\mathbb{Q}^{(n)}/K}(\zeta_{2^e}^i \otimes \zeta_m^j) & \text{for } 1 \leq i \leq 2^{e-1}-1, \end{cases}$$

and extend to a $\mathbb{Q}$-linear map $\mathbb{Q}^{(n)} \to K$.

PROPOSITION 6.2. $\widehat{T}_{\mathbb{Q}^{(n)}/K}(\mathcal{O}^{(n)}) = \mathcal{O}_K$.

Proof. If $\mathbb{Q}^{(n)}/K$ is tamely ramified, this is just Corollary 3.3. Otherwise, using the notation of Proposition 5.4, we see that

$$\widehat{T}_{\mathbb{Q}^{(n)}/K}(\alpha) = \begin{cases} \frac{1}{2} T_{\mathbb{Q}^{(n)}/K}(\alpha) & \text{if } T_{\mathbb{Q}^{(n)}/K}(\alpha) \in D, \\ T_{\mathbb{Q}^{(n)}/K}(\alpha) & \text{if } T_{\mathbb{Q}^{(n)}/K}(\alpha) \in E. \end{cases}$$

The result now follows immediately from Proposition 5.4. ∎

REMARK 6.3. It must be noted that the adjusted trace map of Definition 6.1 is in fact equivalent to the map defined in Lemma 3.4 of [11, p. 51], though it is expressed more explicitly here. Furthermore, it is shown to be surjective in [2]. However, the proof given here (Proposition 6.2) is very different.

LEMMA 6.4. *Let* $\widehat{T}_{\mathbb{Q}^{(n)}/K}(\zeta_n^k) = \varepsilon T_{\mathbb{Q}^{(n)}/K}(\zeta_n^k)$ *where* $\varepsilon = 1/2$ *or* 1. *Then*

$$\widehat{T}_{\mathbb{Q}^{(n)}/K}(\sigma(\zeta_n^k)) = \varepsilon T_{\mathbb{Q}^{(n)}/K}(\sigma(\zeta_n^k)) \quad \forall \sigma \in \mathrm{Gal}(\mathbb{Q}^{(n)}/\mathbb{Q}).$$

Proof. Write $\zeta_n^k = \zeta_{2^e}^i \otimes \zeta_m^j$ and use Definition 6.1. ∎

DEFINITION 6.5. Let L/K be a finite Galois extension with $\mathrm{Gal}(L/K) = G$. Then

$$\mathcal{A}_{L/K} := \{\gamma \in K[G] \mid \gamma(\mathcal{O}_L) \subseteq \mathcal{O}_L\}$$

is the *associated order* of L/K.

The following is a modified version of Lemma 6 in [3]. Note that we use both juxtaposition and the symbol $\cdot$ to denote the action of a group algebra on a field.

THEOREM 6.6. *Let K be an abelian number field of conductor n, and put $G = \mathrm{Gal}(\mathbb{Q}^{(n)}/\mathbb{Q})$, $H = \mathrm{Gal}(\mathbb{Q}^{(n)}/K)$. Let $\pi : \mathbb{Q}[G] \to \mathbb{Q}[G/H]$ denote the $\mathbb{Q}$-linear map induced by the natural projection $G \to G/H$. Suppose $\mathcal{O}^{(n)} = \mathcal{A}_{\mathbb{Q}^{(n)}/\mathbb{Q}} \cdot \alpha$ for some $\alpha \in \mathcal{O}^{(n)}$. Then $\mathcal{A}_{K/\mathbb{Q}} = \pi(\mathcal{A}_{\mathbb{Q}^{(n)}/\mathbb{Q}})$ and $\mathcal{O}_K = \mathcal{A}_{K/\mathbb{Q}} \cdot \beta$ where $\beta = \widehat{T}_{\mathbb{Q}^{(n)}/K}(\alpha)$.*

Proof. Write $G = \{g_1, \dots, g_r\}$ and $H = \{h_1, \dots, h_s\}$. Let $x \in \mathcal{A}_{\mathbb{Q}^{(n)}/\mathbb{Q}}$ and write

$$\begin{aligned} x &= x_1 g_1 + \cdots + x_r g_r && \text{where } x_i \in \mathbb{Q} \text{ and } g_i \in G, \\ \alpha &= y_1 + y_2\zeta + \cdots + y_r \zeta^{r-1} && \text{where } y_i \in \mathbb{Q} \text{ and } \zeta = \zeta_n. \end{aligned}$$

Then using Lemma 6.4, the $\mathbb{Q}$-linearity of $\widehat{T}_{\mathbb{Q}^{(n)}/K}$ and the fact that G is abelian, we have

$$\begin{aligned} \widehat{T}_{\mathbb{Q}^{(n)}/K}(x\alpha) &= \sum_{i=1}^{r} x_i \widehat{T}_{\mathbb{Q}^{(n)}/K}(g_i\alpha) = \sum_{i=1}^{r} x_i \sum_{j=1}^{r} y_j \widehat{T}_{\mathbb{Q}^{(n)}/K}(g_i\zeta^{j-1}) \\ &= \sum_{i=1}^{r} x_i \sum_{j=1}^{r} y_j \varepsilon_j T_{\mathbb{Q}^{(n)}/K}(g_i\zeta^{j-1}) = \sum_{i=1}^{r} x_i \sum_{j=1}^{r} y_j \varepsilon_j \sum_{k=1}^{s} h_k g_i \zeta^{j-1} \\ &= \sum_{i=1}^{r} x_i g_i \sum_{j=1}^{r} y_j \varepsilon_j \sum_{k=1}^{s} h_k \zeta^{j-1} = \sum_{i=1}^{r} x_i g_i \sum_{j=1}^{r} y_j \varepsilon_j T_{\mathbb{Q}^{(n)}/K}(\zeta^{j-1}) \\ &= \sum_{i=1}^{r} x_i g_i \sum_{j=1}^{r} y_j \widehat{T}_{\mathbb{Q}^{(n)}/K}(\zeta^{j-1}) = \sum_{i=1}^{r} x_i g_i \widehat{T}_{\mathbb{Q}^{(n)}/K}(\alpha) \\ &= x\widehat{T}_{\mathbb{Q}^{(n)}/K}(\alpha) \end{aligned}$$

where $\varepsilon_j = 1/2$ or 1, as appropriate. Thus

$$\begin{aligned} \mathcal{O}_K &= \widehat{T}_{\mathbb{Q}^{(n)}/K}(\mathcal{O}^{(n)}) \quad \text{(Proposition 6.2)} \\ &= \widehat{T}_{\mathbb{Q}^{(n)}/K}(\mathcal{A}_{\mathbb{Q}^{(n)}/\mathbb{Q}} \cdot \alpha) = \mathcal{A}_{\mathbb{Q}^{(n)}/\mathbb{Q}} \cdot \widehat{T}_{\mathbb{Q}^{(n)}/K}(\alpha) \\ &= \pi(\mathcal{A}_{\mathbb{Q}^{(n)}/\mathbb{Q}}) \cdot \beta \quad \text{(since } \beta \in K\text{).} \ \blacksquare \end{aligned}$$

REMARK 6.7. Unfortunately, this result cannot be easily extended to the case of relative extensions because $\widehat{T}_{\mathbb{Q}^{(n)}/K}$ is not K-linear for $K \neq \mathbb{Q}$.

COROLLARY 6.8. *The proof of Leopoldt's Theorem can be reduced to the cyclotomic case.*

We can now restate Leopoldt's Theorem (see [8], [10]) with the generator expressed as the image of an element under the adjusted trace map.

DEFINITION 6.9. For $n \in \mathbb{N}$, define the *radical* of n to be $r(n) = \prod_{p|n} p$.

DEFINITION 6.10. For $n \in \mathbb{N}$, define $\mathcal{D}(n) = \{d \in \mathbb{N} : r(n) \mid d \text{ and } d \mid n\}$.

THEOREM 6.11 (Leopoldt). *Let K be an abelian number field of conductor n, let ζ_n be a fixed primitive nth root of unity, and let*

$$\alpha = \widehat{T}_{\mathbb{Q}^{(n)}/K}\Big(\sum_{d\in\mathcal{D}(n)} \zeta_n^{(n/d)}\Big).$$

Then we have $\mathcal{O}_K = \mathcal{A}_{K/\mathbb{Q}} \cdot \alpha$, and so $\mathcal{O}_K$ is a free $\mathcal{A}_K$-module of rank 1.

Proof. By Corollary 6.8, the proof is reduced to the cyclotomic case, which is relatively straightforward. ∎

REMARK 6.12. In particular, the cyclotomic case follows from the version of Leopoldt's Theorem given in [10].

REMARK 6.13. The definition of $\mathcal{D}(n)$ in [10] is different from that given above. However, as noted in [9], Leopoldt's Theorem holds in either case. A routine computation shows that when $\mathcal{D}(n)$ is taken to be as in [10], α as defined above is equal to T defined in [10].

Acknowledgments. The author is grateful to Steven Chase, Ravi Ramakrishna, and Shankar Sen for useful conversations, and to Kurt Girstmair, Spencer Hamblen, and Jason Martin for looking at an initial draft of this paper. The computational algebra system Magma ([1]) was used to verify Theorem 5.7 for abelian number fields of conductor up to 176. The positive results from this "experiment" were psychologically very helpful in proving the theorem.

References

[1] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. 24 (1997), 235–265.

[2] T. Breuer, *Integral bases for subfields of cyclotomic fields*, Appl. Algebra Engrg. Comm. Comput. 8 (1997), 279–289.

[3] N. P. Byott and G. Lettl, *Relative Galois module structure of integers of Abelian fields*, J. Théor. Nombres Bordeaux 8 (1996), 125–141.

[4] A. Fröhlich, *Local fields*, in: Algebraic Number Theory, J. W. S. Cassels and A. Fröhlich (eds.), Thompson, Washington, D.C., 1967, 1–47.

[5] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge Univ. Press, Cambridge, 1991.

[6] K. Girstmair, *On the trace of the ring of integers of an abelian number field*, Acta Arith. 62 (1992), 383–389.

[7] M. James, *Class notes for Math 416, Galois Modules* (taught by L. R. McCulloh), http://www.math.uiuc.edu/∼mjames2/notes/.

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

[9] G. Lettl, *Stickelberger elements and cotangent numbers*, Expo. Math. 10 (1992), 171–182.

[10] —, *The ring of integers of an abelian number field*, J. Reine Angew. Math. 404 (1990), 162–170.

[11] K. Lux and H. Pahlings, *Computational aspects of representation theory of finite groups*, in: Representation Theory of Finite Groups and Finite-Dimensional Algebras, G. O. Michler and C. M. Ringel (eds.), Progr. Math. 95, Birkhäuser, Basel, 1991, 37–64.

[12] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer, New York, 1997.

Department of Mathematics
Malott Hall
Cornell University
Ithaca, NY 14853-4201, U.S.A.
E-mail: henri@math.cornell.edu
http://www.math.cornell.edu/∼henri

Received on 17.5.2005
and in revised form on 26.1.2006 (4985)