ACTA ARITHMETICA
LXII.4 (1992)

On the trace of the ring of integers of an abelian number field

by

Kurt Girstmair (Innsbruck)

1. Introduction. Let K, L be algebraic number fields with $K \subseteq L$, and $\mathcal{O}_K$, $\mathcal{O}_L$ their respective rings of integers. We consider the trace map

$$T = T_{L/K} : L \to K$$

and the $\mathcal{O}_K$-ideal $T(\mathcal{O}_L) \subseteq \mathcal{O}_K$. By $I(L/K)$ we denote the *group index* of $T(\mathcal{O}_L)$ in $\mathcal{O}_K$ (i.e., the norm of $T(\mathcal{O}_L)$ over $\mathbb{Q}$). It seems to be difficult to determine $I(L/K)$ in the general case. If K and L are absolutely abelian number fields, however, we obtain a fairly explicit description of the number $I(L/K)$. This is a consequence of our description of the Galois module structure of $T(\mathcal{O}_L)$ (Theorem 1). The case of equal conductors $f_K = f_L$ of the fields K, L is of particular interest. Here we show that $I(L/K)$ is a certain power of 2 (Theorems 2, 3, 4).

2. Basic notions. Let $d \in \mathbb{N}$ and $\xi_d = e^{2\pi i/d}$. Then $\mathbb{Q}_d = \mathbb{Q}(\xi_d)$ is the dth cyclotomic field. If K is an absolutely abelian number field, we put $K_d = K \cap \mathbb{Q}_d$. By

$$\xi_{d,K} = T_{\mathbb{Q}_d/K_d}(\xi_d)$$

we denote the trace of the root of unity ξ_d over K_d. Let $G_K = \mathrm{Gal}(K/\mathbb{Q})$ be the Galois group of K over $\mathbb{Q}$ and $\mathbb{Z}G_K$ its integral group ring. For a number $m \in \mathbb{N}$ write

$$m^* = \prod \{p\,;\, p \mid m\}\,,$$

i.e., m^* is the maximal square-free divisor of m. Let, in particular, $m = f_K$ be the conductor of K. Then $\mathcal{O}_K$ has a uniquely determined decomposition into indecomposable $\mathbb{Z}G_K$-modules, viz.

$$\mathcal{O}_K = \bigoplus_{m^* \mid d \mid m} \mathbb{Z}G_K \xi_{d,K} \tag{1}$$

(see [3], [4]).

For simplicity we write $\mathcal{O}_m = \mathcal{O}_{\mathbb{Q}_m}$ and $G_m = G_{\mathbb{Q}_m}$. If k is an integer prime to m, we define $\sigma_k \in G_m$ by

$$\sigma_k(\xi_m) = \xi_m^k .$$

Then $G_m = \{\sigma_k ; 1 \le k \le m,\ (k,m) = 1\}$.

Suppose now that both fields K, L, $K \subseteq L$, are abelian. Let X_K, X_L be the character groups of G_K, G_L, resp. The restriction map

$$(\ )_K : G_L \to G_K : \sigma \mapsto \sigma_K = \sigma|_K$$

is surjective, and it defines an injection

$$X_K \to X_L : \chi \mapsto \chi \circ (\ )_K .$$

Hence we consider X_K as a subgroup of X_L. For a character $\chi \in X_K$ let f_χ be the conductor of χ. Then f_χ divides $m = f_K$. Moreover, if $d \in \mathbb{N}$, we write

$$[d] = \{c \in \mathbb{N} ; c \mid d,\ d/c \text{ square-free, } (c, d/c) = 1\} .$$

There is a decomposition of X_K that corresponds to (1) in a canonical way (see [1]). Indeed,

$$X_K = \dot{\bigcup_{m^* \mid d \mid m}} \{\chi \in X_K ; f_\chi \in [d]\} ,$$

and

$$\operatorname{rank}_{\mathbb{Z}}(\mathbb{Z}G_K \xi_{d,K}) = |\{\chi \in X_K ; f_\chi \in [d]\}| \tag{2}$$

for each d, $m^* \mid d \mid m$.

3. Description of $T_{L/K}(\mathcal{O}_L)$ and $I(L/K)$. Let the above notations hold, in particular, let $K \subseteq L$ be abelian number fields with conductors $f_K = m$, $f_L = n$. If d is a divisor of m, write

$$\widehat{d} = d \prod \{p ;\ p \text{ prime},\ p \mid n,\ p \nmid m\} .$$

THEOREM 1. *In the above situation the following assertions hold*:

$$T_{L/K}(\mathcal{O}_L) = \bigoplus_{m^* \mid d \mid m} \mathbb{Z}G_K h_d \xi_{d,K} , \tag{i}$$

with $h_d = [L : K]/[L_{\widehat{d}} : K_d]$; h_d *is an integer whenever* $\xi_{d,K} \neq 0$.

$$I(L/K) = \prod_{m^* \mid d \mid m} h_d^{r_d} , \tag{ii}$$

with $r_d = \operatorname{rank}_{\mathbb{Z}}(\mathbb{Z}G_K \xi_{d,K}) = |\{\chi \in X_K ; f_\chi \in [d]\}|$.

COROLLARY. *Let* $m \mid n$. *For* $K = \mathbb{Q}_m$, $L = \mathbb{Q}_n$,

$$T(\mathcal{O}_n) = n/\widehat{m} \cdot \mathcal{O}_m; \tag{i}$$

(ii) $$I(\mathbb{Q}_n/\mathbb{Q}_m) = (n/\widehat{m})^{\varphi(m)}\,,$$

φ denoting Euler's function.

We turn to the special case of *equal* conductors, so $K \subseteq L$ and $f_K = f_L = n$. Write

$$H = \mathrm{Gal}(L/K)\,, \qquad H_d = \mathrm{Gal}(L/L_d)\,, \qquad d \mid n\,.$$

Suppose, moreover, that q is a prime number and $[L:K]$ a power of q. Put $e = \max\{k\,;2^k \mid n\}$ (i.e., the 2-exponent of n). If $e \ge 1$, define $j, l \in \{1, \ldots, n\}$ by the congruences

$$\begin{aligned} &j \equiv -1 \bmod 2^e\,, \qquad l \equiv -1 + 2^{e-1} \bmod 2^e\,,\\ &j \equiv l \equiv 1 \bmod n/2^e\,. \end{aligned}$$

THEOREM 2. *In this situation the following assertions are equivalent*:

(i) $I(L/K) > 1$;

(ii) $q = 2$, $e \ge 3$, *and either* $H \cap H_{n^*} = \langle \sigma_{j,L}\rangle \ne \{\mathrm{id}\}$ *or* $H \cap H_{n^*} = \langle \sigma_{l,L}\rangle \ne \{\mathrm{id}\}$.

Remark. Let (K, L_{n^*}) be the composite of the subfields K, L_{n^*} of L. Then assertion (ii) can be restated as

(iii) $q = 2$, $e \ge 3$, $[L:(K, L_{n^*})] = 2$, and either $\mathrm{Gal}(L/(K, L_{n^*})) = \langle \sigma_{j,L}\rangle$ or $\mathrm{Gal}(L/(K, L_{n^*})) = \langle \sigma_{l,L}\rangle$.

This is clear by Galois theory.

THEOREM 3. *Let $K \subseteq L$, $f_K = f_L = n$, $e \ge 3$, and let $[L:K]$ be a power of 2. Suppose that the equivalent conditions* (i), (ii) *of Theorem* 2 *are satisfied. If $H \cap H_{n^*} = \langle \sigma_{j,L}\rangle$ put $k = j$, otherwise put $k = l$. Then the numbers h_d of Theorem* 1 *take the following values*:

$$h_d = \begin{cases} 2 & \textit{if } \sigma_{k,L_d} = \mathrm{id},\\ 1 & \textit{else.} \end{cases}$$

In particular, $h_d = 2$ *for all d with* $n^* \mid d \mid n/2^{e-1}$, *and*

$$2^{[K_{n/2^e}:\mathbb{Q}]} \mid I(L/K) \mid 2^{[K:\mathbb{Q}]}\,.$$

COROLLARY. *In the situation of Theorem* 3 *let $L = \mathbb{Q}_n$. Then*

$$T_{\mathbb{Q}_n/K}(\mathcal{O}_n) = 2 \cdot \mathcal{O}_{K_{n/2^e}} \oplus \bigoplus \{\mathbb{Z}G_K\xi_{d,K}\,; n^* \mid d \mid n\,,\ 4 \mid d\}$$

and $I(L/K) = 2^{[K_{n/2^e}:\mathbb{Q}]}$.

Theorems 2 and 3 also yield a description of $T(\mathcal{O}_L)$ and $I(L/K)$ for *arbitrary* abelian number fields $K \subseteq L$ of equal conductor n. As above, let $H = \mathrm{Gal}(L/K)$ and $H_{(p)}$ be the p-Sylow group of H (p prime). Let $L^{(2)}$ be the fixed field of $\prod\{H_{(p)}\,; p \ne 2\}$ (thus $\mathrm{Gal}(L^{(2)}/K)$ is isomorphic to $H_{(2)}$).

THEOREM 4. *In the above situation*,

$$T_{L/K}(\mathcal{O}_L) = T_{L^{(2)}/K}(\mathcal{O}_{L^{(2)}})\,.$$

Hence the structure of $T_{L/K}(\mathcal{O}_L)$ *and the value of* $I(L/K)$ *are given by Theorems* 2 *and* 3 *applied to* $K \subseteq L^{(2)}$.

4. Proofs

Proof of Theorem 1. First we show

$$T(\mathcal{O}_L) = \bigoplus_{n^* \,|\, c \,|\, n} \mathbb{Z}G_K h_c \xi_{c,K}\,, \tag{3}$$

with $h_c = [L:K]/[L_c:K_c]$. Indeed, if $n^* \,|\, c \,|\, n$, then

$$T_{L/K_c}(\xi_{c,L}) = T_{K/K_c}(T_{L/K}(\xi_{c,L})) = [K:K_c]T_{L/K}(\xi_{c,L})\,,$$

and

$$T_{L/K_c}(\xi_{c,L}) = T_{L_c/K_c}(T_{L/L_c}(\xi_{c,L})) = [L:L_c]\xi_{c,K}\,.$$

This yields

$$T_{L/K}(\xi_{c,L}) = ([L:L_c]/[K:K_c])\xi_{c,K} = h_c\xi_{c,K}\,.$$

Hence $T(\mathbb{Z}G_L\xi_{c,L}) = \mathbb{Z}G_L T(\xi_{c,L}) = \mathbb{Z}G_L h_c \xi_{c,K} = \mathbb{Z}G_K h_c \xi_{c,K}$. We obtain

$$T(\mathcal{O}_L) = \sum_{n^* \,|\, c \,|\, n} \mathbb{Z}G_K h_c \xi_{c,K}\,.$$

This sum, however, is direct, due to $\mathbb{Z}G_K h_c \xi_{c,K} \subseteq \mathbb{Z}G_L \xi_{c,L}$ and formula (1). Therefore (3) holds. For the time being, fix c with $n^* \,|\, c \,|\, n$, and put $d = (c, m)$. Then $K_d = K_c$ and

$$\xi_{c,K} = T_{\mathbb{Q}_d/K_d}(T_{\mathbb{Q}_c/\mathbb{Q}_d}(\xi_c))\,. \tag{4}$$

Moreover, formula (34) in [1] yields

$$T_{\mathbb{Q}_c/\mathbb{Q}_d}(\xi_c) = \begin{cases} \pm\sigma_k(\xi_d) & \text{if } d \in [c], \\ 0 & \text{otherwise,} \end{cases} \tag{5}$$

k being a certain number prime to d. From (4), (5) we conclude that $\xi_{c,K} \neq 0$ only if $d \in [c]$, i.e., $c = \widehat{d}$. In this case $h_c = h_d$, and (4), (5) imply $\mathbb{Z}G_K\xi_{c,K} = \mathbb{Z}G_K\xi_{d,K}$. We obtain from (3)

$$T(\mathcal{O}_L) = \bigoplus_{m^* \,|\, d \,|\, m} \mathbb{Z}G_K h_d \xi_{d,K}\,.$$

Observe that $\mathbb{Z}G_K h_d \xi_{d,K} \subseteq \mathcal{O}_K$, $m^* \,|\, d \,|\, m$. Hence (1) implies $h_d\mathbb{Z}G_K\xi_{d,K} \subseteq \mathbb{Z}G_K\xi_{d,K}$. If $\xi_{d,K} \neq 0$, $\mathbb{Z}G_K\xi_{d,K}$ is a free $\mathbb{Z}$-module of $\mathbb{Z}$-rank ≥ 1, and h_d must be an integer. This concludes the proof of (i). Assertion (ii) follows from (i), (1), and (2). ∎

P r o o f o f t h e C o r o l l a r y (of Theorem 1). For each d with $m^* \mid d \mid m$ the number h_d equals $\varphi(n)\varphi(d)/(\varphi(m)\varphi(\widehat{d})) = \varphi(n)/\varphi(\widehat{m}) = n/\widehat{m}$. Since h_d does not depend on the choice of d, the assertions follow from (1). ■

P r o o f o f T h e o r e m 2. Let $n^* \mid d \mid n$. By Galois theory, $\mathrm{Gal}(L/K_d) = \mathrm{Gal}(L/K \cap L_d) = \langle H, H_d \rangle = HH_d$. Moreover, $|HH_d| = |H|\,|H_d|/|H \cap H_d|$. After a short calculation this yields

$$h_d = |H \cap H_d|\,. \tag{6}$$

Suppose that (ii) holds. Then $h_{n^*} = 2$, by (6). Formula (1) shows that

$$\mathcal{O}_{K_{n^*}} = \mathbb{Z}G_K\xi_{n^*,\,K}\,,$$

which yields $r_{n^*} = \mathrm{rank}_{\mathbb{Z}}\,\mathcal{O}_{K_{n^*}} \geq 1$. From Theorem 1(ii), we infer that $I(L/K) > 1$.

Conversely, assume (i). We shall show in the subsequent steps (a)–(d) that (ii) holds.

(a) There is a number d, $n^* \mid d \mid n$, such that $H \cap H_d \neq \{\mathrm{id}\}$. Because of $H_d \subseteq H_{n^*}$, $H \cap H_{n^*} \neq \{\mathrm{id}\}$, too. Since $|H|$ is a power of q, $H \cap H_{n^*}$ is a non-trivial subgroup of the q-Sylow group $H_{n^*,q}$ of H_{n^*}.

(b) Suppose that $q \neq 2$ or $q = 2$, $e \leq 2$. We show that $H_{n^*,q}$ is a cyclic group. Put

$$J = \mathrm{Gal}(\mathbb{Q}_n/L)\,, \qquad J_{n^*} = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}_{n^*})\,.$$

Then $JJ_{n^*} = \mathrm{Gal}(\mathbb{Q}_n/L_{n^*})$. The restriction map

$$(\ )_L : \mathrm{Gal}(\mathbb{Q}_n/L_{n^*}) \to \mathrm{Gal}(L/L_{n^*}) = H_{n^*} : \sigma \mapsto \sigma_L$$

is surjective; because of $(J)_L = 1$ we get $H_{n^*} = (JJ_{n^*})_L = (J_{n^*})_L$. We assert that the q-Sylow group $J_{n^*,q}$ of J_{n^*} is cyclic. Indeed, the Chinese Remainder Theorem yields a canonical isomorphism

$$\psi : G_n \to \prod_{p \mid n} (\mathbb{Z}/p^{e_p}\mathbb{Z})^\times\,,$$

$e_p = \max\{k\,; p^k \mid n\}$ being the p-exponent of n. But ψ maps J_{n^*} onto $\prod_{p \mid n}\{\overline{k}\,; k \equiv 1 \bmod p\}$, whose q-Sylow group is

$$\{\overline{k}\,; k \equiv 1 \bmod q\} \times \prod_{p \neq q}\{\overline{1}\}\,.$$

Since $q \geq 3$ or $q = 2$, $e \leq 2$, this group is cyclic.

(c) Again suppose $q \neq 2$ or $q = 2$, $e \leq 2$. If $e_q = 1$, $|J_{n^*}| = n/n^* \not\equiv 0 \bmod q$; thus $|H_{n^*}| \not\equiv 0 \bmod q$ and $|H \cap H_{n^*}| \not\equiv 0 \bmod q$, contrary to step (a). Hence assume $e_q \geq 2$. Then $H_{n/q} \subseteq H_{n^*}$. Furthermore, $|J_{n/q}| = q$, which gives $|H_{n/q}| \mid q$ and $H_{n/q} \subseteq H_{n^*,q}$. However, $H_{n^*,q}$ is cyclic by step (b), and $H \cap H_{n^*}$ is a non-trivial subgroup, by (a). This requires $H_{n/q} \subseteq H \cap H_{n^*} \subseteq H$. Therefore $K \subseteq L_{n/q}$, which is impossible, due to $f_K = n$.

(d) Step (c) has shown that $q=2$ and $e\geq 3$. Let $\sigma_{k,L}\in H\cap H_{n^*}$, $\sigma_{k,L}\neq \mathrm{id}$. Since there is an epimorphism $(\ )_L : J_{n^*,2}\to H_{n^*,2}$, we can assume that $\sigma_k\in J_{n^*,2}$, i.e., $k\equiv 1 \bmod n/2^e$. It is well-known that k satisfies one of the congruences

$$k\equiv \pm 5^b \bmod 2^e\,,\qquad 1\leq b\leq 2^{e-2}$$

(see, e.g., [2], p. 43). Suppose that $b<2^{e-2}$. Then there is a divisor c of 2^{e-3} such that

$$5^{bc}\equiv 1+2^{e-1}\bmod 2^e$$

(*loc. cit.*). We get $k^c\equiv(\pm1)^c(1+2^{e-1})\bmod 2^e$. If $c>1$, this yields $\sigma_k^c\in J_{n/2}\setminus\{\mathrm{id}\}$. But $|J_{n/2}|=2$, thus $J_{n/2}=\langle\sigma_k^c\rangle$ and $H_{n/2}=\langle\sigma_{k,L}^c\rangle\subseteq H$, contrary to $f_K=n$. Therefore $c=1$, and $k\equiv\pm(1+2^{e-1})\bmod 2^e$. The case $k\equiv 1+2^{e-1}\bmod 2^e$ is impossible again. Altogether, we have shown that $b=2^{e-2}$, $k\equiv -1\bmod 2^e$, or that $k\equiv -1-2^{e-1}\equiv -1+2^{e-1}\bmod 2^e$. This implies $H\cap H_{n^*}=\langle\sigma_{j,L}\rangle\neq\{\mathrm{id}\}$ or $H\cap H_{n^*}=\langle\sigma_{l,L}\rangle\neq\{\mathrm{id}\}$. ∎

Proof of Theorem 3 and the Corollary. Let k be as assumed and $H\cap H_{n^*}=\langle\sigma_{k,L}\rangle\neq\mathrm{id}$. Consider a number d with $n^*\,|\,d\,|\,n$. Then $H\cap H_d\subseteq H\cap H_{n^*}$; by (6) we get $h_d\neq 1$ if and only if $\sigma_{k,L}\in H_d$, which means $\sigma_{k,L_d}=\mathrm{id}$. Obviously this is the case if $4\nmid d$. We have shown

$$\begin{aligned}2\cdot\mathcal{O}_k &\subseteq T(\mathcal{O}_L)\\ &\subseteq \bigoplus\{\mathbb{Z}G_K 2\xi_{d,K}\,;n^*\,|\,d\,|\,n/2^{e-1}\}\oplus\bigoplus\{\mathbb{Z}G_K\xi_{d,K}\,;2n^*\,|\,d\,|\,n\}\\ &=2\cdot\mathcal{O}_{K_{n/2^e}}\oplus\bigoplus\{\mathbb{Z}G_K\xi_{d,K};2n^*\,|\,d\,|\,n\}\,.\end{aligned}$$

This gives

$$2^{[K_{n/2^e}:\mathbb{Q}]}\,|\,I(L/K)\,|\,2^{[K:\mathbb{Q}]}\,.$$

In the case $L=\mathbb{Q}_n$, the last inclusion can be replaced by equality. ∎

Proof of Theorem 4. We have $[L:L^{(2)}]=|H|/|H_{(2)}|$, which is an odd number. For this reason there exists a chain of intermediate fields

$$L^{(2)}\subseteq\ldots\subseteq L'\subseteq L''\subseteq\ldots\subseteq L$$

such that $[L'':L']$ is an odd prime power. All of these fields have conductor n. So Theorem 2 implies $T_{L''/L'}(\mathcal{O}_{L''})=\mathcal{O}_{L'}$, whence $T_{L/L^{(2)}}(\mathcal{O}_L)=\mathcal{O}_{L^{(2)}}$. Finally,

$$T_{L/K}(\mathcal{O}_L)=T_{L^{(2)}/K}(T_{L/L^{(2)}}(\mathcal{O}_L))=T_{L^{(2)}/K}(\mathcal{O}_{L^{(2)}})\,.\ ∎$$

References

[1] K. Girstmair, *Dirichlet convolution of cotangent numbers and relative class number formulas*, Monatsh. Math. 110 (1990), 231–256.

[2] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, New York 1982.

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

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

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT INNSBRUCK
TECHNIKERSTR. 25/7
A-6020 INNSBRUCK, ÖSTERREICH

Received on 10.2.1992
and in revised form on 25.3.1992 (2228)