ACTA ARITHMETICA
LXII.3 (1992)

On the branch order of the ring of integers of an abelian number field

by

Kurt Girstmair (Innsbruck)

1. Introduction. Let K be an (absolutely) abelian number field of conductor n, G_K its Galois group over $\mathbb{Q}$, and $\mathcal{O}_K$ the ring of integers of K. By $\mathbb{Q}G_K$ we denote the rational and by $\mathbb{Z}G_K$ the integral group ring of G_K. The field K is a $\mathbb{Q}G_K$-module via the usual action of G_K on K. Let

$$R_K = \{\alpha \in \mathbb{Q}G_K\,;\, \alpha\mathcal{O}_K \subseteq \mathcal{O}_K\}\,.$$

The set R_K is a subring of $\mathbb{Q}G_K$ that contains $\mathbb{Z}G_K$. As a $\mathbb{Z}G_K$-module, $\mathcal{O}_K$ is isomorphic to R_K. In accordance with Leopoldt [1], we call R_K the *branch order* ("Zweigordnung") of $\mathcal{O}_K$. Let us now describe the order R_K, i.e., the structure of $\mathcal{O}_K$ as a Galois module.

The letter p always means a prime number. We put

$$n^* = \{p\,;\, p \mid n\}\,.$$

Moreover, if d is a natural number, let

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

The set $[d]$ is called the *branch class* of d, and it is easy to see that

$$\{d\,;\, d \mid n\} = \dot{\bigcup}\{[d]\,;\, n^* \mid d \mid n\} \tag{1}$$

(disjoint union). By X_K we denote the character group of G_K. If $\chi \in X_K$, f_χ means the conductor of χ. Moreover, for $\alpha = \sum\{a_\sigma\sigma\,;\, \sigma \in G_K\} \in \mathbb{Q}G_K$ we put

$$\chi(\alpha) = \sum a_\sigma \chi(\sigma)\,.$$

For each divisor d of n with $n^* \mid d$ there is a uniquely determined element $\varepsilon_{d,K} \in \mathbb{Q}G_K$ with

$$\chi(\varepsilon_{d,K}) = \begin{cases} 1 & \text{if } f_\chi \in [d], \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

From (1) and (2) one sees that $(\varepsilon_{d,K}\,;n^*\,|\,d\,|\,n)$ is a complete system of orthogonal idempotents of $\mathbb{Q}G_K$. Hence

$$\mathbb{Q}G_K=\bigoplus\{\mathbb{Q}G_K\varepsilon_{d,K}\,;n^*\,|\,d\,|\,n\}\,,$$

and it is known that

$$R_K=\bigoplus\{\mathbb{Z}G_K\varepsilon_{d,K}\,;n^*\,|\,d\,|\,n\} \tag{3}$$

(cf. [1], [2]). For this reason we call $\varepsilon_{d,K}$ the *branch idempotent* of d, $n^*\,|\,d\,|\,n$. The $\mathbb{Z}G_K$-modules $\mathbb{Z}G_K\varepsilon_{d,K}$ are indecomposable, and there does not exist a decomposition of R_K into indecomposable $\mathbb{Z}G_K$-submodules different from (3). Of course, $\varepsilon_{d,K}$ can be written as

$$\varepsilon_{d,K}=\sum\{c_\sigma\sigma\,;\sigma\in G\}\,,$$

with $c_\sigma\in\mathbb{Q}$. It seems that an explicit formula for the coefficients c_σ has not been given so far. Indeed, in the previous papers [1], [2] the branch idempotent $\varepsilon_{d,K}$ only appears in the form

$$\varepsilon_{d,K}=|G_K|^{-1}\sum\{\chi(\sigma)\sigma\,;\sigma\in G_K,\ f_\chi\in[d]\}\,,$$

which immediately follows from (2). In this note we give an explicit formula for the numbers c_σ, $\sigma\in G_K$, in the case $K=\mathbb{Q}_n=\mathbb{Q}(e^{2\pi i/n})$. We shall see that this also yields an explicit description of $\varepsilon_{d,K}$ in the general case.

2. The main result. The Galois group G_n of $\mathbb{Q}_n$ over $\mathbb{Q}$ has the shape

$$G_n=\{\sigma_k\,;1\le k\le n,\ (k,n)=1\}\,,$$

where σ_k is defined by

$$\sigma_k(e^{2\pi i/n})=e^{2\pi ik/n}\,.$$

It what follows we write ε_d instead of $\varepsilon_{d,\mathbb{Q}_n}$. Suppose now that K is an arbitrary abelian number field with conductor n.

The restriction map

$$\mathrm{res}:\mathbb{Q}G_n\to\mathbb{Q}G_K$$

is $\mathbb{Q}$-linear and defined by $\mathrm{res}(\sigma_k)=\sigma_k\,|\,_K$. We note the following

PROPOSITION. *Let n be the conductor of K, and let $n^*\,|\,d\,|\,n$. Then*

$$\mathrm{res}(\varepsilon_d)=\varepsilon_{d,K}\,.$$

Proof. Take a character $\chi\in X_K$. Then $\widehat{\chi}=\chi\circ\mathrm{res}:\mathbb{Q}G_n\to\mathbb{C}$ is a character of G_n with conductor f_χ. Therefore

$$\chi(\mathrm{res}(\varepsilon_d))=\widehat{\chi}(\varepsilon_d)=\begin{cases}1 & \text{if } f_\chi\in[d],\\ 0 & \text{otherwise.}\end{cases}$$

Thus $\mathrm{res}(\varepsilon_d)$ satisfies condition (2), which means $\mathrm{res}(\varepsilon_d)=\varepsilon_{d,K}$. ■

Due to the Proposition, $\varepsilon_{d,K}$ is explicitly known if ε_d is. Let us therefore describe ε_d. As above, let $n^* \mid d \mid n$ and suppose that $k \in \mathbb{N}$, $1 \le k \le n-1$, $(k,n)=1$. We define

$$d_k = (d, k-1)$$

and, provided that $n^* \mid k-1$,

$$r_k = \prod \{p\,;p \mid d_k/n^*,\ p \nmid d/d_k\}\,.$$

THEOREM. *In the above situation write*

$$\varepsilon_d = \sum \{c_k \sigma_k\,; 1 \le k \le n,\ (k,n)=1\}$$

with $c_k \in \mathbb{Q}$ *for all* k. *Let* $\varphi : \mathbb{N} \to \mathbb{N}$ *be the Euler function and* $\mu : \mathbb{N} \to \mathbb{N}$ *the Möbius function. Then*

$$c_k = \begin{cases} \dfrac{\mu(d/d_k) d_k \varphi(r_k)}{n r_k} & \text{if } n^* \mid k-1, \\ 0 & \text{otherwise.} \end{cases}$$

The coefficient c_k of the branch idempotent can also be described in a somewhat different way. For $m \in \mathbb{N} \cup \{0\}$ put

$$v_p(m) = \begin{cases} \max\{j\,; p^j \mid m\} & \text{if } m \ne 0, \\ \infty & \text{otherwise} \end{cases}$$

(so $v_p(m)$ is the *p-exponent* of m).

COROLLARY. *In the context of the Theorem,* $c_k = 0$ *if* $n^* \nmid k-1$ *or if there is a* p *with* $v_p(d) \ge v_p(k-1)+2$. *Otherwise*

$$c_k = \frac{d}{n} \prod \left\{1 - \frac{1}{p}\,; 2 \le v_p(d) \le v_p(k-1)\right\} \times \prod \left\{-\frac{1}{p}\,; v_p(d) > v_p(k-1)\right\}.$$

Proof of the Theorem. If $n^* \mid d \mid n$ put

$$\gamma_d = \sum \{\varepsilon_q\,; n^* \mid q \mid d\}\,. \tag{4}$$

For a character $\chi \in X_n = X_{\mathbb{Q}_n}$,

$$\chi(\gamma_d) = \begin{cases} 1 & \text{if } f_\chi \mid d, \\ 0 & \text{otherwise.} \end{cases} \tag{5}$$

This follows from (1) and (2). The condition (5) determines γ_d uniquely.

Put

$$\widetilde{\gamma}_d = \frac{\varphi(d)}{\varphi(n)} \sum \{\sigma_k\,; k \equiv 1 \bmod d\}\,. \tag{6}$$

Let $\chi \in X_n$ be such that $f_\chi \nmid d$. Then there exists a number j, $1 \le j \le n$, $j \equiv 1 \bmod d$, with $\chi(\sigma_j) \ne 1$. But $\widetilde{\gamma}_d = \sigma_j \widetilde{\gamma}_d$, hence

$$\chi(\widetilde{\gamma}_d) = \chi(\sigma_j)\chi(\widetilde{\gamma}_d)\,,$$

which implies $\chi(\widetilde{\gamma}_d) = 0$. On the other hand, let f_χ divide d. Then $\chi(\sigma_k) = 1$ for all $k \equiv 1 \bmod d$ and

$$\chi(\widetilde{\gamma}_d) = (\varphi(d)/\varphi(n))|\{k\,; 1 \le k \le n,\ k \equiv 1 \bmod d\}| = 1\,.$$

Since γ_d is determined by (5), we have shown $\gamma_d = \widetilde{\gamma}_d$, i.e., (6) is the explicit form of γ_d.

By means of the Möbius inversion formula we obtain from (4)

$$\varepsilon_d = \sum\{\mu(d/q)\gamma_q\,; n^* \mid q \mid d\}\,. \tag{7}$$

On inserting (6) into (7) we get

$$\varepsilon_d = \sum_{(k,n)=1} \Big(\sum\{\mu(d/q)\varphi(q)/\varphi(n)\,; n^* \mid q \mid d,\ q \mid k-1\}\Big)\sigma_k\,. \tag{8}$$

If $n^* \mid q$, $\varphi(q)/\varphi(n)$ equals q/n. Hence (8) yields

$$c_k = \begin{cases} \sum\{\mu(d/q)q/n\,; n^* \mid q \mid d_k\} & \text{if } n^* \mid k-1, \\ 0 & \text{otherwise.} \end{cases} \tag{9}$$

For the remainder of the proof assume that $n^* \mid k-1$. Then

$$c_k = \mu(d/d_k)\sum\{\mu(d_k/q)q/n\,; n^* \mid q \mid d_k,\ (d/d_k, d_k/q) = 1\}\,.$$

The substitution $l = d_k/q$ yields

$$c_k = \mu(d/d_k)d_k n^{-1}\sum\{\mu(l)/l\,; l \mid d_k/n^*,\ (d/d_k, l) = 1\}\,.$$

But $\mu(l)$ is different from 0 if and only if l is square-free. For a number l of this kind the assertions

$$l \mid d_k/n^*,\ (d/d_k, l) = 1 \quad \text{and} \quad l \mid r_k$$

are equivalent. Therefore we get

$$\begin{aligned} c_k &= \mu(d/d_k)d_k n^{-1} r_k^{-1}\sum\{\mu(l)r_k/l\,; l \mid r_k\} \\ &= \mu(d/d_k)d_k n^{-1} r_k^{-1}\varphi(r_k)\,, \end{aligned}$$

which we had to show. ∎

Example. Let $n = p^m$ and $d = p^q$, $2 \le q \le m$. Then the Corollary yields

$$\begin{aligned} \varepsilon_d = p^{q-m}\Big(&\sum\{(-1/p)\sigma_{1+dj/p}\,; 1 \le j < p^{m-q+1},\ p \nmid j\} \\ &+ \sum\{(1-1/p)\sigma_{1+dj/p}\,; 0 \le j < p^{m-q+1},\ p \mid j\}\Big)\,. \end{aligned}$$

References

[1] H. W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. Reine Angew. Math. 201 (1959), 119–149.
[2] 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 23.12.1991 (2209)