Canad. Math. Bull. Vol. **38** (2), 1995 pp. 141–148

A LEOPOLDT-TYPE RESULT FOR RINGS OF INTEGERS OF CYCLOTOMIC EXTENSIONS

W. BLEY

ABSTRACT. Let p be a prime number and let m, r denote positive integers with $r \geq 1$ if $p \geq 3$ (resp. $r \geq 2$ if $p = 2$) and $m \geq 1$. We put $M = Q(\zeta_{p^r})$, $N = Q(\zeta_{p^{r+m}})$ and $\Gamma = \mathrm{Gal}(N/M)$. Then the associated order of N/M is the unique maximal order $\mathcal{M}$ in the group ring $M\Gamma$ and $\mathcal{O}_N$ is a free, rank one module over $\mathcal{M}$. A generator of $\mathcal{O}_N$ over $\mathcal{M}$ is explicitly given.

1. Introduction and statement of results.

Let N denote a finite abelian extension of a number field M and let Γ denote the Galois group $\mathrm{Gal}(N/M)$. For any number field E we denote the ring of integers by $\mathcal{O}_E$. Defining the associated order $\mathcal{A}_{N/M}$ of the extension N/M by

$$\mathcal{A}_{N/M} = \{\lambda \in M\Gamma \mid \mathcal{O}_N\lambda \subseteq \mathcal{O}_N\},$$

$\mathcal{O}_N$ can by viewed as a module over the order $\mathcal{A}_{N/M}$.

More than 30 years ago Leopoldt [7] described the Galois module structure of $\mathcal{O}_N$ when M is the field of rational numbers Q. He explicitly determined the associated order $\mathcal{A}_{N/Q}$ for any absolutely abelian number field N and exhibited an element $\theta \in \mathcal{O}_N$ such that $\mathcal{O}_N = \theta\mathcal{A}_{N/Q}$.

Some years later Jacobinski [5] generalized the result of Leopoldt for relative abelian extensions N/M which are almost maximally ramified and satisfy the further assumption that every prime ideal $\mathcal{P}$ of $\mathcal{O}_M$ that ramifies wildly in N/M is absolutely unramified in M/Q.

Further explicit results in the relative case have been obtained by Cassou-Noguès, Chan, Schertz, Srivastav and Taylor ([1], [2], [8], [9], [10]) in the case of certain ray class extensions of an imaginary quadratic number field.

The aim of this paper is to establish some Leopoldt-type results when N/M is an extension of cyclotomic fields. For any $k \in N$ we choose a primitive k-th root of unity ζ_k such that for all $k, l \in N$ with $k \mid l$: $\zeta_l^{l/k} = \zeta_k$. Let p be a prime number and let m, r denote positive integers with $r \geq 1$ if $p \geq 3$ (resp. $r \geq 2$ if $p = 2$) and $m \geq 1$. We set

$$M = Q(\zeta_{p^r}), \quad N = Q(\zeta_{p^{r+m}}), \quad \Gamma = \mathrm{Gal}(N/M),$$

and we denote the unique maximal order of $M\Gamma$ by $\mathcal{M}$. Then the main result of this paper reads as follows:

Research supported by the **DFG** and partially supported by the Fields Institute.
Received by the editors November 23, 1993.
AMS subject classification: 11R18, 11R33.

https://doi.org/10.4153/CMB-1995-020-0 Published online by Cambridge University Press

THEOREM 1.1. *The associated order $\mathcal{A}_{N/M}$ is equal to the maximal order $\mathcal{M}$ and O_N is a free, rank one $\mathcal{M}$-module. A generator is explicitly given by (17).*

REMARK. The case $r = 0$ (resp. $r = 0, 1$ if $p = 2$) is completely answered by Leopoldt's theorem.

Based on Theorem 1.1 and the preceding remark we find for the general composite case:

COROLLARY 1.2. *Let f^*, f denote positive integers with $f^* \mid f$. We put $N = Q(\zeta_f)$ and $M = Q(\zeta_{f^*})$. Then O_N is a free, rank one $\mathcal{A}_{N/M}$-module.*

REMARK. Corollary 1.2 generalizes Theorem I, 4.1 of [1], which treats the case where N/M is a Kummer extension.

We also obtain a result of this kind for some intermediate fields.

COROLLARY 1.3. *Let f^*, f denote positive integers with $f^* \mid f$. We put $M = Q(\zeta_{f^*})$. Let N be an extension of M, which is abelian over Q with conductor f. Suppose that either f is odd or $4 \mid f^*$. Then O_N is a free, rank one $\mathcal{A}_{N/M}$-module.*

In Section 2 we briefly recall some well-known facts about maximal orders in group algebras $M\Gamma$, where M is a number field and Γ a finite abelian group. Section 3 contains the proof of Theorem 1.1 and its corollaries.

It must be pointed out that part of Theorem 1.1 and also Corollary 1.2 have already appeared in the Crelle Journal published by Shih-Ping Chan and Chong-Hai Lim [3]. Whereas their proof is of purely computational nature, our approach uses more structural methods. For the proof of Theorem 1.1 we first show that the associated order $\mathcal{A}_{N/M}$ is equal to the unique maximal order $\mathcal{M}$. As a maximal order $\mathcal{M}$ decomposes naturally into a direct sum of Dedekind domains. According to this decomposition the $\mathcal{M}$-lattice O_N decomposes into a direct sum of lattices over these Dedekind domains. Therefore it suffices to construct a generator in each of these components.

2. **Lattices over maximal orders.** We let M denote a number field and Γ a finite abelian group with $\hat{\Gamma}$ its group of abelian characters. For each character $\chi \in \hat{\Gamma}$ we denote the field extension of M generated by the set $\{\chi(\gamma) \mid \gamma \in \Gamma\}$ by $M(\chi)$. We then define the division of χ by

$$[\chi] := \{\chi^g \mid g \in \operatorname{Gal}\bigl(M(\chi)/M\bigr)\}.$$

We therefore have divided $\hat{\Gamma}$ into equivalence classes and this obviously does not depend on the choice of χ in each class. We now extend the action of a character $\chi \in \hat{\Gamma}$ on Γ by linearity to the group algebra $M\Gamma$ and fix an algebra isomorphism

$$\Phi: M\Gamma \longrightarrow \prod_{[\chi]} M(\chi),$$
$$\lambda \longmapsto \bigl(\chi(\lambda)\bigr)_{[\chi]},$$

where the direct product is taken over all divisions of $\hat{\Gamma}$. Of course this isomorphism depends on the choice of the character χ within a fixed division.

https://doi.org/10.4153/CMB-1995-020-0 Published online by Cambridge University Press

For each character ψ of Γ we define an idempotent e_ψ by

$$(1) \qquad e_\psi = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\psi(\gamma)\gamma^{-1}$$

and for each division $[\chi]$ of $\hat{\Gamma}$ we then define the idempotent $e_{[\chi]}$ of $M\Gamma$ by

$$(2) \qquad e_{[\chi]} = \sum_{\psi\in[\chi]} e_\psi.$$

Let now $\mathcal{M}$ denote the maximal O_M-order in $M\Gamma$. Then we have the decomposition

$$(3) \qquad \mathcal{M} = \bigoplus_{[\chi]} \mathcal{M}e_{[\chi]},$$

where each component naturally identifies with $O_{M(\chi)}$ via the isomorphism Φ.

Any $\mathcal{M}$-lattice X may be decomposed into a direct sum

$$X = \bigoplus_{[\chi]} Xe_{[\chi]},$$

where each component is a lattice over $\mathcal{M}e_{[\chi]} \simeq O_{M(\chi)}$. The structure of each lattice $Xe_{[\chi]}$ is uniquely determined by its rank and Steinitz invariant ([4], Theorem 13).

In order to determine the Steinitz invariant $c(Xe_{[\chi]})$ we have to choose a free $\mathcal{M}e_{[\chi]}$-lattice $F_{[\chi]}$ in the $M(\chi)$-vector space spanned by $Xe_{[\chi]}$. Then the Steinitz class $c(Xe_{[\chi]})$ of any $\mathcal{M}e_{[\chi]}$-lattice $Xe_{[\chi]}$ is the element of the ideal class group $\mathrm{cl}(O_{M(\chi)})$ generated by the ideal $[F_{[\chi]} : Xe_{[\chi]}]_{O_{M(\chi)}}$. Herein $[\,:\,]_{O_{M(\chi)}}$ denotes the $O_{M(\chi)}$-module index as defined for any two $O_{M(\chi)}$-lattices spanning the same $M(\chi)$-vector space.

3. **Proof of Theorem 1.1 and the corollaries.** For the proof of Theorem 1.1 we may throughout assume that $m > r$, because the Kummer case $m \leq r$ is already treated by Theorem I, 4.1 of [1].

The Galois group Γ of N/M is cyclic of order p^m. We let σ denote a generator of Γ. Then the character $\chi \in \hat{\Gamma}$ defined by $\chi(\sigma) = \zeta_{p^m}$ is a generator of $\hat{\Gamma}$. Our first aim is to find explicitly the decomposition (3) of the maximal order $\mathcal{M}$.

LEMMA 3.1. *(i) There are exactly p^r characters $\psi \in \hat{\Gamma}$ such that $M(\psi) = M$, namely*

$$\chi^{jp^{m-r}}, \quad j = 0, \ldots, p^r - 1.$$

(ii) Let $0 \leq i < m - r$. Then all equivalence classes of characters of order p^{m-i} are given by

$$[\chi^{jp^i}], \quad j = 1, \ldots, p^r - 1, (j,p) = 1.$$

https://doi.org/10.4153/CMB-1995-020-0 Published online by Cambridge University Press

PROOF. (i) is immediate from the definitions. Let $0 \leq i < m - r$. Any character $\psi \in \hat{\Gamma}$ of order p^{m-i} is of the form χ^{jp^i}, $1 \leq j \leq p^{m-i}$, $(j,p) = 1$. Hence there are exactly $\varphi(p^{m-i})$ characters of order p^{m-i}, where φ denotes the Euler function.

We have $M(\psi) = Q(\zeta_{p^{m-i}})$, which is of degree p^{m-i-r} over M. Moreover there is a bijection

$$\sigma\colon Z/p^{m-i-r}Z \longrightarrow \mathrm{Gal}\big(M(\psi)/M\big) \tag{4}$$

given by

$$\zeta_{p^{m-i}}^{\sigma(\nu)} = \zeta_{p^{m-i}}^{1+p^r\nu}, \qquad \nu \in Z.$$

Let now j, j_1 denote integers such that $0 < j, j_1 < p^r$ and $(j,p) = (j_1,p) = 1$. From $\chi^{jp^i(1+p^r\nu)} = \chi^{j_1p^i}$ we immediately deduce $j = j_1$. Therefore the divisions $[\chi^{jp^i}]$ are mutually disjoint for $0 < j < p^r$, $(j,p) = 1$, and we easily find

$$\begin{aligned}\#\Big(\bigcup_{\substack{j=1\\(j,p)=1}}^{p^r-1} [\chi^{jp^i}]\Big) &= \varphi(p^r)\cdot p^{m-i-r}\\ &= \varphi(p^{m-i}),\end{aligned}$$

which coincides with the total number of characters of order p^{m-i}. ∎

In other words Lemma 3.1 says that the equivalence classes of $\hat{\Gamma}$ are given by $[\chi^{jp^i}]$,

$$\begin{gathered} i = 0, \dots, m-r,\\ j = 0, \dots, p^r - 1, \quad \text{if } i = m - r,\\ j = 1, \dots, p^r - 1,\ (j,p) = 1, \quad \text{if } 0 \leq i < m - r. \end{gathered} \tag{5}$$

For $t = 0, \dots, m$ we denote by Γ_t the subgroup of Γ of order p^{m-t} generated by σ^{p^t}.

LEMMA 3.2. *The elements*

$$e_{ij} = \frac{1}{p^{r+i}} \sum_{\gamma\in\Gamma_{m-r-i}} \chi^{jp^i}(\gamma)\gamma^{-1} \in M\Gamma$$

form a complete system of primitive, orthogonal idempotents. (Here the enumeration is taken as in (5).)

PROOF. For any division $[\chi^{jp^i}]$ we have to calculate

$$\sum_{\psi\in[\chi^{jp^i}]} e_\psi. \tag{6}$$

Using (1), (2) and (4) we can easily evaluate (6):

$$\begin{aligned}\sum_{\psi\in[\chi^{jp^i}]} e_\psi &= \sum_{\nu=0}^{p^{m-i-r}-1} \frac{1}{p^m} \sum_{\gamma\in\Gamma} \chi^{jp^i(1+p^r\nu)}(\gamma)\gamma^{-1} =\\ &= \frac{1}{p^m} \sum_{\gamma\in\Gamma} \Big(\sum_{\nu=0}^{p^{m-i-r}-1} \big(\chi^{jp^{i+r}}(\gamma)\big)^{\nu} \Big) \chi^{jp^i}(\gamma)\gamma^{-1}.\end{aligned}$$

Now the result is immediate from

$$\sum_{\nu=0}^{p^{m-i-r}-1} \left(\chi^{jp^{i+r}}(\gamma)\right)^{\nu} = \begin{cases} 0, & \text{if } \gamma \notin \Gamma_{m-i-r}, \\ p^{m-i-r}, & \text{if } \gamma \in \Gamma_{m-i-r}. \end{cases}$$

■

We now fix an isomorphism

$$\Phi\colon M\Gamma \longrightarrow \prod_{i,j} M(\chi^{jp^i})$$

by

$$\Phi(\lambda) = \left(\chi^{jp^i}(\lambda)\right)_{i,j}, \qquad \lambda \in M\Gamma.$$

The extension $M(\chi^{jp^i})$ is exactly the p^{m-i}-th cyclotomic field $Q(\zeta_{p^{m-i}})$ and it is well-known that

$$o_{M(\chi^{jp^i})} = o_M[\zeta_{p^{m-i}}].$$

Taking into account that

(7) $$\Phi(\sigma^k e_{ij}) = (0, \ldots, 0, \zeta^{jk}_{p^{m-i}}, 0, \ldots, 0), \quad k = 0, \ldots, p^m - 1,$$

we have shown:

PROPOSITION 3.3. *$\mathcal{M}$ is generated over the integral group ring $o_M\Gamma$ by adjoining the idempotents e_{ij}, where i,j ranges over the set of indices described in (5).*

Next we prove that the maximal order $\mathcal{M}$ is equal to the associated order $\mathcal{A}_{N/M}$. To that end it suffices to show

(8) $$o_N e_{ij} \subseteq o_N.$$

Since χ^{jp^i} is trivial on Γ_{m-i} the idempotent e_{ij} can be written in the form

(9) $$e_{ij} = \underbrace{\left(\frac{1}{p^r} \sum_{\gamma \in \Gamma_{m-r-i}/\Gamma_{m-i}} \chi^{jp^i}(\gamma)\gamma^{-1}\right)}_{=:E_{ij}} \left(\frac{1}{p^i} \sum_{\delta \in \Gamma_{m-i}} \delta\right).$$

We are therefore led to consider the tower of extensions $N/L_i/K_i$ with

$$L_i = \mathrm{Fix}(\Gamma_{m-i}) = Q(\zeta_{p^{m+r-i}}),$$
$$K_i = \mathrm{Fix}(\Gamma_{m-i-r}) = Q(\zeta_{p^{m-i}}).$$

We now prove

(i) $\frac{1}{p^i} \mathrm{Tr}_{N/L_i}(o_N) = o_{L_i}$,

(ii) $o_{L_i} E_{ij} \subseteq o_{L_i}$, which immediately implies (8).

We note that in any intermediate field F of N/M the rational prime p is totally ramified. Let $\mathcal{P}_F$ denote the unique prime ideal of O_F above p.

Returning to the proof of (i) we remark that the different D_{N/L_i} of the extension N/L_i is given by

$$D_{N/L_i} = p^i O_N = \mathcal{P}_N^{i\varphi(p^{r+m})}.$$

An obvious calculation using the definition of the inverse different D_{N/L_i}^{-1} shows $\mathrm{Tr}_{N/L_i}(O_N) = p^i O_{L_i}$. This establishes (i).

The extension L_i/K_i is a cyclic extension of degree p^r and, since $r \leq m-i$, it is in fact a Kummer extension. The element E_{ij} is a primitive idempotent of the algebra $K\,\mathrm{Gal}(L_i/K_i)$. In order to prove (ii) we therefore can proceed in exactly the same way as in the proof of Theorem I, 4.1 of [1]. Nevertheless we give the proof since we will later explicitly need some of its calculations.

Since L_i/K_i is a Kummer extension, we have an isomorphism

$$\sigma\colon Z/p^rZ \longrightarrow \Gamma_{m-r-i}/\Gamma_{m-i},$$

given by $\zeta_{p^{m+r-i}}^{\sigma(\nu)} = \zeta_{p^{m+r-i}}^{1+p^{m-i}\nu}$ for $\nu \in Z$.

Let ν_0 be the inverse image of $\sigma^{p^{m-r-i}}$. Then we have $(\nu_0, p) = 1$ and

$$\chi^{jp^i}\big(\sigma(\nu_0)\big) = \zeta_{p^r}^j.$$

We shall show that

$$O_{L_i}E_{ij} = O_{K_i}\zeta_{p^{m+r-i}}^{k'}, \tag{10}$$

where k' is uniquely determined by $\nu_0 k' \equiv j \pmod{p^r}$ and $0 \leq k' \leq p^r - 1$. For $0 \leq k \leq p^r - 1$ we get

$$\begin{aligned}\zeta_{p^{m+r-i}}^k E_{ij} &= \frac{1}{p^r}\sum_{\nu=0}^{p^r-1} \chi^{jp^i}\big(\sigma(\nu\nu_0)\big)\zeta_{p^{m+r-i}}^{k(1-p^{m-i}\nu\nu_0)} \\ &= \Big(\frac{1}{p^r}\sum_{\nu=0}^{p^r-1}\zeta_{p^r}^{\nu(j-k\nu_0)}\Big)\zeta_{p^{m+r-i}}^k.\end{aligned}$$

From

$$\frac{1}{p^r}\sum_{\nu=0}^{p^r-1}\zeta_{p^r}^{\nu(j-k\nu_0)} = \begin{cases} 1, & \text{if } k\nu_0 \equiv j \pmod{p^r}, \\ 0, & \text{otherwise.}\end{cases}$$

we deduce (10).

Combining (i) and (10) we have shown

$$O_N e_{ij} = O_{K_i}\zeta_{p^{m+r-i}}^{k'}, \tag{11}$$

where k' is uniquely determined by $k'\nu_0 \equiv j \pmod{p^r}$ and $0 \leq k' \leq p^r - 1$.

So we deduce:

https://doi.org/10.4153/CMB-1995-020-0 Published online by Cambridge University Press

PROPOSITION 3.4. $\mathcal{A}_{N/M} = \mathcal{M}$.

We now consider the decompositions

$$O_N = \bigoplus_{i,j} O_N e_{ij},$$
$$\mathcal{M} = \bigoplus_{i,j} \mathcal{M} e_{ij},$$

where i,j range over the set of indices in (5).

We put

$$\theta_i = \frac{1-\zeta_{p^{m-i}}}{1-\zeta_{p^{m+r}}}$$

for $i = 0, \ldots, m-r$. We shall prove

$$O_N e_{ij} = \theta_i \cdot \mathcal{M} e_{ij}. \tag{12}$$

In particular this implies that all the Steinitz invariants $c(O_N e_{ij})$ are trivial. We even have a generator of O_N over $\mathcal{M}$, which is given by

$$\theta = \sum_{i,j} \theta_i e_{ij}. \tag{13}$$

Now we come to the proof of (12). The inclusion $O_N e_{ij} \supseteq \theta_i \mathcal{M} e_{ij}$ is trivial. We note that

$$\frac{1}{p^i} \operatorname{Tr}_{N/L_i}(\theta_i) = \frac{1-\zeta_{p^{m-i}}}{1-\zeta_{p^{m+r-i}}} = \sum_{k=0}^{p^r-1} \zeta_{p^{m+r-i}}^k. \tag{14}$$

This, together with (9), implies that

$$\theta_i e_{ij} = \zeta_{p^{m+r-i}}^{k'}, \tag{15}$$

where k' is uniquely determined by $k'\nu_0 \equiv j \pmod{p^r}$ and $0 \leq k' \leq p^r - 1$. Since $\gamma e_{ij} \in \mathcal{M} e_{ij}$ for all $\gamma \in \Gamma$ we deduce that

$$(\zeta_{p^{m+r-i}}^{k'})^\gamma \in \theta_i \mathcal{M} e_{ij} \quad \text{for all } \gamma \in \Gamma. \tag{16}$$

Now (11) and (16) immediately imply $O_N e_{ij} \subseteq \theta_i \mathcal{M} e_{ij}$. From (13) and (15) (resp. Theorem I, 4.1 of [1]) we get the explicit representation

$$\theta = \sum_{i,j} \zeta_{p^{m+r-i}}^j, \tag{17}$$

where i,j range over the set of indices in (5) if $m > r$ (resp. $i = 0, j = 0, \ldots, p^m - 1$, if $m \leq r$).

This finishes the proof of Theorem 1.1.

PROOF OF COROLLARY 1.2. Based on Theorem 1.1 and Leopoldt's result in the case $r = 0$ (resp. $r = 0, 1$ for $p = 2$) the proof of Corollary 1.2 can be achieved in exactly the same way as the proof of Theorem 2.12, Chapter XI of [1]. See also [3].

https://doi.org/10.4153/CMB-1995-020-0 Published online by Cambridge University Press

PROOF OF COROLLARY 1.3. Since the natural number f is minimal subject to the condition $N \subseteq Q(\zeta_f)$, we may prove that under the assumptions of Corollary 1.3 the extension $Q(\zeta_f)/N$ is at most tamely ramified (see *e.g.* [5], p. 157).

We put $\Gamma = \mathrm{Gal}\big(Q(\zeta_f)/M\big)$ and $\Gamma_1 = \mathrm{Gal}\big(Q(\zeta_f)/N\big)$. Then the canonical projection

$$\varphi:\Gamma \longrightarrow \Gamma/\Gamma_1$$

induces a surjective algebra homomorphism

$$\varphi: M\Gamma \longrightarrow M(\Gamma/\Gamma_1).$$

By Corollary 1.2 there exists an element $\theta \in Q(\zeta_f)$ such that

$$O_{Q(\zeta_f)} = \theta \mathcal{A}_{Q(\zeta_f)/M}.$$

Since the extension $Q(\zeta_f)/N$ is at most tamely ramified, we get by taking traces

$$O_N = \mathrm{Tr}_{Q(\zeta_f)/N}(\theta) \cdot \varphi(\mathcal{A}_{Q(\zeta_f)/M}).$$

This establishes the proof of Corollary 1.3.

REFERENCES

1. Ph. Cassou-Nogués and M. J. Taylor, *Elliptic functions and rings of integers*, Progr. Math. **66**, Basel, Stuttgart, Boston, 1987.
2. Shih-Ping Chan, *Modular functions, elliptic functions and Galois module structure*, J. Reine Angew. Math. (1987), 67–82.
3. Shih-Ping Chan and Chong-Hai Lim, *Relative Galois module structure of rings of integers of cyclotomic fields*, J. Reine Angew. Math. **434**(1993), 205–220.
4. A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge Stud. Adv. Math. **27**, Cambridge University Press, 1991.
5. H. Jacobinski, *Über die Hauptordnung eines Körpers als Gruppenmodul*, J. Reine Angew. Math. **213**(1964), 151–164.
6. S. Lang, *Elliptic Functions*, New York, Heidelberg, Berlin, 1987.
7. H. W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. Reine. Angew. Math. **209**(1962), 54–71.
8. R. Schertz, *Galoismodulstruktur und Elliptische Funktionen*, J. Number Theory, **39**(1991), 285–326.
9. A. Srivastav, *Swan modules and elliptic functions*, Illinois J. Math. **32**(1988).
10. ———, *Modules de Swan et courbes elliptiques à Multiplication complexe*, Séminaire de Théorie des Nombres **2**, Bordeaux, 1990.

Werner Bley
Institut für Mathematik
Universität Augsburg
Universitätsstr. 8
86135 Augsburg
Germany
e-mail: Bley@Uni-Augsburg.DE

https://doi.org/10.4153/CMB-1995-020-0 Published online by Cambridge University Press