About the kernel of the augmentation of finitely generated Z-modules

MARC CONRAD*

Abstract. *Let M be a free finitely generated* $\mathbf{Z}$*-module with basis B and ΔM the kernel of the homomorphism $M \to \mathbf{Z}$ which maps B to 1. A basis of ΔM can be easily constructed from the basis B of M. Let further R be a submodule of M such that $N = M/R$ is free. The subject of investigation is the module $\Delta N = (\Delta M + R)/R$. We compute the index $[N : \Delta N]$ and construct bases of ΔN with the help of a basis of N. Finally, the results are applied to a special class of modules which is connected with the group of cyclotomic units.*

Key words: *augmentation, basis, module, cyclotomic units*

AMS subject classifications: 20K05, 11R18, 20C05

Received August 20, 1999 Accepted February 28, 2000

1. Introduction

Well known in the context of group rings is the *augmentation* of a group ring element which is the homomorphism obtained by mapping the group elements to 1. The augmentation defines the *augmentation ideal* of the group ring which denotes the kernel of the augmentation [3]. Similarly, in a free $\mathbf{Z}$-module M each basis B defines a homomorphism $\mathrm{aug} : M \to \mathbf{Z}$, $\sum_{b \in B} \alpha_b b \mapsto \sum_{b \in B} \alpha_b$. We denote the kernel of aug by ΔM. We consider further the module $N = M/R$ where R is a submodule of M such that N is free, and let $\Delta N = (\Delta M + R)/R$. In the following we assume that the module M is finitely generated. It is easy to see that the index $[M : \Delta M]$ is infinite. In *Theorem 1.* we identify the index $[N : \Delta N]$ as the greatest common divisor of the augmentation of the elements of R.

It can be seen straightforwardly that for a fixed $b_0 \in B$ the set

$$B_0 = \{b - b_0;\ b \in B,\ b \neq b_0\} \tag{1}$$

is a basis of ΔM. A similar result is obtained for ΔN in *Theorem 2.* In *Section 4.* we will apply this result to a class of modules which is connected to the group of cyclotomic units. This group plays an important role in the theory of cyclotomic fields [4].

*Universität des Saarlandes, Postfach 151150, D-66041 Saarbrücken, Germany, e-mail: `marc@math.uni-sb.de`, http: `//simath.math.uni-sb.de/~marc`

2. The index of ΔN

We use in the following the notation of the introduction.

Theorem 1. *We have* $[N : \Delta N] = \gcd \operatorname{aug}(R)$ *where the greatest common divisor of* $\{0\}$ *is defined as* ∞*.*

Proof. Let $b_0 \in B$. Because $b \equiv b_0 \bmod \Delta M$ for all $b \in B$ we see that $N/\Delta N$ is cyclic and generated by b_0. The index is the smallest positive number such that $mb_0 \in R + \Delta M$. Note that $\operatorname{aug}(mb_0) = m$ for $m \in \mathbf{Z}$.

In the case $R \subseteq \Delta M$ we have $\operatorname{aug} R = \{0\}$. From $mb_0 \notin \Delta M$ for all $m \neq 0$ we see $[N : \Delta N] = \infty$ as it was claimed in the Theorem.

For $R \not\subseteq \Delta M$ there exists an element $r \in R$ with minimal positive augmentation ρ. Noting that $\rho b_0 \equiv r \bmod \Delta M$, it follows $[N : \Delta N] \leq \rho$.

On the other hand, if we have $k \in \mathbf{Z}$ and $r' \in R$ such that $kb_0 \equiv r' \bmod \Delta M$, it follows $\rho \leq k = \operatorname{aug}(r')$ because of the minimality of ρ, and we obtain $[N : \Delta N] = \rho$.

It remains to show that $\rho = \gcd \operatorname{aug}(R)$. Suppose there exists $r' \in R$ such that ρ is not a divisor of $\rho' = \operatorname{aug}(r')$. Then by computing $\delta = \gcd(\rho, \rho')$ we find numbers $\alpha, \beta \in \mathbf{Z}$ with $\delta = \alpha\rho + \beta\rho'$. But $\alpha r + \beta r' \in R$ is an element with positive augmentation $\delta < \rho$ which is a contradiction to the minimality of ρ. □

We show in the next lemma how the index $[N : \Delta N]$ can be explicitly computed.

Lemma 1. *If* $E \subseteq R$ *generates* R*, then* $\gcd \operatorname{aug}(R) = \gcd \operatorname{aug}(E)$*.*

Proof. For $[N : \Delta N] = \infty$ there is nothing to show. In the case when $\rho = [N : \Delta N] < \infty$, the claim follows from the existence of $r \in R$ and $\alpha_e \in \mathbf{Z}$ such that $\rho = \operatorname{aug}(r) = \sum_{e \in E} \alpha_e \operatorname{aug}(e)$. With this we obtain

$$\gcd \operatorname{aug}(R) = \rho = \gcd(\operatorname{aug}(E) \cup \{\rho\}) = \gcd \operatorname{aug}(E). \tag{2}$$

□

Remark 1. *Similarly to* ΔM*, we can identify* ΔN *as a kernel of a homomorphism. With* $k = [N : \Delta N]$ *for a finite and* $k = 0$ *for an infinite index we have a homomorphism*

$$\overline{\operatorname{aug}} : N \to \mathbf{Z}/k\mathbf{Z},\ a + R \mapsto \operatorname{aug}(a) + k\mathbf{Z} \tag{3}$$

and $\Delta N = \ker_N \overline{\operatorname{aug}}$.

3. Construction of a basis of ΔN

In the following, let $C \subseteq M$ induce a basis of N, i. e. let $\{c + R;\ c \in C\}$ be a basis of N. We assume that there exist $\gamma \in \mathbf{Z}$ such that $\operatorname{aug}(c) = \gamma$ for all $c \in C$. Note that this is no restriction to the module N. In *Algorithm 1* we will show how such a basis can be constructed from an arbitrary basis of N.

Let $\rho = [N : \Delta N]$. In the case $\rho = \infty$ it is easy to see that similarly to (1) for a fixed $c_0 \in C$, the set $C_0 = \{c - c_0;\ c \in C,\ c \neq c_0\}$ is a basis of ΔN. We assume in the following $\rho < \infty$ and show in the next *Lemma* and the subsequent *Theorem* how to construct bases of ΔN in this case.

Lemma 2. *Let $c_1 \in C$. Then*

$$C_1 = \{c - c_1;\ c \in C,\, c \neq c_1\} \cup \{\rho c_1\} \tag{4}$$

induces a basis of ΔN.

Proof. We show that the elements $b - b_0$ with $b, b_0 \in B$ are modulo R generated by C_1. Because C is a basis of N, we have $\alpha_c, \beta \in \mathbf{Z}$ such that

$$b - b_0 = r + \beta c_1 + \sum_{c \in C,\, c \neq c_1} \alpha_c (c - c_1). \tag{5}$$

The application of aug to (5) and reducing modulo ρ gives $\beta\gamma \equiv 0 \bmod \rho$. We show in the rest of the proof that $\gcd(\gamma, \rho) = 1$. Then we have $\rho | \beta$ and the claim of the *Lemma* follows.

We can write any $b \in B$ as $b = c + r$ with $c \in \langle C \rangle$ and $r \in R$. This gives $1 = \operatorname{aug}(c) + \operatorname{aug}(r) = \nu\gamma + \mu\rho$ with $\nu, \mu \in \mathbf{Z}$ which leads to $\gcd(\gamma, \rho) = 1$. $\square$

Compared with the basis B_0 of ΔM in (1), the basis C_1 from (4) has the extra element ρc_1 added to the expected elements $c - c_1$. In the next theorem we give a basis which looks more similar to B_0.

Theorem 2. *Let $c_0 \equiv c' \bmod R$ such that $c' \in \langle C \rangle$ and $\operatorname{aug}(c') = (1 - \rho)\gamma$. Then*

$$C_0 = \{c - c_0;\ c \in C\} \tag{6}$$

induces a basis of ΔN.

Proof. Let c_1 be as in *Lemma 2.* and $C' = \{c - c_1;\ c \in C,\, c \neq c_1\}$ such that $C_1 = C' \cup \{\rho c_1\}$ induces a basis of ΔN. Because of $c_1 - c' \equiv \rho c_1 \bmod \langle C' \rangle$ we can replace ρc_1 by $c_1 - c'$ in C_1. By replacing the other elements of C_1 using the relation $c - c' = c - c_1 + (c_1 - c')$ for $c \in C$ we obtain $\{c - c';\ c \in C\}$ as a basis of ΔN. With $c_0 \equiv c' \bmod R$ we get the claim. $\square$

Remark 2. *If we choose $c_0 = c' + \gamma r$ with $r \in R$ such that $\operatorname{aug}(r) = \rho$ we obtain $\operatorname{aug}(c_0) = \gamma$ and therefore $C_0 \subseteq \Delta M$. So, with C_0, we directly obtain a basis of $\Delta M/(\Delta M \cap R)$ (which is of course isomorphic to ΔN).*

In *Lemma 2.* and *Theorem 2.* we assume that there is a basis $C \subseteq M$ of N with $\operatorname{aug}(c) = \gamma$ for all $c \in C$. We give here an Euclidean-like algorithm which shows how to construct such a basis from an arbitrary basis.

Algorithm 1 . *Let $C \subseteq M$ induce a basis of N. The algorithm leads to $\operatorname{aug}(c) = \gamma$ for all $c \in C$ by successively replacing elements of C.*

If $\operatorname{aug}(c) = 0$ for all $c \in C$, there remains nothing to be done. Otherwise, we choose first c' with $\operatorname{aug}(c') \neq 0$ and replace each $c \in C \setminus \{c'\}$ by $c + \lambda c'$ with $\lambda \in \mathbf{Z}$ such that $\operatorname{aug}(c) > 0$. If $\operatorname{aug}(c') < 0$, we also have to replace c' by $-c'$. After that we perform the following steps.

1. *If all elements of C have the same augmentation, the algorithm is finished.*
2. *Pick c, $c' \in C$ such that $\operatorname{aug}(c) < \operatorname{aug}(c')$ and replace c' by $c' - c$.*
3. *Go to Step 1.*

The algorithm terminates because $\sum_{c \in C} \operatorname{aug}(c) \in \mathbf{N}$ decreases in every run of Step 2.

4. A special class of modules

For a finite set A we denote by ΣA the sum $\sum_{a\in A} a$ in the free module $\langle A\rangle$ generated by A. For $i = 1,\dots,r$ let A_i be a finite set with an involution σ operating nontrivially on each element. So we have sets H_i such that $B_i = H_i \cup \sigma H_i$ and $H_i \cap \sigma H_i = \emptyset$ for $i = 1,\dots,r$. We define further the module

$$Z = \langle B_1\rangle/\langle\Sigma B_1\rangle \otimes\cdots\otimes \langle B_r\rangle/\langle\Sigma B_r\rangle. \tag{7}$$

The involution on B_i defines an involution on Z and we may interpret Z also as a $\mathbf{Z}[\sigma]$-module. The subject of investigation is the module $N = Z/\ker_Z(\sigma+1)$.

Remark 3. *The module N is directly connected with the group of cyclotomic units $C^{(n)}$. Let ϵ_n be a primitive n^{th} root of unity. Then $C^{(n)}$ is defined as the multiplicative subgroup of $D^{(n)}$ which are units of $\mathbf{Z}[\epsilon_n]$. The group $D^{(n)}$ is generated by the elements $1-\epsilon_n^a$ with $1 \le a < n$ modulo torsion. With $\widehat{C^{(n)}} = C^{(n)}/L^{(n)}$ where $L^{(n)} = \prod_{d|n,\, d\neq n} C^{(d)}$ we have for $n = p_1\cdots p_r$ an odd, square free and not a prime isomorphism $N \cong \widehat{C^{(n)}}$ when we choose $B_i = \{1,\dots,p_i-1\}$. For general n we have similar isomorphisms (see [1]).*

Let $M = \langle B_1\times\cdots\times B_r\rangle$ and let S be the module generated by the sums

$$s_i(a_1,\dots,a_r) = \sum_{b\in B_i}(a_1,\dots,a_{i-1},b,a_{i+1},\dots,a_r), \quad i = 1,\dots,r \tag{8}$$

where $a_j \in B_j$ for $j = 1,\dots,r$. By [2] we have then for r even

$$N \cong M/(S + (1-\sigma)M) \tag{9}$$

and for r odd

$$N \cong M/(S + (1-\sigma)M + \langle e\rangle) \tag{10}$$

with $e = \Sigma(H_1\times\cdots\times H_r)$.

Theorem 3. *For $i = 1,\dots,r$ let $\beta_i = |B_i|$, the number of elements of B_i, and $\beta = \gcd(\beta_1,\dots,\beta_r)$. Then we have for $\rho = [N : \Delta N]$ that*

$$\rho = \begin{cases} \beta/2, & \text{if } r = 1 \text{ or} \\ & r \text{ odd and } \beta_i \equiv 2 \bmod 4 \text{ for } i = 1,\dots,r, \\ \beta, & \text{else.} \end{cases}$$

Proof. The claim follows for r even and $r = 1$ from *Lemma 1.* and the isomorphisms (9) and (10). For r odd we additionally use $\operatorname{aug}(e) = \prod_{i=1}^r(\beta_i/2)$. □

A basis of N can be constructed with weak σ-bases according to [1]. We get the following result.

Lemma 3. *For each $i = 1,\dots,r$ we fix $h_i \in H_i$. Let $H_i^\flat = H_i \setminus \{h_i\}$ and $A_i^\flat = A_i \setminus \{h_i\}$. Then we obtain $C = F^0 \cup F^+$ as a basis of N where*

$$F^0 = \bigcup_{i=1}^r \{h_1\}\times\cdots\times\{h_{i-1}\}\times H_i^\flat\times B_{i+1}^\flat\times\cdots\times B_r^\flat \tag{11}$$

and

$$F^+ = \begin{cases} \emptyset, & \textit{for } r \textit{ odd,} \\ \{h_1\} \times \cdots \times \{h_r\}, & \textit{for } r \textit{ even.} \end{cases} \tag{12}$$

We see here that the basis C can be chosen as a subset of $B = B_1 \times \cdots \times B_r$. So, all elements of C have augmentation 1, and we may apply *Theorem 2.* with $\gamma = 1$ and $c_0 = (1-\rho)c$, where c is any element of C. This leads to a basis of ΔN as in (6).

However, we might ask a stronger question: Can we find a basis $C \subseteq B$ of N such that we can choose $c_0 \in B$? Up to now there is no general answer to this. We will discuss in the rest of this section some special cases where the answer is affirmative.

In the following, we call a basis C_0 of ΔN which has the form $C_0 = \{c - c_0;\ c \in C\}$ with $C \subseteq B$ and $c_0 \in B$ a *handsome* basis of ΔN.

Theorem 4. *If there exists a $j \in \{1, \ldots, r\}$ such that $\beta_j = \rho$, then ΔN has a handsome basis.*

Proof. In the case $F_0 \neq \emptyset$, we rearrange the sets B_i such that $j = r$. Let $(a_1, \ldots, a_{r-1}, a_r)$ be any element of F^0. Then $(a_1, \ldots, a_{r-1}, b) \in F^0$ for $b \neq h_r$. So, we may choose in *Theorem 2.* $c' = -\sum_{b \in B^\flat}(a_1, \ldots, a_{r-1}, b)$, and the claim follows with $c_0 = (a_1, \ldots, a_{r-1}, h_r)$. In the case $F_0 = \emptyset$, we take $c_0 = (h_1, \ldots, h_{r-1}, \sigma h_r)$. $\square$

The converse of *Theorem 2.* is not true. Even if a basis of the form $C = F^0 \cup F^+$ as in *Lemma 3.* cannot be used for the construction of a handsome basis we may have more success when starting with a different basis. We will give an example in the next *Lemma.*

Lemma 4. *Let $B_1 = \{a, b, \sigma a, \sigma b\}$ and $B_2 = \{a, b, c, \sigma a, \sigma b, \sigma c\}$ be two sets of four respectively six elements with σ acting nontrivially on B_1 and B_2. The module N is as in (9) given as the free module M generated over $B = B_1 \times B_2$ modulo $(1-\sigma)M$ and the relations described in (8). With*

$$C = \{(a, b), (b, c), (\sigma b, a), (\sigma b, b), (\sigma b, c), (a, \sigma a), (a, \sigma b), (\sigma a, c)\}$$

and $c_0 = (a, a)$ we obtain $\{c - c_0;\ c \in C\}$ as a basis of ΔN.

Proof. We show first that C is a basis of N. By *Lemma 3.* we obtain $\operatorname{rank} N = 8 = |C|$ and it is sufficient to show that C generates N. Because of $c \equiv \sigma c \bmod (1-\sigma)M$ we see that σC is generated by C. The elements of $B \setminus (C \cup \sigma C)$ can then be generated by $C \cup \sigma C$ directly by relations of S.

Theorem 1. gives $[N : \Delta N] = 2$. We will now apply *Theorem 2.* in order to construct a basis of ΔN. Let $c' = c_0 + r$ with

$$r = \sum_{x \in B_1}(x, c) - \sum_{y \in B_2}(a, y) - (1-\sigma)(\sigma a, c). \tag{13}$$

Because c' satisfies the conditions in *Theorem 2.* the claim follows. $\square$

Without going into details, we note that a construction as in *Lemma 4.* can be generalized to more complicated cases. However, the problem of giving a general algorithm for the construction of a handsome basis remains open.

References

[1] M. CONRAD, *Construction of bases for the group of cyclotomic units*, J. Number Theory **81**(2000), 1–15.

[2] M. CONRAD, *On explicit relations between cyclotomic numbers*, Acta Arithmetica, to appear.

[3] G. KARPILOVSKI, *Commutative Group Algebras*, Dekker, New York, 1983.

[4] L. C. WASHINGTON, *Introduction to Cyclotomic Fields*, Springer, New York, 1982.