On the Augmentation Terminal of a Finite Abelian Group

MICHAEL SINGER

Department of Mathematics, California Institute of Technology, Pasadena, California 91125

Communicated by A. Fröhlich

Received May 28, 1975

We apply our earlier results on invertible powers of ideals in commutative separable algebras to obtain a generalization of a theorem of Bachmann and Grünenfelder on filtrations of the augmentation ideal of the integral group ring of a finite abelian group.

Let $R$ be a dedekind domain (to avoid trivial exceptions, not a field) with quotient field $K$. Let $A$ be a finite-dimensional commutative separable $K$-algebra. An $A$-$R$-ideal, or simply, when no confusion is likely to result, an ideal, $M$, is a finitely generated $R$-module contained in $A$ such that $KM = A$. Suppose that $(A : K) = n \geq 2$. Then it is well known ([3, 5, 7]) that $M^1$, and all higher powers of $M$ are invertible. We may, however, adapt our results on componentwise dedekind ideals [5, 7] to state a sharper theorem. Since the rational integral group ring of a finite abelian group is componentwise dedekind as an order in the rational group algebra, this added sharpness is of some use in applications.

Let $d(A)$ denote the number of primitive idempotents in $A$. If $L$ is a finite separable extension field of $K$, with maximal order $S$ over $R$, we shall always identify $A$ with $A \otimes_K L$; thus $A$ is naturally embedded in $AL = A \otimes_K L$. If $M$ is an $A$-$R$-ideal, we further identify the $AL$-$S$-ideals $MS$ and $M \otimes_R S$.

We now have:

THEOREM 1. Let $L$ be a finite separable extension field of $K$, with maximal order $S$ over $R$. Let $M$ be an $A$-$R$-ideal such that for every primitive idempotent $e$ of $AL$, $MSe$ is locally isomorphic to the maximal order of the field $ALe$ over $Se$. Let $d = d(AL)$. Then $M^{d-1}$ and all higher powers of $M$ are invertible.

We wish to consider ideals $M$ such that $M^r \supseteq M^{r+1}$ for all natural numbers $r$. We are particularly interested in the behavior of the sequence $M^r/M^{r+1}$, $r = 1, 2, \ldots$. To illuminate this we shall need to look more closely at the high powers of an ideal $M$. 

Copyright © 1976 by Academic Press, Inc.
All rights of reproduction in any form reserved.
Let the notation be as in Theorem 1. We may further enlarge $L$ by a finite separable extension field (which we shall still call $L$) such that $d(AL)$ is not increased, and such that the following statement holds locally at each prime of $S$:

Let $\mathcal{B}$ be the maximal order in $AL$ over $S$; then there is an element $v \in AL$ such that

$$1 \in vMS \subseteq \mathcal{B}.$$ 

Of course $v$ must be invertible in $AL$. For a proof of this statement see [6, 7].

We continue to consider the local situation. For $r = 1, 2,...$ the ideals $(vMS)^{r}$ form an increasing sequence contained in $\mathcal{B}$. From, let us write, the $s$th term on, where $s = s(M) \leq d(AL) - 1$, all terms are equal, and indeed equal to an order in $AL$. Let $\mathcal{H}$ denote the intersection of this order with $A$.

Then $\mathcal{H}$ is an order in $A$ over $R$, and we have $M^r \cong \mathcal{H}$ for all $r \geq s(M)$.

So now, locally at each prime of $R$, we have $M^r = u_r \mathcal{H}$ for all $r \geq s(M)$, where the $u_r \in A$ are invertible elements. Now we have for all $r \geq s = s(M)$,

$$M^{sr} = u^{s}^r \mathcal{H} = u^{s+1} \mathcal{H}.$$

and

$$M^{(s+1)r} = u^{s+1} \mathcal{H} = u^{s+1} \mathcal{H}.$$

Hence

$$u_r \mathcal{H} = (u^{s+1} \mathcal{H})^{r} \mathcal{H}.$$ 

However, $u_r$ is at our disposal to the extent of multiplication by a unit in $\mathcal{H}$. So, writing $u = u^{s+1} \mathcal{H}$, we may take $u_r = u^r$. Specifically, we now have:

**Theorem 2.** Let $M$ be a $A-R$-ideal, and let $s = s(M)$ be the least index such that $M^s$ is invertible. For each prime $p$ of $R$ let $R_p$ denote the localization of $R$ at $p$. Then there is an order $\mathcal{H}$ in $A$, and for each $p$ an element $u_p \in A$, such that for all $r \geq s$, $M^r R_p = u_p^r \mathcal{H} R_p$.

We may further state:

**Theorem 3.** Let $M$ be an $A-R$-ideal such that $M^r \supseteq M^{r+1}$ for all $r \geq 1$. Then we have an isomorphism of $R$-modules

$$M^r/M^{r+1} \cong M^t/M^{t+1}$$

for all $r, t \geq s = s(M)$. Furthermore $M^{s-1}/M^s$ is isomorphic to a proper $R$-submodule of $M^s/M^{s+1}$.
Proof. In the notation of Theorem 2, we have \( u_p^{s+1} \mathfrak{A} \subseteq u_p^s \mathfrak{A} \), so that \( u_p \in \mathfrak{A} \). And now
\[
(M^r/M^{r+1})R_p \cong (\mathfrak{A}/u_p \mathfrak{A})R_p,
\]
for all \( r \geq s \) and for all \( p \). From the structure theory of finitely generated modules over Dedekind domains we now have
\[
M^r/M^{r+1} \cong M^t/M^{t+1} \quad \text{as } R\text{-modules},
\]
for all \( r, t \geq s \).

There is a prime \( p \) of \( R \) such that \( M^{s-1}R_p \not\subseteq \mathfrak{A}R_p \). For any \( r \geq 1 \) we have
\[
(u_p^{-1}M)^r \mathfrak{A}R_p = (u_p^{-1}M)^r(u_p^{-1}M)^sR_p = (u_p^{-1}M)^{r+s}R_p = \mathfrak{A}R_p.
\]
Since \( \mathfrak{A}R_p \) is an order in \( A \) over \( R_p \), we have
\[
(u_p^{-1}M)^r \mathfrak{A}R_p \subseteq \mathfrak{A}R_p
\]
for all \( r \geq 1 \). For our choice of \( p \) we must have
\[
M^{s-1}/M^s \subseteq (u_p^{-1}M)^{s-1}/u_p \cdot (u_p^{-1}M)^s
\]
isomorphic to a proper \( R_p \)-submodule of \( (\mathfrak{A}/u_p \mathfrak{A})R_p \). The theorem now follows.

The terminal value \( M^s/M^{s+1} \) of quotients of successive powers of \( M \) is of considerable importance for the applications to group rings below. We are now able to calculate the module index [2], \([M^s : M^{s+1}]\).

**Theorem 4.** With notation as in Theorem 3, for \( r < s \),
\[
[M^r : M^{r+1}] \supset [M^s : M^{s+1}] = \prod_p \left[ R_p : u_p R_p \right].
\]
Here the product is taken over all primes of \( R \), \( \mathcal{B} \) is the maximal order of \( A \) over \( R \) (of course \( u_p \) is a unit in \( \mathcal{B} \) for almost all \( p \)), and the inclusion on the left is strict.

Proof. Without loss of generality we may assume that \( R \) is a local ring, that \( u \in A \) is such that \( 1 \in u^{-1}M \subseteq \mathcal{B} \), and we must now prove that
\[
[M^r : M^{r+1}] \supset [\mathcal{B} : u \mathcal{B}]
\]
with equality if and only if \( r \geq s \).
Now for $r \geq 1$ we have

$$[M^r : M^{r+1}] = [(u^{-1}M)^r : u(u^{-1}M)^{r+1}]$$

$$= [(u^{-1}M)^r : u(u^{-1}M)^r][u^{-1}M^{r+1} : (u^{-1}M)^r]^{-1}$$

$$= [M^r : uM][u^{-1}M^{r+1} : u^{-1}M]^r]^{-1}.$$

The sequence $(u^{-1}M)^r$, $r \geq 1$, is increasing, and stationary if and only if $r \geq s$. Hence

$$[(u^{-1}M)^r : (u^{-1}M)^s] \subseteq R$$

with equality if and only if $r \geq s$. The $R$-ideal $[N : uN]$ depends only on $u$, and not on the $A$-$R$-ideal $N$. The theorem now follows.

**Corollary.** With notation as in Theorem 4,

$$[M^r : M^{r+1}] \supseteq [B : BM]$$

with equality if and only if $r \geq s$.

**Proof.** For each $p$ we have

$$(u_p^{-1}M)BR_p = BR_p$$

hence

$$u_pBR_p = MBR_p.$$}

Therefore $[BR_p : u_pBR_p] = [B : BM]R_p$, and

$$\prod_p [B : BM]R_p = [B : BM].$$

The following generalizes the results of [1] for abelian groups.

**Theorem 5.** Let $G$ be an abelian group, and let $IG$ be the augmentation ideal of the integral group ring $\mathbb{Z}G$. Then there is a positive integer $s$ such that the sequence $IG^r|IG^{r+1}$ of abelian groups is stationary for $r \geq s$. Let $B$ denote the maximal order in $QG$ over $\mathbb{Z}$. Then for $r \geq s$ the order of $IG^r|IG^{r+1}$ is equal to that of the $\mathbb{Z}$-module $[B \cap Q \cdot IG : B \cdot IG]$ regarded as abelian group, while for $r < s$ it is strictly less than this value.

**Proof.** There is a splitting $QG = Qe \oplus Q \cdot IG$, where

$$e = (1/|G|) \sum_{g \in G} g$$

is a primitive idempotent. So $\mathbb{Z}e \oplus IG$ is a $QG$-$\mathbb{Z}$-ideal. There is an integer
\( s \leq d(QG) - 2 \) such that \((Ze \oplus IG)^r = Ze \oplus IG^r\) is invertible for all \( r \geq s \); this is because \( \mathcal{Z}G\)-ideals are componentwise Dedekind [5]. Since \( IG^r \supset IG^{r+1} \) for all \( r \geq 1 \), we may apply Theorem 4 and its Corollary. So for all \( r \geq s \), we have isomorphisms of abelian groups:

\[
IG^r/IG^{r+1} \cong (Ze \oplus IG^r)/(Ze \oplus IG^{r+1}) 
\cong IG^r/IG^{r+1}
\]

for all \( r \geq s \); while for \( r < s \) there can be no isomorphism. Note that \( s \) is also defined by the statement: \( IG^r \cong IG^s \) as \( \mathcal{Z}G\)-modules if and only if \( r \geq s \). The order of the group \( IG^r/IG^{r+1} \) is less than or equal to

\[
\left[ \mathcal{B} : \mathcal{B}(Ze \oplus IG) \right] = \left[ \mathcal{B}e \oplus (\mathcal{B} \cap Q \cdot IG) : \mathcal{B}e \oplus \mathcal{B} \cdot IG \right] = \left[ \mathcal{B} \cap Q \cdot IG : \mathcal{B} \cdot IG \right]
\]

with equality if and only if \( r \geq s \).

Now, for example, it is easy to obtain a result of Passi [4]. We write \( Q_rG = IG^r/IG^{r+1} \).

**Theorem 6.** Let \( G \) be an elementary abelian \( p \)-group of rank \( m \), where \( p \) is an odd prime. Then the terminal value of \( Q_rG \) is an elementary abelian \( p \)-group of rank \( (p^m - 1)/(p - 1) \).

**Proof.** By straightforward calculation, we find representations

\[
\mathcal{B} = Ze \oplus \Sigma \oplus \mathbb{Z}[\theta_i] \\
IG = \Sigma \oplus (1 - \theta_i) \mathbb{Z}[\theta_i];
\]

here \( e = (1/|G|) \sum_{g \in G} g \), the \( \theta_i \) are \( p \)th roots of unity in \( A \), and the sum is taken over \( 1 \leq i \leq (p^m - 1)/(p - 1) \). Since \( [\mathbb{Z}[\theta_i] : (1 - \theta_i) \mathbb{Z}[\theta_i]] = p\mathbb{Z} \), the theorem follows.

Finally, as an application, we confirm a conjecture we made in [8]. Let \( G \) be the direct product of \( k \) cyclic groups of order 4. In [8] we determined a sequence \( P_rG \) of finite abelian groups, of which the \( Q_rG \) were shown to be homomorphic images. We now determine the sequence \( Q_rG \) by establishing:

**Theorem 7.** For all \( r \geq 1 \), \( P_rG = Q_rG \).

**Proof.** It is enough to establish that \( P_qG = Q_qG \) for some \( q \geq s \). For, \( P_rG \) was defined in [8] for each \( r \) on a set of generators of \( Q_rG \), subject to certain relations on the whole sequence of \( Q_rG \). If for any \( r \), \( P_rG \supset Q_rG \), there must be some other relation (obtained as in [8] from an eliminant of polynomials) on the \( Q_rG \), which in turn, since it does not hold for the \( P_rG \), would entail \( P_rG \supset Q_rG \) for all subsequent \( r \).
We set $q = \max(s, 3k - 1)$. By Theorem 2 of [8], $P_qG$ is a group of order $2^h$, where $h = 2^{2k-1} + 2^{k-1} - 1$. Let us calculate the order of $Q_qG$ from Theorem 4, Corollary. It is readily calculated that

$$\mathfrak{B} = \mathbb{Z}e \oplus \Sigma \oplus \mathbb{Z}e_i \oplus \Sigma \oplus \mathbb{Z}[\theta_i]$$

while

$$\mathfrak{B} \cdot IG = \Sigma \oplus 2\mathbb{Z}e_i \oplus \Sigma \oplus (1 - \theta_i) \mathbb{Z}[\theta_i];$$

here $e = (1/|G|) \sum_{g \in G} g$ is a primitive idempotent; the $e_i$ are primitive idempotents, $1 \leq i \leq 2^k - 1$; each $\theta_i$ satisfies $\theta_i^2 = -1$ in $A$; and $1 \leq j \leq 2^{2k-1} - 2^{k-1}$. Since $[\mathbb{Z}[\theta_i] : (1 - \theta_i) \mathbb{Z}[\theta_i]] = 2\mathbb{Z}$, we have

$$[\mathfrak{B} : \mathfrak{B}e \oplus \mathfrak{B} \cdot IG] = 2^t\mathbb{Z},$$

where $t = 2^k - 1 + (2^{2k-1} - 2^{k-1}) = 2^{2k-1} + 2^{k-1} - 1$, proving the theorem.

REFERENCES