On the graded ring associated to integral group rings

Anthony Hayward

Department of Mathematics, King's College London, Strand, London WC2R 2LS.
anthony.hayward@kcl.ac.uk   www.mth.kcl.ac.uk/~hayward

This is a preliminary version of this document.

Abstract

For small finite abelian p-groups we determine, with the help of a computer, the structure of some of the augmentation quotients of the integral group ring $\mathbb{Z}[G]$. We also investigate how much can be learned by projecting to cyclic quotients of G.

1 Introduction

Let p be a prime number and G a finite abelian p-group. $\mathbb{Z}[G]$ denotes the integral group ring of G, and I the augmentation ideal of this ring, defined as the kernel of the augmentation homomorphism

$$\begin{array}{cccc} \text{aug}: & \mathbb{Z}[G] & \longrightarrow & \mathbb{Z} \\ & \sum_{g\in G} n_g g & \longmapsto & \sum_{g\in G} n_g. \end{array}$$

The powers of I form a filtration of $\mathbb{Z}[G]$ by ideals. One wishes to study the structure of the quotients I^d/I^{d+1}. It is well known that I/I^2 is isomorphic to G; in general, the quotients are finitely-generated abelian groups. We observe below that I^d/I^{d+1} is killed by the exponent of G, therefore the quotients are all finite abelian p-groups. Useful structural results are known in the cases where G is cyclic (eg. [1]) and elementary (ie. exponent p) ([8], §3). On the other hand, for general finite abelian groups the quotients decompose according to the Sylow p-subgroups of G ([7], Proposition 3.25). Therefore the main gap in knowledge concerning the quotients I^d/I^{d+1} for finite abelian G is when G is a p-group with exponent greater than p, but which is not cyclic. In this report we discuss how a computer was used to study the structure in this case.

If H is a subgroup of G such that G/H is cyclic, there is a natural surjective homomorphism $\mathbb{Z}[G] \longrightarrow \mathbb{Z}[G/H]$. One might hope that it is sufficient in our case to study the image of I^d/I^{d+1} in all of these quotient rings, where the structure is well-understood. David Burns and Joongul Lee have asked (in private correspondence) whether

$$I^d/I^{d+1} \longrightarrow \prod_H I^d_{G/H}/I^{d+1}_{G/H} \tag{1}$$

is an injection, which is the same as saying that if $x \in \mathbb{Z}[G]$ is in $I^{d+1}_{G/H}$ after projection to each $\mathbb{Z}[G/H]$, then it is in I^{d+1}. This is known to be true in the elementary case ([5], Corollary 5) and obviously in the cyclic case. In fact, it turns out not to be true in general. We will study an example where it fails. This fact has significance for example for those studying the conjecture of Gross [4], showing that its verification cannot easily be reduced to studying cyclic field extensions.

2 Method

2.1 The $\mathbb{Z}$-submodule I^d of $\mathbb{Z}[G]$

Let f be the number of cyclic factors of G and fix a generator $a_i \in G$ for the i-th factor.

Fix an ordering of the elements of G, $g_1, \ldots, g_{\#G}$. Such an ordering gives us an obvious isomorphism of $\mathbb{Z}$-modules

$$\begin{array}{ccc} \mathbb{Z}[G] & \longrightarrow & \mathbb{Z}^{\#G} \\ \sum_i n_i g_i & \longmapsto & (n_i)_i. \end{array}$$

Via this isomorphism we can use linear algebra to study the structure of the augmentation filtrations. Multiplication by an element $x \in \mathbb{Z}[G]$ induces a $\mathbb{Z}$-endomorphism of $\mathbb{Z}[G]$ by $x \sum_i n_i g_i = \sum_i (\sum_j m_{ij} n_j) g_i$, that is, $xy = A_x y$ where $(A_x)_{ij} = m_{ij}$ and y is considered as a vector in $\mathbb{Z}^{\#G}$. On the other hand, for an integer $d \geq 1$, the d-th power I^d of the augmentation ideal is generated over $\mathbb{Z}[G]$ by the finite set

$$S = \{(a_1 - 1)^{r_1}(a_2 - 1)^{r_2} \cdots (a_f - 1)^{r_f} : r_i \geq 0,\ r_1 + \ldots + r_f = d\}.$$

Therefore I^d is equal to the $\mathbb{Z}$-span of the columns of the matrix $A' = (A_{x_1} | \cdots | A_{x_{\#S}})$ where x_i runs through the elements of S. Given A', there exists a unique matrix M_{I^d} in *Hermite Normal Form* ([3], §2.4.2) whose column span over $\mathbb{Z}$ is the same as that of A'. The columns of M_{I^d} form a basis for the free $\mathbb{Z}$-module I^d. We observe that the rank of M_{I^d} is always $\#G - 1$, since this may easily be seen to be the rank of I^1, and the quotients I^d/I^{d+1} are finite.

For any $d \geq 1$, the $\mathbb{Z}$-module I^{d+1} is a submodule of I^d with finite index. Thus it is possible to express the basis $M_{I^{d+1}}$ of I^{d+1} in terms of the basis M_{I^d} of I^d as $M_{I^{d+1}} = M_{I^d} B$, B some $(\#G - 1)$-square matrix with integer entries. B may now be reduced to Smith normal form by elementary row and column operations. If U, V are square invertible matrices over $\mathbb{Z}$ such that $UBV = \operatorname{diag}(d_1, \ldots, d_{\#G-1})$ with $d_1 \mid d_2 \mid \ldots \mid d_{\#G-1}$, d_i positive integers, then $I^d/I^{d+1} \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_{\#G-1}\mathbb{Z}$ and the columns of $M_{I^d} U^{-1}$ are generators of each cyclic factor. In this way the structure of the I^d/I^{d+1} and a minimal set of representatives in $\mathbb{Z}[G]$ were determined.

2.2 Augmentation structures

We do some simple manipulations useful for studying the augmentation filtrations. Let $g \in G$ have order n and write $N_g = \sum_{i=0}^{n-1} g^i$. Then the following equalities are easy to check:

$$(g-1)N_g = 0 \tag{2}$$

$$(g-1)(-g^{n-2} - 2g^{n-3} - 3g^{n-4} - \ldots - (n-2)g - (n-1)) = n - N_g \tag{3}$$

$$(g-1)(n-N_g) = n(g-1) \tag{4}$$

This shows that $n(g-1) \in I^2$, and in particular it proves that I^d/I^{d+1} is annihilated by the exponent of G for $d \geq 1$.

It is easy to "divide" by the augmentation element $(g-1)$ in the group ring $\mathbb{Z}[\langle g \rangle]$. If $y = \sum_{i=0}^{n-1} y_i g^i$ is an element with augmentation 0, then $y = (g-1)x$ where $x = -(y_0) - (y_0 + y_1)g - \ldots - (y_0 + \ldots + y_{n-2})g^{n-2}$. Also, by (2) we may add multiples of N_g to x until its augmentation is in the range $0 \leq \operatorname{aug} x < n$. This then turns out to be uniquely determined by y, and it tells us whether y is in I^2 by the next result.

Proposition 1. *Let Γ be a cyclic group of order p^m generated by γ. Then every $x \in \mathbb{Z}[\Gamma]$ has a unique expression*

$$x = \sum_{i=0}^{\infty} x_i(\gamma - 1)^i$$

with $0 \leq x_i < p^m$ for $i > 0$.

Proof. It is obvious by the above that such an expression exists, with $x_0 = \operatorname{aug}(x)$. Suppose $\sum x_i'(\gamma-1)^i$ is a different expression for x. Let r be the first i where $x_i' \neq x_i$ and assume (without loss of generality) that $0 < t := x_i' - x_i$. Then $t(\gamma-1)^r \in I^{r+1}$. But multiplication by $\gamma - 1$ induces an isomorphism $I^d \longrightarrow I^{d+1}$ for all $d \geq 1$ (see eg. [6], Lemma 3). Hence $t(\gamma - 1) \in I^2$. But this means $\gamma^t = 1$ in G, which is impossible since $0 < t < p^m$. Hence the expression for x is unique. □

Thus we see that by iterating the above process we can find the highest power of the augmentation ideal containing a given element of $\mathbb{Z}[\langle g \rangle]$. This method is used to determine the kernel of the map (1).

3 Results

3.1 Cyclic quotients do not suffice

In this section we show that the map (1) is not always injective.

Let $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ be the smallest odd, non-elementary, non-cyclic p-group. Write $a = (1,0)$ and $b = (0,1)$ for the generators of the first and second cyclic factors respectively. We will first determine all the nontrivial cyclic quotients of G. The subgroups H such that G/H is cyclic are easily seen to be the kernels of the characters $\chi : G \longrightarrow \mathbb{C}^\times$. Since G has exponent 9, the image of any χ is contained in the group of 9th roots of unity, which is isomorphic to $\mathbb{Z}/9\mathbb{Z}$. So we consider all homomorphisms $\omega : G \longrightarrow \mathbb{Z}/9\mathbb{Z}$.

$\omega(a) = 0$, 3 or 6. Firstly assume $\omega(a) = 0$, so $b \in H := \ker \omega$. The order of $\omega(b)$ is either 1, 3 or 9. If $\omega(b) = 0$ then $H = G$ gives the trivial quotient, which we denote by Γ_0. If $\omega(b)$ has order 3 then $H = \langle a, b^3 \rangle$ giving quotient Γ_1. Otherwise $H = \langle a \rangle$, giving quotient Γ_2.

Note that the Galois group $\mathfrak{G} = (\mathbb{Z}/9\mathbb{Z})^\times$ acts on $\mathbb{Z}/9\mathbb{Z}$ and permutes the ω, the kernel being an invariant of the orbit. Every character with $\omega(a) = 6$ is in the same orbit as a character with $\omega(a) = 3$ by the action of $-1 \in \mathfrak{G}$. So we may assume $\omega(a) = 3$ to find the rest of the kernels. Now the possible $\mathfrak{G}$-orbits of $\omega(b)$ are $\{0\}$, $\{1,4,7\}$, $\{2,5,8\}$,$\{3\}$ and $\{6\}$, giving subgroups as follows:

$\omega(b)$	0	1	2	3	6
H	$\langle b\rangle$	$\langle a^2b^3\rangle$	$\langle ab^3\rangle$	$\langle a^2b\rangle$	$\langle ab\rangle$
G/H name	Γ_3	Γ_4	Γ_5	Γ_6	Γ_7

Thus there are 7 nontrivial cyclic quotients $\Gamma_1, \ldots, \Gamma_7$.

We now present an element which shows that the map (1) is not injective for $d = 5$. Let

$$x := 2(a-1)^2(b-1)^3 + (a-1)^4(b-1).$$

Then $x \in I^5$ is clear. It is also clear that x projects to 0 in $\mathbb{Z}[\Gamma_1], \mathbb{Z}[\Gamma_2]$ and $\mathbb{Z}[\Gamma_3]$ since the corresponding H contains a or b. So we wish to show it projects to an element of $I^6_{\Gamma_i}$ in $\mathbb{Z}[\Gamma_i]$ for $i = 4, 5, 6, 7$. The fastidious reader may wish to check the following table (in which σ denotes the stated generator of the cyclic quotient Γ_i):

Quotient	σ	$\#\Gamma_i$	$\bar{x}$
Γ_4	b	9	$(\sigma-1)^6(12+15\sigma+10\sigma^2+\sigma^3-9\sigma^4$ $-14\sigma^5-13\sigma^6-6\sigma^7+4\sigma^8)$
Γ_5	$\bar{b}$	9	$(\sigma-1)^6(5-3\sigma-8\sigma^2-9\sigma^3-6\sigma^4$ $-2\sigma^5+4\sigma^6+9\sigma^7+10\sigma^8)$
Γ_6	$\bar{a}$	3	$(\sigma-1)^6(-1+\sigma^2)$
Γ_7	$\bar{a^2}$	3	$(\sigma-1)^6$

Therefore x is in the kernel of the map (1). On the other hand, x is not in I^6. This is proved as follows: the matrix M_{I^6} whose columns form a Hermite normal form basis for the $\mathbb{Z}$-module $I^6 \subseteq \mathbb{Z}[G]$ has top-right entry -51. But reducing the matrix $(M_{I^6}|x)$ to Hermite normal form produces a matrix with top-right entry -53. Because the Hermite normal form is an invariant of the $\mathbb{Z}$-span of the columns of the matrix, this shows that $x \notin I^6$. Therefore x is a nontrivial element of the kernel of the map (1).

We remark furthermore that all the proper quotients of G are cyclic or elementary. Since the map (1) is known to be injective for G elementary, this shows that $x \in I^6_{G/H}$ for *all* proper subgroups H.

3.2 Explicit structures

The following table shows the structure of the first few augmentation quotients for some small p-groups. The notation $C_a^b C_c^d$ is short for $(\mathbb{Z}/a\mathbb{Z})^b \times (\mathbb{Z}/c\mathbb{Z})^d$. K denotes the kernel of the map (1). Where the size of K is not recorded it is equal to 1.

We observe that it is proved in [2] that the decomposition of the quotients I^d/I^{d+1} is eventually constant. This can be seen in the following table for the smaller groups.

G	$\#G$	I^2/I^3	I^3/I^4	I^4/I^5	I^5/I^6	I^6/I^7	I^7/I^8
C_2C_4	8	$C_2^2C_4$	$C_2^3C_4$	$C_2^3C_4$	$C_2^3C_4$	$C_2^3C_4$	$C_2^3C_4$
C_4C_4	16	C_4^3	$C_2C_4^3$	$C_2^2C_4^3$	$C_2^3C_4^3$	$C_2^3C_4^3$	$C_2^3C_4^3$
C_2C_8	16	$C_2^2C_8$	$C_2^3C_8$	$C_2^4C_8$ $\#K=2$	$C_2^4C_8$ $\#K=2$	$C_2^4C_8$ $\#K=2$	$C_2^4C_8$ $\#K=2$
$C_2C_2C_4$	16	$C_2^5C_4$	$C_2^8C_4$	$C_2^9C_4$ $\#K=2$	$C_2^9C_4$ $\#K=2$	$C_2^9C_4$ $\#K=2$	$C_2^9C_4$ $\#K=2$
C_4C_8	32	$C_4^2C_8$	$C_4^3C_8$	$C_2C_4^3C_8$	$C_2^2C_4^3C_8$	$C_2^3C_4^3C_8$ $\#K=2$	$C_2^4C_4^3C_8$ $\#K=4$
$C_2C_4C_4$	32	$C_2^3C_4^3$	$C_2^7C_4^3$	$C_2^{10}C_4^3$ $\#K=2$	$C_2^{12}C_4^3$ $\#K=4$	$C_2^{13}C_4^3$ $\#K=8$	$C_2^{13}C_4^3$ $\#K=8$
C_8C_8	64	C_8^3	$C_4C_8^3$	$C_4^2C_8^3$	$C_4^3C_8^3$	$C_2C_4^3C_8^3$ $\#K=2$	$C_2^2C_4^3C_8^3$ $\#K=4$
C_3C_9	27	$C_3^2C_9$	$C_3^3C_9$	$C_3^4C_9$	$C_3^5C_9$ $\#K=3$	$C_3^5C_9$ $\#K=3$	$C_3^5C_9$ $\#K=3$
C_9C_9	81	C_9^3	C_9^4	$C_3C_9^4$	$C_3^2C_9^4$	$C_3^3C_9^4$	$C_3^4C_9^4$
C_3C_{27}	81	$C_3^2C_{27}$	$C_3^3C_{27}$	$C_3^4C_{27}$	$C_3^5C_{27}$ $\#K=3$	$C_3^6C_{27}$ $\#K=9$	$C_3^7C_{27}$ $\#K=27$
C_9C_{27}	243	$C_9^2C_{27}$	$C_9^3C_{27}$	$C_9^4C_{27}$	$C_9^5C_{27}$ $\#K=3$	$C_3C_9^5C_{27}$ $\#K=3$	$C_3^2C_9^5C_{27}$ $\#K=3$
C_5C_{25}	125	$C_5^2C_{25}$	$C_5^3C_{25}$	$C_5^4C_{25}$	$C_5^5C_{25}$	$C_5^6C_{25}$	$C_5^7C_{25}$ $\#K=5$

4 Technical Notes

The computer program used to produce the results in this paper is available from the author's website http://www.mth.kcl.ac.uk/~hayward. It uses the package PARI to compute the Hermite normal form of matrices. PARI is available from here: http://www.parigp-home.de/.

Portability problems may be caused by the two routines at the bottom of the file aug.cpp. These are hacks to fill the omission in PARI of conversion routines between the C++ type "long long" (intended here to be a 64-bit number) and the PARI type "t_INT". These routines will have to be rewritten if the program is to be run on a big-endian processor (eg. SPARC, Macintosh) or a 64-bit processor, or if new versions of PARI change the structure of t_INT.

The program needs PARI to have been compiled and installed. The program was successfully run on a 32-bit Pentium-based Linux system with PARI v2.1.4.

The complexity of the calculations performed by the program increases rapidly with the integers $\#G$ and d. As these numbers increase, the program becomes very slow, and the matrix calculations unwieldy even for a computer. Also, the sizes of the quotient groups become large, making the calculation of $\#K$ slow. For example, we tested every element of the quotient I^7/I^8 for the group $G = \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$, which number $14,348,907$. On a modern (2002) computer with a 1.7GHz processor, this took 40 minutes.

The program could be improved by using PARI to calculate the Smith normal form (our method is efficient but is limited by 64-bit numbers), or analysing K using techniques of linear algebra.

References

[1] F. Bachmann and L. Grünenfelder, *Über Lie-Ringe von Gruppen und ihre universellen Enveloppen*, Comment. Math. Helv. **47** (1972), 332-240.

[2] F. Bachmann and L. Grünenfelder, *The periodicity in the graded ring associated with an integral group ring*, J. Pure and Applied Algebra **5** (1974), 253-264.

[3] Henri Cohen, *A Course in Computational Algebraic Number Theory* (Springer GTM 128), Springer Verlag 1996.

[4] Benedict H. Gross, *On the values of abelian L-functions at s=0*, J. Fac. Sci. Univ. Tokyo, Sect 1A, Math. **35** (1988) 177-197.

[5] Joongul Lee, *On Gross's refined class number formula for elementary abelian extensions*, J. Math. Sci. Univ. Tokyo **4** (1997), 373-383.

[6] Joongul Lee, *Stickelberger element for cyclic extensions*, preprint.

[7] Inder Bir S. Passi, *Polynomial maps on groups*, J. Algebra **9** (1968), 121-151.

[8] Inder Bir S. Passi and Lekh Raj Vermani, *The associated graded ring of an integral group ring*, Math. Proc. Camb. Phil. Soc. **82** (1977), 25-33.