Honam Mathematical J. **45** (2023), No. 4, pp. 678–681
https://doi.org/10.5831/HMJ.2023.45.4.678

A FORMAL DERIVATION ON INTEGRAL GROUP RINGS FOR CYCLIC GROUPS

Joongul Lee

Abstract. Let G be a cyclic group of prime power order p^k, and let I be the augmentation ideal of the integral group ring $\mathbb{Z}[G]$. We define a derivation on $\mathbb{Z}/p^k\mathbb{Z}[G]$, and show that for $2 \leq n \leq p$, an element $\alpha \in I$ is in I^n if and only if the i-th derivative of the image of α in $\mathbb{Z}/p^k\mathbb{Z}[G]$ vanishes for $1 \leq i \leq (n-1)$.

1. Introduction

Let G be a finite abelian group, and let I be the augmentation ideal of $\mathbb{Z}[G]$, which is the kernel of the augmentation map

$$\epsilon \colon \mathbb{Z}[G] \to \mathbb{Z}$$
$$\epsilon(\sum_{g\in G} a_g g) = \sum_{g \in G} a_g.$$

For $\alpha \in \mathbb{Z}[G]$ and a positive integer n, it is of considerable interest to determine whether $\alpha \in I^n$. The Stickelberger element is used by Iwasawa to construct the p-adic L-functions for cyclotomic $\mathbb{Z}_p$-extensions of number fields, therefore the arithmetic properties of the Stickelberger elements may give important information on the p-adic L-functions. See [1], [2] for example.

2. Reduction modulo p^k

Let G be a cyclic group of order p^k for a prime p, and let A be the commutative ring $\mathbb{Z}/p^k\mathbb{Z}$. Reducing the coefficients of elements of $\mathbb{Z}[G]$ modulo p^k, we have the map

$$\pi \colon \mathbb{Z}[G] \to A[G]$$

which is a surjective ring homomorphism.

Let I be the augmentation ideal of $\mathbb{Z}[G]$, and let J be the augmentation ideal of $A[G]$. It is clear that π sends I onto J, I^n onto J^n, and therefore

Received April 11, 2023. Accepted May 28, 2023.
2020 Mathematics Subject Classification. 16S34, 20C05.
Key words and phrases. integral group ring, augmentation ideal.
This work was supported by 2019 Hongik University Research Fund.

induces a surjective homomorphism from I^n/I^{n+1} to J^n/J^{n+1} for a positive integer n.

Proposition 1. *For $1 \le n \le p-1$, π induces an isomorphism from I^n/I^{n+1} to J^n/J^{n+1}.*

Proof. Let σ be a generator of G and let $\tau = \sigma - 1$. It is well-known that I^n/I^{n+1} is a cyclic $\mathbb{Z}$-module of order p^k generated by τ^n. Similarly, J^n/J^{n+1} is a cyclic A-module generated by τ^n, therefore we need to show that the annihilator of J^n/J^{n+1} as an A-module is (0) for $1 \le n \le p-1$.

Note that

$$A[G] \cong A[x]/(x^{p^k} - 1),$$

where σ maps to x. If we make a change of variable using $\tau = \sigma - 1$, we obtain

$$A[G] \cong A[x]/((x+1)^{p^k} - 1), \tag{1}$$

where τ maps to x. Let

$$\phi(x) = (x+1)^{p^k} - 1 = \sum_{i=1}^{p^k} \binom{p^k}{i} x^i \in A[x].$$

The isomorphism (1) implies that for $f(x) \in A[x]$, $f(\tau) = 0$ in $A[G]$ if and only if $f(x)$ is divisible by $\phi(x)$ in $A[x]$.

Let $l \in A$. l annihilates J^n/J^{n+1} if and only if $l\tau^n$ can be written as a linear combination of τ^i for $i > n$, which is equivalent to the existence of a multiple of $\phi(x)$ in $A[x]$ whose term with lowest degree is lx^n. As the coefficient of x^i in $\phi(x)$ is 0 for $i \le p-1$, it is impossible to find a multiple of $\phi(x)$ in $A[x]$ which has term with degree lower than p. Therefore, for $1 \le n \le p-1$, J^n/J^{n+1} is an additive cyclic group of order p^k, and the induced map from I^n/I^{n+1} to J^n/J^{n+1} is an isomorphism for $1 \le n \le p-1$. ☐

3. Derivation on $A[G]$

Let us first consider

$$d\colon A[x] \to A[x]$$

$$d\Big(\sum_{i=0}^{p^k-1} a_i x^i\Big) = \sum_{i=0}^{p^k-1} i a_i x^{i-1}.$$

It is straightforward to verify that for $f, g \in A[x]$,

$$d(f+g) = df + dg,$$
$$d(fg) = fdg + gdf,$$

from which it follows that if

$$f \equiv g \pmod{(x^{p^k} - 1)},$$

then

$$df \equiv dg \pmod{(x^{p^k}-1)},$$

as $d(x^{p^k}-1)=0$ in $A[x]$.

We fix a generator σ of G, and define

$$D\colon A[G] \to A[G],$$
$$D(\sum_{i=0}^{p^k-1} a_i\sigma^i) = \sum_{i=0}^{p^k-1} i a_i \sigma^{i-1}.$$

The above discussion implies that D is a well-defined A-derivation on $A[G]$.

For $\alpha \in A[G]$ and a positive integer n, we adopt the notations $\alpha^{(n)} = D^n\alpha$ and $\alpha^{(n)}(\epsilon) = \epsilon(D^n\alpha)$. We also adopt the notation $\alpha^{(0)} = \alpha$.

Theorem 2. *Suppose α is an element of J. For $2 \le n \le p$, $\alpha \in J^n$ if and only if $\alpha^{(i)}(\epsilon) = 0$ for $1 \le i \le n-1$.*

Proof. We prove the theorem by mathematical induction on n.

For $n = 2$, let us write

$$\alpha = \beta\tau = \beta(\sigma - 1).$$

Then $D\alpha = \tau D\beta + \beta$, so $\alpha^{(1)}(\epsilon) = \epsilon(\beta)$ from which the result follows.

Let us assume that the theorem holds for $n \le k$ with $2 \le k \le p-1$. Suppose $\alpha = \beta\tau^k$. Using Leibniz's law we have

$$\alpha^{(k)} = \sum_{i=0}^{k} \binom{k}{i} \frac{k!}{i!} \beta^{(i)}\tau^i$$

from which we get $\alpha^{(k)}(\epsilon) = k! \cdot \epsilon(\beta)$. As $k!$ is a unit in A, we get $\alpha^{(k)}(\epsilon) = 0$ if and only if $\beta \in J$, in other words $\alpha \in J^{k+1}$. □

Combining Proposition 1 and Theorem 2, we get the following

Theorem 3. *For $\alpha \in I$ and $2 \le n \le p$, $\alpha \in I^n$ if and only if $(\pi\alpha)^{(i)}(\epsilon) = 0$ for $1 \le i \le n-1$.*

Remarks. 1. Theorem 3 does not hold for $n = p+1$. For $\alpha = p^{k-1}\tau^p$, $(\pi\alpha)^{(i)} = 0$ for all $i \ge 1$ but $\alpha \notin I^{p+1}$.

2. Our definition of the derivation D depends on the choice of the generator of G. One can use "chain rule" to prove that while the value $D\alpha$ depends on the choice of the generator, the fact that $\epsilon(D\alpha) = 0$ is independent of the choice of the generator. Hence the statement of Theorem 2 and Theorem 3 remains valid if another generator of G is used to define the derivation.

References

[1] B. H. Gross, *On the values of abelian L-functions at $s = 0$*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **35** (1988), no. 1, 177–197.

[2] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, VOl. 83, Second Edition, Springer-Verlag, New York, 1997.

Joongul Lee
Department of Mathematics Education, Hongik University,
Mapo-gu Wausan-ro 94, Seoul, 04066, Republic of Korea.
E-mail: jglee@hongik.ac.kr