Commun. Korean Math. Soc. **30** (2015), No. 1, pp. 1–5
http://dx.doi.org/10.4134/CKMS.2015.30.1.001

# CHARACTERIZATION OF A CYCLIC GROUP RING IN TERMS OF CHARACTER VALUES

Joongul Lee

Abstract. Let $G$ be a cyclic group of prime power order. There is a natural embedding of $\mathbb{Z}[G]$ into a product of rings of integers of cyclotomic fields. In this paper the image of the embedding is determined, and we also compute the index of the image.

## 1. Introduction

For a finite abelian group $G$ let $\mathbb{Z}[G]$ be the integral group ring of $G$, and let $I_G$ be the augmentation ideal. For each complex character $\chi$ of $G$ let $\mathbb{Q}(\chi)$ be the cyclotomic field generated by the values of $\chi$ and $\mathbb{Z}[\chi]$ be its ring of integers.

Consider

$$\Phi : \mathbb{Z}[G] \longrightarrow \prod_{\chi\in\widehat{G}} \mathbb{Z}[\chi]$$

$$\Phi(\alpha) = (\ldots, \chi(\alpha), \ldots),$$

where the domain of $\chi$ is extended to $\mathbb{Z}[G]$ by linearity. The map $\Phi$ is an injective ring homomorphism. The goal of this paper is to determine $\Phi(\mathbb{Z}[G])$ when $G$ is cyclic of prime power order.

For an element

$$\beta = (\ldots, \beta_\chi, \ldots) \in \prod_{\chi\in\widehat{G}} \mathbb{Z}[\chi],$$

let us refer to its components $\beta_\chi$ as the character values of $\beta$. We find that, when $G$ is cyclic of prime power order, we can express the necessary and sufficient condition for $\beta \in \Phi(\mathbb{Z}[G])$ as congruence relations among the character values of $\beta$. As a byproduct, we also compute the index of $\Phi(\mathbb{Z}[G])$ in $\prod \mathbb{Z}[\chi]$.

There are refined type of conjectures on the values of $L$-functions (cf. [1], [2], [4], [5]) which predict (among others) that certain elements of $\prod_{\chi\in\widehat{G}} \mathbb{Z}[\chi]$ whose character values come from special values of $L$-functions belong to $\Phi(I_G^n)$

Received August 20, 2014.
2010 *Mathematics Subject Classification.* 16S34, 20C05.
*Key words and phrases.* group rings.
This work was supported by 2013 Hongik University Research Fund.

for a prescribed positive integer $n$. The author hopes that the result of this paper offers an aid in understanding the meaning of those very deep conjectures in concrete situations.

## 2. Cyclic case

Fix a prime $p$ and a positive integer $k$. Let $G$ be a cyclic group of order $p^k$ with generator $\sigma$. Let $H$ be the subgroup of $G$ of order $p$, and let $\overline{\sigma}$ be the element $\sigma$ modulo $H$. Let us choose a complex character $\chi_k$ of $G$ with order $p^k$, and for $0 \leq i \leq k-1$ we inductively define $\chi_i = \chi_{i+1}^p$ so that the order of $\chi_i$ is $p^i$. We may view $\chi_i$ as complex characters of $G/H$ for $i < k$. We also set $\zeta_i = \chi_i(\sigma)$ and $\lambda_i = \zeta_i - 1$.

Consider

$$\Phi : \mathbb{Z}[G] \longrightarrow \prod_{i=0}^{k} \mathbb{Z}[\zeta_i]$$
$$\Phi(\alpha) = (\chi_0(\alpha), \ldots, \chi_k(\alpha))$$

and

$$\overline{\Phi} : \mathbb{Z}[G/H] \longrightarrow \prod_{i=0}^{k-1} \mathbb{Z}[\zeta_i]$$
$$\overline{\Phi}(\alpha) = (\chi_0(\alpha), \ldots, \chi_{k-1}(\alpha)).$$

We need the following generalization of the Chinese remainder theorem, the proof of which can be found in [3].

**Proposition 1.** *Let $R$ be a commutative ring with 1, and $I, J$ be ideals of $R$. There exists a short exact sequence of $R$-modules*

$$0 \to R/(I \cap J) \to R/I \times R/J \to R/(I+J) \to 0,$$

*where the first map sends $r \bmod (I \cap J)$ to $(r \bmod I, r \bmod J)$ and the second sends $(r_1 \bmod I, r_2 \bmod J)$ to $r_1 - r_2 \bmod (I+J)$.*

Let $\phi_i(x)$ be the $p^i$-th cyclotomic polynomial. Note that there is a natural isomorphism from $\mathbb{Z}[x]/(x^{p^k}-1)$ to $\mathbb{Z}[G]$ that sends $x$ to $\sigma$, and from $\mathbb{Z}[x]/(\phi_i(x))$ to $\mathbb{Z}[\zeta_i]$ sending $x$ to $\zeta_i$. Via these identifications, it is useful to view $\Phi$ and $\overline{\Phi}$ as the natural maps

$$\Phi : \mathbb{Z}[x]/(x^{p^k}-1) \longrightarrow \prod_{i=0}^{k} \mathbb{Z}[x]/(\phi_i(x)),$$
$$\overline{\Phi} : \mathbb{Z}[x]/(x^{p^{k-1}}-1) \longrightarrow \prod_{i=0}^{k-1} \mathbb{Z}[x]/(\phi_i(x)).$$

Let us apply Proposition 1 to the case $R = \mathbb{Z}[x]$, $I = (x^{p^{k-1}}-1)$, $J = (\phi_k(x))$. We have

$$x^{p^k} - 1 = (x^{p^{k-1}} - 1)\phi_k(x),$$

hence

$$I \cap J = IJ = (x^{p^k} - 1)$$

as ideals of $\mathbb{Z}[x]$, because $\mathbb{Z}[x]$ is a unique factorization domain and the polynomials $x^{p^{k-1}} - 1$ and $\phi_k(x)$ have no common irreducible factor. On the other hand, it is clear that

$$\phi_k(x) \equiv p \bmod (x^{p^{k-1}} - 1),$$

which implies

$$I + J = (\phi_k(x),\, x^{p^{k-1}} - 1) = (p,\, x^{p^{k-1}} - 1).$$

Let us consider the ring homomorphism

$$\psi_k : \mathbb{Z}[\zeta_k] \longrightarrow \mathbb{Z}[G/H]/p\mathbb{Z}[G/H]$$
$$\psi_k(\sum a_j \zeta_k^j) := \sum a_j \overline{\sigma}^j \bmod p\mathbb{Z}[G/H].$$

This map comes from the isomorphisms

$$\mathbb{Z}[x]/(I + J) \cong (\mathbb{Z}[x]/J)/((I + J)/J) \cong (\mathbb{Z}[x]/I)/((I + J)/I),$$

hence we may identify $\mathbb{Z}[\zeta_k]/(\lambda_1)$ with $\mathbb{Z}[G/H]/p\mathbb{Z}[G/H]$. $\psi_k$ is surjective with $\ker(\psi_k) = (\lambda_1)$. The following theorem is now a direct consequence of Proposition 1.

**Theorem 2.** *Let $\alpha = (\alpha_0, \dots, \alpha_k)$ be an element of $\prod_{i=0}^{k} \mathbb{Z}[\zeta_i]$. $\alpha$ is in $\Phi(\mathbb{Z}[G])$ if and only if the following conditions hold*;

(i) $(\alpha_0, \dots, \alpha_{k-1}) = \overline{\Phi}(\eta)$ *for some* $\eta \in \mathbb{Z}[G/H]$,

(ii) $\eta \in \psi_k(\alpha_k)$.

**Corollary 3.** $\Phi(\mathbb{Z}[G])$ *has index* $p^{(p^k-1)/(p-1)}$ *in* $\prod_{i=0}^{k} \mathbb{Z}[\zeta_i]$.

*Proof.* When $k = 0$, $\Phi$ is clearly surjective so the statement holds. In general, $\Phi(\mathbb{Z}[G])$ has index

$$|\mathbb{Z}[G/H]/p\mathbb{Z}[G/H]| = p^{p^{k-1}}$$

in $\overline{\Phi}(\mathbb{Z}[G/H]) \times \mathbb{Z}[\zeta_k]$ which follows from condition (ii) of Theorem 2. We obtain the result by mathematical induction on $k$. □

Let us analyze condition (ii) of Theorem 2 in more detail. Define

$$\kappa_k = Z[\zeta_k] \longrightarrow (\prod_{i=0}^{k-1} \mathbb{Z}[\zeta_i])/\overline{\Phi}(p\mathbb{Z}[G/H])$$
$$\kappa_k(\alpha_k) := \overline{\Phi}(\psi_k(\alpha_k)) \bmod \overline{\Phi}(p\mathbb{Z}[G/H]).$$

As $\overline{\Phi}$ is injective, condition (ii) of Theorem 2 holds if and only if

$$(\alpha_0, \dots, \alpha_{k-1}) \in \kappa_k(\alpha_k). \tag{1}$$

For $\alpha_k = \sum a_j \zeta_k^j$ and for $0 \le i \le k-1$, let

$$\kappa_k(\alpha_k)_i = \sum a_j \zeta_i^j.$$

Each element $\kappa_k(\alpha_k)_i$ is not well defined in general, but

$$(\kappa_k(\alpha_k)_0, \ldots, \kappa_k(\alpha_k)_{k-1})$$

is well defined modulo $\overline{\Phi}(p\mathbb{Z}[G/H])$ and it belongs to $\kappa_k(\alpha_k)$, hence $\kappa_k(\alpha_k)_i$ is defined modulo $p$.

Relation (1) is now equivalent to the following congruence relation

$$(\alpha_0, \ldots, \alpha_{k-1}) \equiv (\kappa_k(\alpha_k)_0, \ldots, \kappa_k(\alpha_k)_{k-1}) \bmod \overline{\Phi}(p\mathbb{Z}[G/H]). \tag{2}$$

The following theorem is now a direct consequence of the above discussion, and enables us to determine $\Phi(\mathbb{Z}[G])$ inductively.

**Theorem 4.** *Let $\alpha = (\alpha_0, \ldots, \alpha_k)$ be an element of $\prod_{i=0}^{k} \mathbb{Z}[\zeta_i]$. $\alpha$ is in $\Phi(\mathbb{Z}[G])$ if and only if the following conditions hold;*

(i) *$(\alpha_0, \ldots, \alpha_{k-1})$ is in $\overline{\Phi}(\mathbb{Z}[G/H])$,*
(ii) *$\alpha_i \equiv \kappa_k(\alpha_k)_i \pmod p$ for $0 \le i \le k-1$,*
(iii) *$\frac{1}{p}(\alpha_0 - \kappa_k(\alpha_k)_0, \ldots, \alpha_{k-1} - \kappa_k(\alpha_k)_{k-1})$ is in $\overline{\Phi}(\mathbb{Z}[G/H])$.*

## 3. A few cases

In this section, we record the explicit condition for $\alpha$ to be in $\Phi(\mathbb{Z}[G])$, following Theorem 4.

**Corollary 5.** *($k = 1$) $\alpha = (\alpha_0, \alpha_1)$ is in $\Phi(\mathbb{Z}[G])$ if and only if*

$$\alpha_0 \equiv \kappa_1(\alpha_1)_0 \pmod p.$$

*$\alpha$ is in $\Phi(p\mathbb{Z}[G])$ if and only if the following conditions hold;*

(i) *$\alpha_i = p\beta_i$ for some $\beta_i \in \mathbb{Z}[\zeta_i]$ for $i = 0, 1$,*
(ii) *$\beta_0 \equiv \kappa_1(\beta_1)_0 \pmod p$.*

**Corollary 6.** *($k = 2$) $\alpha = (\alpha_0, \alpha_1, \alpha_2)$ is in $\Phi(\mathbb{Z}[G])$ if and only if the following conditions hold;*

(i) *$\alpha_0 \equiv \kappa_1(\alpha_1)_0 \pmod p$,*
(ii) *$\alpha_i \equiv \kappa_2(\alpha_2)_i \pmod p$ for $i = 0, 1$,*
(iii) *$(\alpha_0 - \kappa_2(\alpha_2)_0)/p \equiv \kappa_1((\alpha_1 - \kappa_2(\alpha_2)_1)/p)_0 \pmod p$.*

*Therefore $\alpha$ is in $\Phi(p\mathbb{Z}[G])$ if and only if the following conditions hold;*

(iv) *$\alpha_i = p\beta_i$ for some $\beta_i \in \mathbb{Z}[\zeta_i]$ for $i = 0, 1, 2$,*
(v) *$(\beta_0, \beta_1, \beta_2)$ satisfies the above conditions (i)-(iii).*

**Corollary 7.** *($k = 3$) $\alpha = (\alpha_0, \alpha_1, \alpha_2, \alpha_3)$ is in $\Phi(\mathbb{Z}[G])$ if and only if the following conditions hold;*

(i) *$\alpha_0 \equiv \kappa_1(\alpha_1)_0 \pmod p$,*
(ii) *$\alpha_i \equiv \kappa_2(\alpha_2)_i \pmod p$ for $i = 0, 1$,*
(iii) *$(\alpha_0 - \kappa_2(\alpha_2)_0)/p \equiv \kappa_1((\alpha_1 - \kappa_2(\alpha_2)_1)/p)_0 \pmod p$,*
(iv) *$(\alpha_0 - \kappa_3(\alpha_3)_0, \alpha_1 - \kappa_3(\alpha_3)_1, \alpha_2 - \kappa_3(\alpha_3)_2)$ satisfies condition (iv), (v) of Corollary 6.*

*Remark.* The congruence relations in $\mathbb{Z}[\zeta_i]$ can be made more explicit using the integral basis $\{1, \lambda_i, \lambda_i^2, \ldots, \lambda_i^{l-1}\}$ where $l = p^{i-1}(p-1)$. Let

$$\alpha = \sum_{j=0}^{l-1} a_j \lambda_i^j, \quad a_j \in \mathbb{Z} \text{ for } 0 \le j \le l-1.$$

Using the discrete valuation on $\mathbb{Z}[\zeta_i]$ with local uniformizer $\lambda_i$, it is easy to see that

$$\alpha \equiv 0 \pmod p \Longleftrightarrow a_j \equiv 0 \pmod p \text{ for } 0 \le j \le l-1.$$

## References


[1] D. Burns, *Congruences between derivatives of abelian $L$-functions at $s = 0$*, Invent. Math. **169** (2007), no. 3, 451–499.

[2] 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.

[3] J. Lee, *Congruences of $L$-values for cyclic extensions*, Honam Math. J. **32** (2010), no. 4, 791–795.

[4] B. Mazur and J. Tate, *Refined conjectures of the "Birch and Swinnerton-Dyer type"*, Duke Math. J. **54** (1987), no. 2, 711–750.

[5] K. Rubin, *A Stark conjecture "over* **Z***" for abelian $L$-functions with multiple zeros*, Ann. Inst. Fourier (Grenoble) **46** (1996), no. 1, 33–62.



Department of Mathematics Education
Hongik University
Seoul 72-1, Korea
*E-mail address*: jglee@hongik.ac.kr