Bull. Korean Math. Soc. **59** (2022), No. 6, pp. 1511–1522
https://doi.org/10.4134/BKMS.b210864
pISSN: 1015-8634 / eISSN: 2234-3016

MODIFIED CYCLOTOMIC POLYNOMIALS

Ae-Kyoung Cha, Miyeon Kwon, Ki-Suk Lee, and Seong-Mo Yang

Abstract. Let H be a subgroup of $\mathbb{Z}_n^*$ (the multiplicative group of integers modulo n) and $h_1, h_2, \ldots, h_l$ distinct representatives of the cosets of H in $\mathbb{Z}_n^*$. We now define a polynomial $J_{n,H}(x)$ to be

$$J_{n,H}(x) = \prod_{j=1}^{l} \left(x - \sum_{h \in H} \zeta_n^{h_j h} \right),$$

where $\zeta_n = e^{\frac{2\pi i}{n}}$ is the nth primitive root of unity. Polynomials of such form generalize the nth cyclotomic polynomial $\Phi_n(x) = \prod_{k \in \mathbb{Z}_n^*} (x - \zeta_n^k)$ as $J_{n,\{1\}}(x) = \Phi_n(x)$. While the nth cyclotomic polynomial $\Phi_n(x)$ is irreducible over $\mathbb{Q}$, $J_{n,H}(x)$ is not necessarily irreducible. In this paper, we determine the subgroups H for which $J_{n,H}(x)$ is irreducible over $\mathbb{Q}$.

1. Introduction

Let n be a positive integer and $\zeta_n = e^{\frac{2\pi i}{n}}$ be the nth primitive root of unity. The polynomial

$$\Phi_n(x) = \prod_{k \in \mathbb{Z}_n^*} (x - \zeta_n^k),$$

where $\mathbb{Z}_n^*$ is the multiplicative group of integers modulo n, is called the nth cyclotomic polynomial over $\mathbb{Q}$. It is well known (e.g. see [8]) that $\Phi_n(x) \in \mathbb{Z}[x]$ with $\Phi_n(\zeta_n) = 0$ and is irreducible over $\mathbb{Q}$.

To generalize the notion of cyclotomic polynomials, let H be a subgroup of $\mathbb{Z}_n^*$ and $h_1, h_2, \ldots, h_l$ distinct representatives of the cosets of H in $\mathbb{Z}_n^*$. We now define a polynomial $J_{n,H}(x)$ to be

$$J_{n,H}(x) = \prod_{j=1}^{l} \left(x - \sum_{h \in H} \zeta_n^{h_j h} \right).$$

Received December 1, 2021; Revised April 11, 2022; Accepted May 2, 2022.
2020 *Mathematics Subject Classification.* Primary 12E05.
Key words and phrases. Cyclotomic polynomials, irreducible polynomials, Gauss sum.
This work was financially supported by the 2021 Sabbatical Leave Research Grant funded by Korea National University of Education.

The polynomial $J_{n,H}(x)$ is a monic polynomial with integer coefficients. Particularly, if we take $H = \{1\}$, then $J_{n,H}(x) = \Phi_n(x)$. While the nth cyclotomic polynomial $\Phi_n(x)$ is irreducible over $\mathbb{Q}$, $J_{n,H}(x)$ is not necessarily irreducible over $\mathbb{Q}$.

This paper aims to determine the subgroups of $\mathbb{Z}_n^*$ for which $J_{n,H}(x)$ is irreducible over $\mathbb{Q}$. Some special cases have already been studied. For $n = p_1 p_2 \cdots p_r$, where $p_1, \ldots, p_r$ are distinct primes, Kwon et al. [7] showed that any polynomial of the form $J_{n,H}(x)$ is irreducible over $\mathbb{Q}$. Shin et al. [9] have established some criteria on H for the irreducibility of $J_{n,H}(x)$ in the case of $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, where $\alpha_j > 1$, adopting Evan's work in [3]. Diamond et al. [2] have generalized Evan's result. In their paper, they determined the subgroups H of $\mathbb{Z}_q^*$ for which the $|H| \times |H|$ matrix defined by $\{q^{-\frac{1}{2}} \zeta_q^{-nm}\}_{n,m \in H}$ is invertible.

In this paper, we relate the results in Diamond et al.'s paper to the irreducibility of $J_{n,H}(x)$ for an arbitrary positive integer n. We show that the conditions on H in [2] are equivalent to $J_{n,H}$ being irreducible over $\mathbb{Q}$.

To state the main result, we define $v := v(n)$ to be the divisor of n determined by

$$v(n) = \begin{cases} \prod_{p \mid n} p & \text{if } 8 \nmid n, \\ 2 \prod_{p \mid n} p & \text{if } 8 \mid n, \end{cases} \tag{1}$$

where the products run over distinct primes p which divide n. For examples, $v(2^2 \cdot 5^3 \cdot 7) = 2 \cdot 5 \cdot 7$ and $v(2^5 \cdot 3 \cdot 5^2) = 2(2 \cdot 3 \cdot 5)$. It follows from a simple calculation that $v(m \cdot n) = v(m) \cdot v(n)$ whenever m and n are coprime. Subsequently, we let

$$U(n) = \{m \in \mathbb{Z}_n^* : m \equiv 1 \pmod{v(n)}\}. \tag{2}$$

Hasse [5] has established the important roles of $U(n)$ in describing the structure of the multiplicative group of integers modulo n. In fact, the relation of H to $U(n)$, particularly $H \cap U(n)$, determines the irreduciblity of $J_{n,H}$ as stated in the following.

Main Result. *Let H be a proper subgroup of $\mathbb{Z}_n^*$. Then the following conditions are equivalent.*

(i) $\sum_{h \in H} \zeta_n^h \neq 0$.
(ii) $H \cap U(n) = \{1\}$.
(iii) $\{\zeta_n^h : h \in H\}$ *are linearly independent over* $\mathbb{Q}$.
(iv) $\sum_{h \in H} \zeta_n^h \neq \sum_{h \in H} \zeta_n^{kh}$ *whenever* $k \notin H$.
(v) $J_{n,H}(x)$ *is irreducible over* $\mathbb{Q}$.

In Section 2, we gather some properties of $J_{n,H}(x)$ and characterize the irreducibility of $J_{n,H}(x)$ over $\mathbb{Q}$ in view of Galois group of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$. In Section 3, we connect $H \cap U(n)$ to $\sum_{h \in H} \zeta_n^h$, which is known as a Gauss sum

associated with H. In Section 4, we discuss the relation between $H \cap U(n)$ and the linear independence of $\{\zeta_n^h : h \in H\}$ over $\mathbb{Q}$. Lastly, we put together the results from Sections 2-4 to give a complete proof of the main theorem in Section 5.

Throughout the paper, n denotes a positive integer and $\zeta_n = e^{\frac{2\pi i}{n}}$ is the nth primitive root of unity. Following the conventional notations, $\mathbb{Q}$, $\mathbb{Q}[x]$, $\mathbb{Q}(\zeta_n)$, and $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ denote the field of rational numbers, the polynomial ring over $\mathbb{Q}$, and the simple extension field of $\mathbb{Q}$ containing ζ_n, and the Galois group of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$, respectively.

2. Polynomials $J_{n,H}(x)$

In this section, we show that $J_{n,H}(x)$ belongs to $\mathbb{Z}[x]$. We also characterize the irreducible polynomials $J_{n,H}(x)$ in view of the Galois group of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$, which is the set of all isomorphisms of $\mathbb{Q}(\zeta_n)$ that fix $\mathbb{Q}$ pointwise.

It is well known (e.g. see [1]) that $\mathbb{Z}_n^* \cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ via the mapping $k \in \mathbb{Z}_n^* \mapsto \sigma_k \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ satisfying $\sigma_k(\zeta_n) = \zeta_n^k$. Thus $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \{\sigma_k : k \in \mathbb{Z}_n^*\}$ equipped with group operation $\sigma_k \circ \sigma_l = \sigma_{kl}$. For the remaining paper, σ_k denotes the isomorphism on $\mathbb{Q}(\zeta_n)$ defined as such.

Theorem 2.1. *Let H be a subgroup of $\mathbb{Z}_n^*$ and $h_1, h_2, \ldots, h_l$ be distinct representatives of the cosets of H in $\mathbb{Z}_n^*$. Then $J_{n,H}(x) = \prod_{j=1}^{l} \left(x - \sum_{h\in H} \zeta_n^{h_j h}\right) \in \mathbb{Q}[x]$. Furthermore, $J_{n,H}(x) \in \mathbb{Z}[x]$.*

Proof. We first note that $\sum_{h\in H} \zeta_n^{h_j h} = \sum_{t\in h_j H} \zeta_n^t$. This means that $J_{n,H}(x)$ is determined by cosets of H and not by the coset representatives $h_1, h_2, \ldots, h_l$. In regard to the cosets, $J_{n,H}(x)$ can be written as $J_{n,H}(x) = \prod_{j=1}^{l} \left(x - \sum_{t\in H_j} \zeta_n^t\right)$, where $H_j,\ j = 1, \ldots, l$ are the cosets of H in $\mathbb{Z}_n^*$.

For each $k \in \mathbb{Z}_n^*$, $\{kH_j : j = 1, \ldots, l\} = \{H_j : j = 1, \ldots, l\}$. Consequently, we have

$$\prod_{j=1}^{l} \Big(x - \sigma_k\Big(\sum_{t\in H_j} \zeta_n^t\Big)\Big) = \prod_{j=1}^{l} \Big(x - \sum_{t\in H_j} \zeta_n^{kt}\Big)$$
$$= \prod_{j=1}^{l} \big(x - \sum_{t\in kH_j} \zeta_n^t\big) \ = \ \prod_{j=1}^{l} \big(x - \sum_{t\in H_j} \zeta_n^t\big).$$

We have just showed that the coefficients of $J_{n,H}(x)$ are invariant over all $\sigma_k \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Therefore, $J_{n,H}(x) \in \mathbb{Q}[x]$.

To see $J_{n,H}(x) \in \mathbb{Z}[x]$, note that each coefficient of $J_{n,H}(x)$ is of the form $c_0 + c_1\zeta_n + \cdots + c_m\zeta_n^m$ with $c_j \in \mathbb{Z}$. We shall show that any rational number of such form must be an integer.

Suppose $c_0 + c_1\zeta_n + \cdots + c_m\zeta_n^m = q \in \mathbb{Q}$, where $c_j \in \mathbb{Z}$. Define a polynomial $P(x)$ as $P(x) = c_0 + c_1x + \cdots + c_mx^m$. Clearly, $P(x) \in \mathbb{Z}[x]$ by its construction.

Dividing $P(x)$ by the nth cyclotomic polynomial $\Phi_n(x) = \prod_{k\in\mathbb{Z}_n^*}(x-\zeta_n^k) \in \mathbb{Z}[x]$, we get

$$P(x) = Q(x)\Phi_n(x) + R(x), \tag{3}$$

where $R(x) \in \mathbb{Z}[x]$ of degree less than $\varphi(n)$. Here $\varphi(n)$ is the Euler's totient function. By substituting x with ζ_n in the equation (3), we have $q = R(\zeta_n)$ equivalently $R(\zeta_n) - q = 0$. This implies that $R(x) - q$ is a polynomial in $\mathbb{Q}[x]$ with ζ_n as its zero. Since $\Phi_n(x)$ is the minimal polynomial of ζ_n over $\mathbb{Q}$ (i.e., the monic irreducible polynomial over $\mathbb{Q}$ with ζ_n as its zero), we can conclude that $R(x) - q$ is the zero polynomial, implying $q = R(0)$. Since $R(x) \in \mathbb{Z}[x]$, $q \in \mathbb{Z}$. This completes the proof. □

Let $h_1, \ldots, h_l$ be the distinct representatives of the cosets of H in $\mathbb{Z}_n^*$ and $\eta = \sum_{h\in H}\zeta_n^h$. Then we can express $J_{n,H}(x)$ as $J_{n,H}(x) = \prod_{j=1}^{l}\big(x - \sigma_{h_j}(\eta)\big)$, where σ_{h_j} denotes the isomorphism in $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ satisfying $\sigma_{h_j}(\zeta_n) = \zeta_n^{h_j}$.

In what follows, we characterize the irreducible polynomials of the form $J_{n,H}(x)$ with respect to $\sigma_k(\eta)$ for $\sigma_k \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Theorem 2.2. *Let H be a proper subgroup of $\mathbb{Z}_n^*$ and $h_1(=1), h_2, \ldots, h_l$ be distinct representatives of the cosets of H in $\mathbb{Z}_n^*$. Suppose $\eta := \sum_{h\in H}\zeta_n^h$. Then the following conditions are equivalent.*

(i) $J_{n,H}(x) = \prod_{j=1}^{l}\big(x - \sigma_{h_j}(\eta)\big)$ *is irreducible over* $\mathbb{Q}$.
(ii) $\sigma_{h_j}(\eta)$, $j = 1, \ldots, l$, *are distinct.*
(iii) $\eta \neq \sigma_k(\eta)$ *whenever* $k \notin H$.

Proof. It is known (see [4, 6]) that $\mathbb{Q}(\zeta_n)$ is a finite normal extension of $\mathbb{Q}$. It means that for any $\alpha \in \mathbb{Q}(\zeta_n)$, the minimal polynomial of α over $\mathbb{Q}$ (i.e., the monic irreducible polynomial in $\mathbb{Q}[x]$ that has α as its zero) splits into non-repeated linear factors in $\mathbb{Q}(\zeta_n)$.

Suppose $P(x)$ is the minimal polynomial of η over $\mathbb{Q}$. Then $P(\sigma(\eta)) = 0$ for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ (see [4]) and $P(x)$ has no repeated zeros. As a result, each $\big(x - \sigma_{h_j}(\eta)\big)$ divides $P(x)$. Moreover, $\sigma_{h_j}(\eta)$, $j = 1, \ldots, l$, are distinct if and only if $J_{n,H}(x) = \prod_{j=1}^{l}\big(x - \sigma_{h_j}(\eta)\big)$ divides $P(x)$, which is equivalent to $J_{n,H}(x) = P(x)$ since $J_{n,H}(x) \in \mathbb{Q}[x]$ with η as its zero. We just have showed (i) ⇔ (ii).

To show (ii) ⇔ (iii), we first suppose that $\sigma_{h_j}(\eta)$, $j = 1, \ldots, l$, are distinct. If $k \notin H$, then $k \in h_jH$ for some $h_j \neq 1$ and so $kH = h_jH$. This implies that $\sigma_k(\eta) = \sigma_{h_j}(\eta) \neq \eta$. Conversely, we assume that $\eta \neq \sigma_k(\eta)$ whenever $k \notin H$. Contrary to the statement (ii), suppose that $\sigma_{h_j}(\eta) = \sigma_{h_k}(\eta)$ but $h_j \neq h_k$. Then, by applying the inverse of σ_{h_j} to the equation, we get $\eta = \sigma_{\tilde{h_j}}(\sigma_{h_k}(\eta)) = \sigma_{\tilde{h_j}h_k}(\eta)$, where $\tilde{h_j}$ is the multiplicative inverse of h_j modulo n. Since h_j and h_k are representatives of distinct cosets of H, $\tilde{h_j}h_k \notin H$. This contradicts to (iii). □

3. $U(n)$ and the Gauss sum

In this section, we review some important properties of $U(n)$ which are defined in (2). The results in this section are not new and can be found in several literatures (e.g. [2] and [5]). While we do not wish to recap already established results, there are important components of which we shall make considerable use. For that reason, we present the proofs that are relevant to the later arguments.

If $n = p^\alpha$ is a prime power with $p \neq 2$, the order of $\mathbb{Z}_n^*$, $\varphi(n) = p^{\alpha-1}(p-1)$, is decomposed into two coprime factors $p-1$ and $p^{\alpha-1}$. Therefore, $\mathbb{Z}_n^*$ is the direct product of the two cyclic subgroups $L(n)$ and $U(n)$ of orders $p-1$ and $p^{\alpha-1}$, respectively. Since $\mathbb{Z}_n^*$ is cyclic, such decomposition is unique and they consist of all elements whose orders divide $p-1$ and $p^{\alpha-1}$, respectively. In other words, $U(n) = \{u \in \mathbb{Z}_n^* : u^{p^{\alpha-1}} \equiv 1 \pmod{n}\}$ and

$$L(n) = \{l \in \mathbb{Z}_n^* : l^{p-1} \equiv 1 \pmod{n}\}. \tag{4}$$

Hasse [5] obtained the explicit representations for $L(n)$ and $U(n)$ from the homomorphisms of $\mathbb{Z}_n^*$.

Theorem 3.1 (Hasse [5])**.** *Let $n = p^\alpha$ be a prime power with $p \neq 2$. Then $\mathbb{Z}_n^* \cong L(n) \times U(n)$ is the direct product of the two cyclic subgroups $L(n)$ and $U(n)$ of orders $p-1$ and $p^{\alpha-1}$, respectively. Those subgroups can be expressed explicitly as $L(n) = \{l \in \mathbb{Z}_n^* : l \equiv a^{p^{\alpha-1}} \pmod{n}$ for $a \in \mathbb{Z}_n^*\}$ and $U(n) = \{u \in \mathbb{Z}_n^* : u \equiv 1 \pmod{p}\}$, as defined in* (2).

Proof. As we discussed previously, the implicit representations for the subgroups in question are $L(n) = \{l \in \mathbb{Z}_n^* : l^{p-1} \equiv 1 \pmod{n}\}$ and $U(n) = \{u \in \mathbb{Z}_n^* : u^{p^{\alpha-1}} \equiv 1 \pmod{n}\}$. To express the subgroups explicitly, we consider the mapping $\tau : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ defined by $\tau(a) \equiv a^{p^{\alpha-1}} \pmod{n}$. Then τ is a homomorphism of $\mathbb{Z}_n^*$ with the kernel of τ, $\ker(\tau) = U(n)$, and hence $\mathbb{Z}_n^*/U(n) \cong \tau(\mathbb{Z}_n^*)$. Since $\mathbb{Z}_n^*$ is cyclic, the subgroup of order $p-1$ is unique and thus $L(n) = \tau(\mathbb{Z}_n^*)$. On the other hand, the mapping $\mu : \mathbb{Z}_n^* \to \mathbb{Z}_p^*$ defined by $\mu(a) \equiv a \pmod{p}$ provides a homomorphism of $\mathbb{Z}_n^*$ onto $\mathbb{Z}_p^*$ with $\ker(\mu) = \{a \in \mathbb{Z}_n^* : a \equiv 1 \pmod{p}\}$. Since the order of $\mathbb{Z}_p^*$, denoted by $|\mathbb{Z}_p^*|$, is $p-1$, we find that $|\ker(\mu)| = p^{\alpha-1}$. Since $\mathbb{Z}_n^*$ is cyclic, by virtue of uniqueness we obtain $U(n) = \{a \in \mathbb{Z}_n^* : a \equiv 1 \pmod{p}\}$. □

For $n > 1$, let $v(n)$ and $U(n)$ be defined as in (1) and (2), respectively. Then, the assertion regarding $U(n)$ in Theorem 3.1 still holds for the general case: $U(n)$ is a cyclic subgroup of $\mathbb{Z}_n^*$ of order $n/v(n)$.

If $n = 2$ or 2^2, then $v(n) = 2$ and thus $U(n) = \mathbb{Z}_n^*$. If $n = 2^\alpha$, $\alpha \geq 3$, then $v(n) = 4$ and so $U(n) = \{1 + 4k : k = 0, \ldots, 2^{\alpha-2} - 1\}$ has order $2^{\alpha-2}$. Hasse showed in [5] that $U(n)$ is a cyclic group generated by $1 + 2^2$. Therefore, the claim is true when $n = p^\alpha$ is any prime power, including $p = 2$.

For the case $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, where $p_1 < p_2 < \cdots < p_r$ are distinct primes, we have $\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{\alpha_1}}^* \times \cdots \mathbb{Z}_{p_r^{\alpha_r}}^*$ via the mapping

$$m \mapsto (m \pmod{p_1^{\alpha_1}}, \ \ldots, \ m \pmod{p_r^{\alpha_r}}).$$

Since $u \equiv 1 \pmod{v(n)}$ if and only if $u \equiv 1 \pmod{v(p_j^{\alpha_j})}$, $j = 1, \ldots, r$, the mapping restricted to $U(n)$ induces an isomorphism from $U(n)$ onto $U(p_1^{\alpha_1}) \times \cdots \times U(p_r^{\alpha_r})$. Recall that each $U(p_j^{\alpha_j})$ is a cyclic group of order $p_j^{\alpha_j}/v(p_j^{\alpha_j})$ and p_j's are distinct primes. Hence, $U(n)$ is cyclic of order $\prod(p_j^{\alpha_j}/v(p_j^{\alpha_j})) = \frac{n}{v(n)}$ as $v(q_1 q_2) = v(q_1)v(q_2)$ when $(q_1, q_2) = 1$.

The group $U(n)$ has been considered as a multiplicative subgroup of $\mathbb{Z}_n^*$. It also has an additive structure that we can take advantage of. The set $U(n)$ is a coset of the additive subgroup $\{m \in \mathbb{Z}_n : m \equiv 0 \pmod{v(n)}\}$ of $\mathbb{Z}_n$, where $\mathbb{Z}_n$ denotes the ring of integers modulo n. Due to this additive property in $U(n)$, any subgroup H of $\mathbb{Z}_n^*$ containing a nontrivial element of $U(n)$ has the Gauss sum nullified.

Theorem 3.2 (Diamond et al. [2])**.** *Let H be a subgroup of $\mathbb{Z}_n^*$. If $H \cap U(n) \neq \{1\}$, then $\sum_{h \in H} \zeta_n^h = 0$.*

Proof. Let $d = |H \cap U(n)|$ with $d > 1$, where $|\cdot|$ denotes the number of elements in the given set. Since $H \cap U(n)$ is a subgroup of $U(n)$, d is a divisor of $|U(n)| = \frac{n}{v(n)}$, and then $\frac{n}{d}$ is a multiple of $v(n)$ since $\frac{n}{d} = \frac{(n/v(n))}{d} v(n)$. We now let $K = \{m \in \mathbb{Z}_n^* : m \equiv 1 \pmod{\frac{n}{d}}\}$; then

$$K = \Big\{1, 1 + \Big(\frac{n}{d}\Big), 1 + 2\Big(\frac{n}{d}\Big), \ldots, 1 + (d-1)\Big(\frac{n}{d}\Big)\Big\}.$$

Since $\frac{n}{d}$ is a multiple of $v(n)$, it is clear that K is a subgroup of $U(n)$ with $|K| = d$. Since $U(n)$ is cyclic and thus contains exactly one subgroup of order d, we get $K = H \cap U(n)$. Let $h_1, h_2, \ldots, h_{\frac{|H|}{d}}$ denote distinct representatives of the cosets of K in H. We then have

$$\begin{aligned}
\sum_{h \in H} \zeta_n^h &= \sum_{j=1}^{\frac{|H|}{d}} \left(\sum_{k \in K} \zeta_n^{h_j k} \right) \\
&= \sum_{j=1}^{\frac{|H|}{d}} \left(\sum_{l=0}^{d-1} \zeta_n^{h_j \left(1 + l\left(\frac{n}{d}\right)\right)} \right) \\
&= \sum_{j=1}^{\frac{|H|}{d}} \zeta_n^{h_j} \left(\sum_{l=0}^{d-1} \left(\zeta_n^{h_j \frac{n}{d}}\right)^l \right) = \sum_{j=1}^{\frac{|H|}{d}} \zeta_n^{h_j} \left(\frac{1 - (\zeta_n^{h_j \frac{n}{d}})^d}{1 - \zeta_n^{\frac{n}{d}}} \right) = 0,
\end{aligned}$$

since $(\zeta_n^{h_j \frac{n}{d}})^d = \zeta_n^{h_j n} = 1$ and $d > 1$. □

Theorem 3.2 implies that $H \cap U(n) = \{1\}$ is a necessary condition for $J_{n,H}(x)$ to be irreducible over $\mathbb{Q}$. In the following section, we shall see if it is sufficient for the irreducibility of $J_{n,H}(x)$.

4. $U(n)$ and linear independence of $\{\zeta_n^h : h \in H\}$ over $\mathbb{Q}$

In this section, we gather some properties of a subgroup $H \subset \mathbb{Z}_n^*$ satisfying $H \cap U(n) = \{1\}$. We then relate the condition $H \cap U(n) = \{1\}$ to the linear independence of $\{\zeta_n^h : h \in H\}$ over $\mathbb{Q}$, which allows us to prove the irreducibility of $J_{n,H}(x)$ in the later section.

Lemma 4.1. *Let H be a subgroup of $\mathbb{Z}_n^*$ satisfying $H \cap U(n) = \{1\}$. Then the following statements hold.*

(i) *$|H|$ divides $\varphi(v(n))$.*
(ii) *$h^{\varphi(v(n))} \equiv 1 \pmod{n}$ for each $h \in H$.*
(iii) *If $n = p^\alpha$ is a power of odd prime, then $H \subset L(n)$, where $L(n)$ is defined in (4).*

Proof. Throughout the proof, $v(n)$ and $U(n)$ are denoted by v and U, respectively. Define a map $\tau : \mathbb{Z}_n^* \to \mathbb{Z}_v^*$ by $\tau(k) = k \pmod{v}$. Then τ is a homomorphism with $\ker(\tau) = U$. Thus $H \cap U = \{1\}$ implies that the homomorphism τ restricted to H is one-to-one, equivalently $H \cong \tau(H)$. Since $\tau(H)$ is a subgroup of $\mathbb{Z}_v^*$, $|\tau(H)|$ is a divisor of $\varphi(v)$ and thus $(\tau(h))^{\varphi(v)} \equiv \tau(h^{\varphi(v)}) \equiv 1 \pmod{v}$ for each $h \in H$. Since H and $\tau(H)$ are isomorphic, (i) and (ii) follow.

In particular, if $n = p^\alpha$ is a power of odd prime, it follows from (ii) that $H \cap U = \{1\}$ implies $h^{p-1} \equiv 1 \pmod{p^\alpha}$. Thus, $h \in L(n)$ for any $h \in H$. The proof is completed. □

To describe what the condition $H \cap U(n) = \{1\}$ says about $\{\zeta_n^h : h \in H\}$, we begin with the case $n = p^\alpha$, where p is an odd prime. For the case $n = p^\alpha$, it follows from Lemma 4.1(iii) that $L(n)$ is the maximum subgroup satisfying $H \cap U(n) = \{1\}$. Thus, it is reasonable to start with $L(n)$.

Theorem 4.2. *Suppose that $n = p^\alpha$ is a power of odd prime. Then $\{\zeta_n^h : h \in L(n)\}$ are linearly independent over $\mathbb{Q}(\zeta_m)$, where ζ_m is an mth primitive root of unity and $(m, n) = 1$.*

Proof. For each $h \in L(p^\alpha)$, there exist integers $q(h), r(h)$ such that $h = q(h)p + r(h)$ and $0 \le r(h) < p$. Moreover, the correspondence $h \mapsto r(h)$ is bijective from $L(p^\alpha)$ to $\{1, \ldots, p-1\}$ as follows. If $r(h_1) = r(h_2)$, then $h_1 \equiv h_2 \pmod{p}$. By multiplying both sides by the multiplicative inverse $\tilde{h_1}$ of h_1 modulo p^α, we have $1 \equiv h_2\tilde{h_1} \pmod{p}$. This implies $h_2\tilde{h_1} \in U(p^\alpha) \cap L(p^\alpha)$ since $\tilde{h_1}$ and h_2 are in $L(p^\alpha)$. Since $U(p^\alpha) \cap L(p^\alpha) = \{1\}$, $h_2\tilde{h_1} \equiv 1 \pmod{p^\alpha}$ and thus $h_2 \equiv h_1 \pmod{p^\alpha}$. We have just showed that $h \mapsto r(h)$ is one-to-one. But $|L(p^\alpha)| = p - 1$ by Theorem 3.1 and $r(h) \neq 0$ since $(h, p) = 1$. Thus $\{r(h) : h \in L(p^\alpha)\} = \{1, 2, \ldots, p-1\}$.

We now suppose, contrary to the statement, that there are $c_j \in \mathbb{Q}(\zeta_m)$, but not all zero, such that $\sum_{h\in L(n)} c_j\zeta_n^h = 0$. Then

$$0 = \sum_{h\in L(n)} c_j\zeta_n^h = \sum_{h\in L(n)} c_j\zeta_{p^{\alpha-1}}^{q(h)}\zeta_n^{r(h)} = \zeta_n \sum_{h\in L(n)} c_j\zeta_{p^{\alpha-1}}^{q(h)}\zeta_n^{r(h)-1},$$

where $q(h)$ and $r(h)$ are the quotient and the remainder after diving h by p as defined at the start of the proof.

Let $P(x) = \sum_{h\in L(n)} c_j\zeta_{p^{\alpha-1}}^{q(h)}x^{r(h)-1}$. Then $P(x)$ is a nonzero polynomial in $\mathbb{Q}(\zeta_{p^{\alpha-1}}, \zeta_m)[x]$ with degree strictly less than $p-1$ and $P(\zeta_n) = 0$. However, $[\mathbb{Q}(\zeta_{p^\alpha}, \zeta_m) : \mathbb{Q}] = \varphi(p^\alpha)\varphi(m)$ and $[\mathbb{Q}(\zeta_{p^{\alpha-1}}, \zeta_m) : \mathbb{Q}] = \varphi(p^{\alpha-1})\varphi(m)$, where $[F : \mathbb{Q}]$ denotes the degree of the extension field F over $\mathbb{Q}$. This implies that $[\mathbb{Q}(\zeta_{p^\alpha}, \zeta_m) : \mathbb{Q}(\zeta_{p^{\alpha-1}}, \zeta_m)] = \frac{\varphi(p^\alpha)}{\varphi(p^{\alpha-1})}$, which is $p-1$ if $\alpha = 1$ and p otherwise. Thus a nonzero polynomial in $\mathbb{Q}(\zeta_{p^{\alpha-1}}, \zeta_m)[x]$ that vanishes at ζ_n must have degree at least $p-1$: this leads to a contradiction. □

The following is an immediate consequence from Theorem 4.2.

Corollary 4.3. *Let $n = p^\alpha$ be a prime power. If H is a subgroup of $\mathbb{Z}_n^*$ satisfying $H \cap U(n) = \{1\}$, then $\{\zeta_n^h : h \in H\}$ are linearly independent over $\mathbb{Q}(\zeta_m)$, where ζ_m is an mth primitive root of unity and $(m, n) = 1$.*

Proof. If $n = p^\alpha$ with $p > 2$, then $H \subset L(n)$ by Lemma 4.1. In Theorem 4.2, we have showed $\{\zeta_n^h : h \in L(n)\}$ are linearly independent over $\mathbb{Q}(\zeta_m)$. Thus, it is clear that $\{\zeta_n^h : h \in H\}$ are linearly independent over $\mathbb{Q}(\zeta_m)$.

To complete the proof, we only need to deal with the case $n = 2^\alpha$. If $\alpha = 1$ or 2, then $U(n) = \mathbb{Z}_n^*$ and hence $H \cap U(n) = \{1\}$ implies $H = \{1\}$; it is trivial. We now suppose that $n = 2^\alpha$ and $\alpha \geq 3$. In this case, it follows from Lemma 4.1 that $H \cap U(n) = \{1\} \Rightarrow |H|$ divides $\varphi(4) = 2$. Hence, $H = \{1\}$ or $\{1, a\}$ for some $a \in \mathbb{Z}_n^*$ of order 2. If $H = \{1\}$, it is obvious as before. For the latter case $H = \{1, a\}$, we can assume $1 < a < n$. Suppose not: that is, $\{\zeta_n,\ \zeta_n^a\}$ are linearly dependent over $\mathbb{Q}(\zeta_m)$. Then $\zeta_n^{a-1} \in \mathbb{Q}(\zeta_m)$. Since $[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_m)] = \varphi(n)$, the minimal polynomial of ζ_n over $\mathbb{Q}(\zeta_m)$ has degree equal to $\varphi(n)$. Hence $\zeta_n^{a-1} \in \mathbb{Q}(\zeta_m)$ implies that $a-1$ is a multiple of $\varphi(n) = 2^{\alpha-1}$ and so $a = 2^{\alpha-1} + 1$, which is in $U(n)$. This contradicts to $H \cap U(n) = \{1\}$. □

In what follows, we deal with the general case when n is an arbitrary positive integer. The arguments presented here are credited to Diamond et al. in [2].

Lemma 4.4. *Let H be a subgroup of $\mathbb{Z}_n^*$ and ζ_m be an mth primitive root of unity with $(m, n) = 1$. Then $\{\zeta_n^h : h \in H\}$ are linearly independent over $\mathbb{Q}(\zeta_m)$ if and only if $\{\zeta_n^{kh} : h \in H\}$ are linearly independent over $\mathbb{Q}(\zeta_m)$ for any $k \in \mathbb{Z}_n^*$.*

Proof. This can be shown by sending a given set through the Galois isomorphism σ_k of $\mathbb{Q}(\zeta_m, \zeta_n)$ over $\mathbb{Q}(\zeta_m)$ such that $\sigma_k(\zeta_m) = \zeta_m$ and $\sigma_k(\zeta_n) = \zeta_n^k$. □

Lemma 4.5. *Let $n = mp^\alpha$, where $(m, p) = 1$ and p is the largest prime factor of n with $p > 2$. Let the mappings τ_1 and τ_2 be the canonical homomorphisms of $\mathbb{Z}_n^*$ to $\mathbb{Z}_m^*$ and $\mathbb{Z}_{p^\alpha}^*$, respectively. That is, $\tau_1(t) \equiv t \pmod m$ and $\tau_2(t) \equiv t \pmod{p^\alpha}$. If H is a subgroup of $\mathbb{Z}_n^*$ satisfying $H \cap U(n) = \{1\}$, then the followings hold.*

(i) $\tau_2(H) \subset L(p^\alpha)$.
(ii) *If $K = \{k \in H : k \equiv 1 \pmod{p^\alpha}\}$, then $K \simeq \tau_1(K)$ and $\tau_1(K) \cap U(m) = \{1\}$.*

Proof. By Lemma 4.1, $H \cap U(n) = \{1\}$ implies $h^{\varphi(v(n))} \equiv 1 \pmod n$ for each $h \in H$. Consequently, $\tau_2(h^{\varphi(v(n))}) \equiv (\tau_2(h))^{\varphi(v(n))} \equiv 1 \pmod{p^\alpha}$. On the other hand, $(\tau_2(h))^{\varphi(p^\alpha)} \equiv 1 \pmod{p^\alpha}$ by Euler's Theorem. Thus, the order of $\tau_2(h)$ modulo p^α is a common factor of $\varphi(v(n))$ and $\varphi(p^\alpha)$. Since p is the largest prime factor of n with $p > 2$, $\big(\varphi(v(m)), p\big) = 1$ and thus $\big(\varphi(v(n)), \varphi(p^\alpha)\big) = (p-1)\big(\varphi(v(m)), p^{\alpha-1}\big) = p - 1$. This implies that the order of $\tau_2(h)$ modulo p^α divides $p - 1$. As a result, $\tau_2(h) \in L(p^\alpha)$ for each $h \in H$.

For (ii), we note that K is a subgroup of H as $K = H \cap \ker(\tau_2)$. The first assertion in (ii) follows from $\ker(\tau_1) \cap K = \{1\}$. For the second assertion, suppose $t \in \tau_1(K) \cap U(m)$. Then, for some $k \in K$, $t \equiv k \pmod m$ and $t \equiv 1 \pmod{v(m)}$. Since $t \equiv k \pmod m$ implies $t \equiv k \pmod{v(m)}$, we have $k \equiv 1 \pmod{v(m)}$. On the other hand, $k \equiv 1 \pmod{p^\alpha}$ by the definition of K. Consequently, $k \equiv 1 \pmod{v(p^\alpha)}$. Since $(v(m), v(p^\alpha)) = 1$, $k \equiv 1 \pmod{v(mp^\alpha)}$, implying $k \in U(n)$. Recalling K is a subgroup of H, we can assert that $k \equiv 1 \pmod n$. Thus $k \equiv 1 \pmod m$. As a result, $t \equiv k \equiv 1 \pmod m$. □

Theorem 4.6. *Let H be a subgroup of $\mathbb{Z}_n^*$ satisfying $H \cap U(n) = \{1\}$. Then $\{\zeta_n^h : h \in H\}$ are linearly independent over $\mathbb{Q}$.*

Proof. By Corollary 4.3, it is true if $n = p^\alpha$ is a power of prime. For the sake of induction on r, assume that the statement holds for $n = p_1^{\alpha_1} \cdots p_{r-1}^{\alpha_{r-1}}$, where $p_1 < p_2 < \cdots < p_{r-1}$ are distinct primes. We then claim that it is also true for $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, where $p_1 < p_2 < \cdots < p_r$ are distinct primes.

Let $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, where $p_1 < p_2 < \cdots < p_r$ are distinct primes and $r > 1$. We denote $q_1 = p_1^{\alpha_1} \cdots p_{r-1}^{\alpha_{r-1}}$ and $q_2 = p_r^{\alpha_r}$. Suppose $\sum_{h \in H} c_h \zeta_n^h = 0$, where $c_h \in \mathbb{Q}$.

Since $(q_1, q_2) = 1$, there exist integers x and y such that $xq_1 \equiv 1 \pmod{q_2}$ and $yq_2 \equiv 1 \pmod{q_1}$. Let the mappings τ_1 and τ_2 be canonical homomorphisms of $\mathbb{Z}_n^*$ to $\mathbb{Z}_{q_1}^*$ and $\mathbb{Z}_{q_2}^*$, respectively, as before. That is, $\tau_1(t) \equiv t \pmod{q_1}$ and $\tau_2(t) \equiv t \pmod{q_2}$. Then, each $t \in \mathbb{Z}_n^*$ can be expressed as $t \equiv yq_2\tau_1(t) + xq_1\tau_2(t) \pmod n$. As a result,

$$\sum_{h \in H} c_h \zeta_n^h = \sum_{h \in H} c_h \zeta_{q_1}^{y\tau_1(h)} \zeta_{q_2}^{x\tau_2(h)}.$$

We now let $K = \{h \in H : h \equiv 1 \pmod{q_2}\}$. Then K is a subgroup of H. If we let $h_1, \ldots, h_l$ be the representatives of the cosets of K in H, then $h \in h_j K \Rightarrow \tau_2(h) = \tau_2(h_j)$. Therefore,

$$\begin{aligned}\sum_{h\in H} c_h \zeta_n^h &= \sum_{h\in h_1 K} c_h \zeta_{q_1}^{y\tau_1(h)} \zeta_{q_2}^{x\tau_2(h)} + \cdots + \sum_{h\in h_l K} c_h \zeta_{q_1}^{y\tau_1(h)} \zeta_{q_2}^{x\tau_2(h)} \\ &= \left(\sum_{h\in h_1 K} c_h \zeta_{q_1}^{y\tau_1(h)}\right) \zeta_{q_2}^{x\tau_2(h_1)} + \cdots + \left(\sum_{h\in h_l K} c_h \zeta_{q_1}^{y\tau_1(h)}\right) \zeta_{q_2}^{x\tau_2(h_l)}.\end{aligned}$$

By Lemma 4.5, $\{\tau_2(h_j) : j = 1, \ldots, l\} \subset L(q_2)$. It then follows from Theorem 4.3 that $\{\zeta_{q_2}^{\tau_2(h_1)}, \ldots, \zeta_{q_2}^{\tau_2(h_l)}\}$ are linearly independent over $\mathbb{Q}(\zeta_{q_1})$. So are $\{\zeta_{q_2}^{x\tau_2(h_1)}, \ldots, \zeta_{q_2}^{x\tau_2(h_l)}\}$ by Lemma 4.4. We then have

$$\sum_{h\in H} c_h \zeta_n^h = 0 \Rightarrow \sum_{h\in h_j K} c_h \zeta_{q_1}^{y\tau_1(h)} = 0 \text{ for each } j = 1, \ldots, l.$$

Since $K \cong \tau_1(K)$ and $\tau_1(K) \cap U(q_1) = \{1\}$ by Lemma 4.5, the assumption that the statement holds for $q_1 = p_1^{\alpha_1} \cdots p_{r-1}^{\alpha_{r-1}}$ allows us to assert that $\{\zeta_{q_1}^{\tau_1(h)} : h \in K\}$ are linearly independent over $\mathbb{Q}$. So are $\{\zeta_{q_1}^{y\tau_1(h)} : h \in h_j K\} = \{\zeta_{q_1}^{y\tau_1(h_j)\tau_1(h)} : h \in K\}$ by Lemma 4.4. Therefore,

$$\sum_{h\in H} c_h \zeta_n^h = 0 \Rightarrow \sum_{h\in h_j K} c_h \zeta_{q_1}^{y\tau_1(h)} = 0 \text{ for each } j = 1, \ldots, l \Rightarrow c_h = 0 \ \forall h \in H.$$

This completes the proof. □

5. Equivalent conditions for the irreducibility of $J_{n,H}(x)$

In this section, we give the equivalent conditions for $J_{n,H}(x)$ being irreducible over $\mathbb{Q}$.

Lemma 5.1. *For a subgroup H of $\mathbb{Z}_n^*$, let $M = \{m \in \mathbb{Z}_n^* : \sum_{h\in H} \zeta_n^h = \sum_{h\in H} \zeta_n^{mh}\}$. Then M satisfies the following properties.*

(i) *M is a subgroup of $\mathbb{Z}_n^*$ that includes H.*

(ii) $\sum_{m\in M} \zeta_n^m = \frac{|M|}{|H|} \sum_{h\in H} \zeta_n^h$.

Proof. We prove this by associating each $a \in \mathbb{Z}_n^*$ to its corresponding field isomorphism $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ satisfying $\sigma_a(\zeta_n) = \zeta_n^a$. Suppose that $a, b \in M$. Then

$$\sum_{h\in H} \zeta_n^{abh} = \sigma_a\left(\sum_{h\in H} \zeta_n^{bh}\right) = \sigma_a\left(\sum_{h\in H} \zeta_n^h\right) = \sum_{h\in H} \zeta_n^{ah} = \sum_{h\in H} \zeta_n^h;$$

$$\sum_{h\in H} \zeta_n^{\tilde{a}h} = \sigma_{\tilde{a}}\left(\sum_{h\in H} \zeta_n^h\right) = \sigma_{\tilde{a}}\left(\sum_{h\in H} \zeta_n^{ah}\right) = \sum_{h\in H} \zeta_n^h,$$

where $\tilde{a}$ is the multiplicative inverse of a modulo n. This proves that M is a subgroup of $\mathbb{Z}_n^*$. Furthermore, if $h' \in H$, then $h'H = H$ and so $\sum_{h\in H} \zeta_n^h =$

$\sum_{h\in H}\zeta_n^{h'h}$. Hence H is contained in M. We now let $m_1,\dots,m_l$ be distinct representatives of the cosets of H in M. Then $l=\frac{|M|}{|H|}$ and

$$\sum_{m\in M}\zeta_n^m=\sum_{j=1}^{l}\left\{\sum_{h\in H}\zeta_n^{m_jh}\right\}=l\sum_{h\in H}\zeta_n^h.$$

□

Theorem 5.2. *Let H be a proper subgroup of $\mathbb{Z}_n^*$. Then the following conditions are equivalent.*

(i) $\sum_{h\in H}\zeta_n^h\neq 0$.
(ii) $H\cap U(n)=\{1\}$.
(iii) $\{\zeta_n^h : h\in H\}$ *are linearly independent over* $\mathbb{Q}$.
(iv) $\sum_{h\in H}\zeta_n^h\neq\sum_{h\in H}\zeta_n^{kh}$ *whenever* $k\notin H$.
(v) $J_{n,H}(x)$ *is irreducible over* $\mathbb{Q}$.

Proof. We first show that (i), (ii), and (iii) are equivalent.

(i) ⇒ (ii): Contrary to the statement, suppose that $H\cap U(n)\neq\{1\}$. Then, by Theorem 3.2, $\sum_{h\in H}\zeta_n^h=0$, contradicting to (i).

(ii) ⇒ (iii): See Theorem 4.6.

(iii) ⇒ (i): It is obvious by the definition of linear independence.

This completes the proof of (i)⇔(ii)⇔(iii).

(iv) ⇔ (v): See Theorem 2.2.

(v) ⇒ (i): Contrary to the statement, suppose $\sum_{h\in H}\zeta_n^h=0$. Then

$$\sum_{h\in H}\zeta_n^{ah}=\sigma_a\Big(\sum_{h\in H}\zeta_n^h\Big)=0$$

for each $a\in\mathbb{Z}_n^*$ and so $J_{n,H}(x)=x^d$, $d=\frac{|\mathbb{Z}_n^*|}{|H|}>1$, contradicting to (v).

(i) ⇒ (v): Contrary to the statement, suppose that $J_{n,H}(x)$ is not irreducible over $\mathbb{Q}$. By the equivalence (iv) ⇔ (v), there exists $a\in\mathbb{Z}_n^*$, but not in H, such that $\sum_{h\in H}\zeta_n^{ah}=\sum_{h\in H}\zeta_n^h$. Then $\{\zeta_n^k : k\in H\cup aH\}$ are linearly dependent over $\mathbb{Q}$. Let $M=\{m\in\mathbb{Z}_n^* : \sum_{h\in H}\zeta_n^{mh}=\sum_{h\in H}\zeta_n^h\}$. By Lemma 5.1, M is a subgroup of $\mathbb{Z}_n^*$ containing H and aH with $\sum_{m\in M}\zeta_n^m=\frac{|M|}{|H|}\sum_{h\in H}\zeta_n^h$. Since M includes $H\cup aH$, $\{\zeta_n^m : m\in M\}$ are linearly dependent over $\mathbb{Q}$ and thus $\sum_{m\in M}\zeta_n^m=0$ by the equivalence (i)⇔(iii). It contradicts to $\sum_{m\in M}\zeta_n^m=\frac{|M|}{|H|}\sum_{h\in H}\zeta_n^h\neq 0$. □

References

[1] J. R. Bastida, *Field extensions and Galois theory*, Encyclopedia of Mathematics and its Applications, 22, Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1984. https://doi.org/10.1017/CBO9781107340749

[2] H. G. Diamond, F. Gerth, III, and J. D. Vaaler, *Gauss sums and Fourier analysis on multiplicative subgroups of Z_q*, Trans. Amer. Math. Soc. **277** (1983), no. 2, 711–726. https://doi.org/10.2307/1999232

[3] R. J. Evans, *Generalized cyclotomic periods*, Proc. Amer. Math. Soc. **81** (1981), no. 2, 207–212. https://doi.org/10.2307/2044195

[4] J. B. Fraleigh, *A First Course in Abstract Algebra*, Addison-Wesley Publishing Co., Reading, MA, 1967.
[5] H. Hasse, *Number Theory*, Springer-Verlag, Berlin, 1980.
[6] I. M. Isaacs, *Algebra*, Brooks/Cole Publishing Co., Pacific Grove, CA, 1994.
[7] M. Kwon, J.-E. Lee, and K.-S. Lee, *Galois irreducible polynomials*, Commun. Korean Math. Soc. **32** (2017), no. 1, 1–6. https://doi.org/10.4134/CKMS.c160003
[8] T. Nagell, *Introduction to Number Theory*, John Wiley & Sons, Inc., New York, 1951.
[9] G. Shin, J. Y. Bae, and K.-S. Lee, *Irreducibility of Galois polynomials*, Honam Math. J. **40** (2018), no. 2, 281–291.

Ae-Kyoung Cha
Department of Mathematics Education
Korea National University of Education
Chungbuk 28173, Korea
Email address: ccaakk7@naver.com

Miyeon Kwon
Department of Mathematics
University of Wisconsin-Platteville
Wisconsin 53818, USA
Email address: kwonmi@uwplatt.edu

Ki-Suk Lee
Department of Mathematics Education
Korea National University of Education
Chungbuk 28173, Korea
Email address: ksleeknue@gmail.com

Seong-Mo Yang
Department of Mathematics Education
Korea National University of Education
Chungbuk 28173, Korea
Email address: t2tospace@naver.com