Honam Mathematical J. **40** (2018), No. 2, pp. 281–291
https://dx.doi.org/10.5831/HMJ.2018.40.2.281

IRREDUCIBILITY OF GALOIS POLYNOMIALS

Gicheol Shin, Jae Yun Bae, and Ki-Suk Lee*

Abstract. We associate a positive integer n and a subgroup H of the group $(\mathbb{Z}/n\mathbb{Z})^\times$ with a polynomial $J_{n,H}(x)$, which is called the Galois polynomial. It turns out that $J_{n,H}(x)$ is a polynomial with integer coefficients for any n and H. In this paper, we provide an equivalent condition for a subgroup H to provide the Galois polynomial which is irreducible over $\mathbb{Q}$ in the case of $n = p_1^{e_1} \cdots p_r^{e_r}$ (prime decomposition) with all $e_i \geq 2$.

For a positive integer n, we denote the n^{th} primitive root $e^{2\pi i/n}$ of unity by ζ_n, and the (multiplicative) group consisting of all invertible elements in the ring $\mathbb{Z}/n\mathbb{Z}$ by $(\mathbb{Z}/n\mathbb{Z})^\times$ throughout this paper. Also, $\phi(n)$ denotes the Euler's phi function, *i.e.*, $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.

1. Introduction

Let n be a positive integer. It is well known that the n^{th} cyclotomic polynomial

$$\Phi_n(x) = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta_n^i)$$

is a polynomial of degree $\phi(n)$ with integer coefficients, and that it is irreducible over $\mathbb{Q}$, the field of rational numbers.

Let H be a subgroup of the group $(\mathbb{Z}/n\mathbb{Z})^\times$. In paper [1], Kwon, Lee, and the third author first introduced the Galois polynomial $J_{n,H}(x)$ associated with n and H as a generalization of the cyclotomic polynomial $\Phi_n(x)$, and provided several properties of $J_{n,H}(x)$: as the cyclotomic polynomial $\Phi_n(x)$ is, the Galois polynomial $J_{n,H}(x)$ is a polynomial with integer coefficients. In addition, if n is square-free, then $J_{n,H}$ is

Received January 11, 2018. Revised March 3, 2018. Accepted March 14, 2018.
2010 Mathematics Subject Classification. 12D05, 12E05, 12F05, 12F10.
Key words and phrases. n-th cyclotomic polynomial, Galois irreducible polynomial, semi-cyclotomic polynomial
*corresponding author

irreducible over $\mathbb{Q}$ for any subgroup H. We will give a brief review of definition of Galois polynomials and their properties in the next section.

However, if n is divisible by p^2 for some prime number p, some subgroup H fails to produce the Galois polynomial which is irreducible over $\mathbb{Q}$. The question then arises: for such an integer n, what are (sufficient, necessary, or both) conditions for a subgroup H to produce the irreducible Galois polynomial over $\mathbb{Q}$? In the last section, we will provide an answer to this question when n has prime decomposition $n = p_1^{e_1} \cdots p_r^{e_r}$ with $e_i \geq 2$ $(1 \leq i \leq r)$, where $p_1, \cdots, p_r$ are distinct prime numbers. Also, we will briefly discuss some possible directions for future research.

2. A review of Galois Polynomials

In this section, we briefly review Galois polynomials and their basic properties.

2.1. Definition of $J_{n,H}(x)$

Let n be a positive integer. It is well known that the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ of the field extension $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is isomorphic to the group $(\mathbb{Z}/n\mathbb{Z})^\times$ via the isomorphism $\theta\colon (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, $\theta(g) = \theta_g$, which is given by $\theta_g(\zeta_n) = \zeta_n^g$.

Definition 2.1. *Let n be a positive integer, and let H be a subgroup of $G = (\mathbb{Z}/n\mathbb{Z})^\times$. The Galois polynomial $J_{n,H}(x)$ associated with n and H is the polynomial defined as*

$$J_{n,H}(x) = \prod_{K \in G/H} (x - \alpha_K),$$

where $\alpha_K = \sum_{k \in K} \theta_k(\zeta_n) = \sum_{k \in K} \zeta_n^k$. In other words, if $\{g_1, \cdots, g_m\}$ is a system of representatives of cosets of G by H, then

$$J_{n,H}(x) = \left(x - \sum_{h \in H} \zeta_n^{g_1 h}\right) \cdots \left(x - \sum_{h \in H} \zeta_n^{g_m h}\right).$$

Remark 2.2. *From the definition, we can directly see that the Galois polynomial associated with n and the trivial subgroup $\{1\}$ is nothing but the n^{th} cyclotomic polynomial $\Phi_n(x)$. Also, the Galois polynomial associated with the subgroup $\{1, n-1\}$ was studied in* [2].

Example 2.3. *Consider the case of $n = 16$. There are exactly eight subgroups of $(\mathbb{Z}/16\mathbb{Z})^\times$:*

$$\begin{aligned} H_1 &= \{1, 9\}, \\ H_2 &= \{1, 3, 9, 11\}, \\ H_3 &= \{1, 5, 9, 13\}, \\ H_4 &= \{1, 7, 9, 15\}, \\ H_5 &= \{1, 3, 5, 7, 9, 11, 13, 15\}, \\ K_1 &= \{1\}, \\ K_2 &= \{1, 7\}, \\ K_3 &= \{1, 15\}. \end{aligned}$$

For each subgroup, the associated Galois polynomials is given as follows:

$$\begin{aligned} J_{16,H_1}(x) &= x^4, \\ J_{16,H_2}(x) &= x^2, \\ J_{16,H_3}(x) &= x^2, \\ J_{16,H_4}(x) &= x^2, \\ J_{16,H_5}(x) &= x, \\ J_{16,K_1}(x) &= x^8 + 1 = \Phi_{16}(x), \\ J_{16,K_2}(x) &= x^4 + 4x^2 + 2, \\ J_{16,K_3}(x) &= x^4 - 4x^2 + 2. \end{aligned}$$

2.2. An action of G/H on the set $\{\alpha_K \mid K \in G/H\}$

Let n be a positive integer and $G = (\mathbb{Z}/n\mathbb{Z})^\times$. Via the map $\theta\colon G \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, the group G acts on the set $\{\alpha_K \mid K \in G/H\}$ as follows:

$$g \cdot \alpha_K = \theta_g(\alpha_K) = \theta_g\left(\sum_{k \in K} \zeta_n^k\right) = \sum_{k \in K} \zeta_n^{gk} = \alpha_{gK}.$$

Since H is a subgroup of G, and since G is abelian, it can be easily seen that H acts on $\{\alpha_K \mid K \in G/H\}$ trivially, from which it follows that the action of G induces the action of G/H on the set $\{\alpha_K \mid K \in G/H\}$. Moreover, the action of G on $\{\alpha_K \mid K \in G/H\}$ is transitive. In fact, for any $K \in G/H$, if $k \in K$ then we have $k \cdot \alpha_H = \alpha_{kH} = \alpha_K$. Thus, G/H also acts on $\{\alpha_K \mid K \in G/H\}$ transitively; that is, the orbit of α_H under the action of G/H is equal to $\{\alpha_K \mid K \in G/H\}$.

2.3. Basic properties

Notice that the extension $\mathbb{Q}(\zeta_n)$ of $\mathbb{Q}$ is a Galois extension. It follows that the minimal polynomial $\mathrm{irr}(\alpha_H, \mathbb{Q})$ of α_H over $\mathbb{Q}$ is

$$\mathrm{irr}(\alpha_H, \mathbb{Q})(x) = \prod_{\alpha_K \in \mathrm{Orb}_G(\alpha_H)} (x - \alpha_K), \tag{1}$$

where $\mathrm{Orb}_G(\alpha_H)$ is the orbit of α_H, *i.e.*, $\mathrm{Orb}_G(\alpha_H) = \{\alpha_K \mid K \in G/H\}$. Hence, the Galois polynomial $J_{n,H}(x)$ is a power of $\mathrm{irr}(\alpha_H, \mathbb{Q})(x)$; more precisely, we have

$$J_{n,H}(x) = \left(\mathrm{irr}(\alpha_H, \mathbb{Q})(x)\right)^{\ell}, \tag{2}$$

where $\ell = |\mathrm{Stab}_{G/H}(\alpha_H)| = |G/H|/|\mathrm{Orb}_G(\alpha_H)|$.

Hence, we obtain the following lemma:

Lemma 2.4. *Let n be a positive integer, and let H be a subgroup of $G = (\mathbb{Z}/n\mathbb{Z})^{\times}$. Then the following statements are true.*

1. *All coefficients of $J_{n,H}(x)$ are rational, i.e., $J_{n,H}(x) \in \mathbb{Q}[x]$.*
2. $\mathrm{Stab}_{G/H}(\alpha_H) = G/H$ *if and only if $J_{n,H}(x)$ is of the form x^{ℓ}.*
3. $\mathrm{Stab}_{G/H} = \{1\}$ *if and only if $J_{n,H}(x)$ is irreducible over $\mathbb{Q}$.*

Remark 2.5. *In fact, for any n and H, the Galois polynomial $J_{n,H}(x)$ is a monic polynomial with integer coefficients. Moreover, for a proper subgroup H,* $\mathrm{Stab}_{G/H}(\alpha_H) = G/H$ *if and only if $\alpha_H = 0$. See* [1] *for a proof and details. Also, in* [1], *it was proven that if n is square-free, then the Galois polynomial $J_{n,H}(x)$ associated with any subgroup is irreducible over $\mathbb{Q}$.*

3. Galois Polynomials for $n = p_1^{e_1} \cdots p_r^{e_r}$ with $e_i \geq 2$ $(1 \leq i \leq r)$

Throughout this section, we assume that n is a fixed positive integer with prime decomposition $n = p_1^{e_1} \cdots p_r^{e_r}$, where $p_1, \cdots, p_r$ are distinct prime numbers and each e_i $(1 \leq i \leq r)$ is greater than 1. Under this assumption, we will characterize subgroups H for which $J_{n,H}$ is irreducible over $\mathbb{Q}$.

Let $\overline{n} = p_1 \cdots p_r$ denote the radical of n and $d = n/\overline{n}$.

3.1. The subgroup C of $(\mathbb{Z}/n\mathbb{Z})^{\times}$

Since $\gcd(1 + \ell d, n) = 1$ for any $\ell \in \mathbb{Z}$, we may regard $1 + \ell d$ as an element of the group $(\mathbb{Z}/n\mathbb{Z})^{\times}$. Consider the subset $C = \{1 + \ell d \mid \ell \in \mathbb{Z}\}$

of $(\mathbb{Z}/n\mathbb{Z})^\times$. Observe that $e_i \geq 2$ $(1 \leq i \leq r)$ implies

$$d^2 \equiv p_1^{2(e_1-1)} \cdots p_r^{2(e_r-1)} \equiv np_1^{e_1-2} \cdots p_r^{e_r-2} \equiv 0 \ (mod\ n), \tag{3}$$

hence, $d^k \equiv 0 \mod n$ for all $k \geq 2$. Thus, we obtain

$$(1+d)^\ell \equiv 1 + \ell d \ (mod\ n) \qquad (\ell \in \mathbb{Z}), \tag{4}$$

from which it follows that the subset C is the cyclic subgroup of H generated by the element $1+d$.

3.2. The sum $\alpha_H = \sum_{h\in H} \zeta_n^h$

We first provide a criterion for a subset H of $(\mathbb{Z}/n\mathbb{Z})^\times$ to satisfy $\sum_{h\in H} \zeta_n^h = 0$, which plays an important role in proving our main theorem (Theorem 3.7).

Lemma 3.1. *Let H be a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ with $H \cap C \neq \{1\}$. Then we have $\sum_{h\in H} \zeta_n^h = 0$.*

Proof. Since C is a cyclic group, $K = H \cap C$ is also cyclic. Let $1 + \ell d$ be a generator of K. Then by assumption, we have $1 + \ell d \not\equiv 1 \ (mod\ n)$.

Thus if m is the order of the element $1 + \ell d$, then

$$\begin{aligned}\sum_{k\in K} \zeta_n^k &= \sum_{i=0}^{m-1} \zeta_n^{1+i\ell d} = \zeta_n \sum_{i=0}^{m-1} \zeta_n^{i\ell d} \\ &= \zeta_n \frac{1-\zeta_n^{m\ell d}}{1-\zeta_n^{\ell d}} = 0.\end{aligned}$$

Now pick a system $\{h_1, \cdots, h_s\}$ of representatives of cosets of H by K. Then we have

$$\sum_{h\in H} \zeta_n^h = \sum_{j=1}^{s} \theta_{h_j} \left(\sum_{k\in K} \zeta_n^k \right) = \sum_{j=1}^{s} \theta_{h_j}(0) = 0,$$

as desired. □

Example 3.2. *Consider the case of $n = 16 = 2^4$, $\overline{n} = 2$, and $d = 8$. In this case, we have $C = \{1, 9\}$. Only subgroups containing 9 of $(\mathbb{Z}/16\mathbb{Z})^\times$ are*

$$\begin{aligned}&H_1 = \{1, 9\} = C,\\ &H_2 = \{1, 3, 9, 11\},\\ &H_3 = \{1, 5, 9, 13\},\\ &H_4 = \{1, 7, 9, 15\}, \text{ and}\\ &H_5 = \{1, 3, 5, 7, 9, 11, 13, 15\} = (\mathbb{Z}/16\mathbb{Z})^\times.\end{aligned}$$

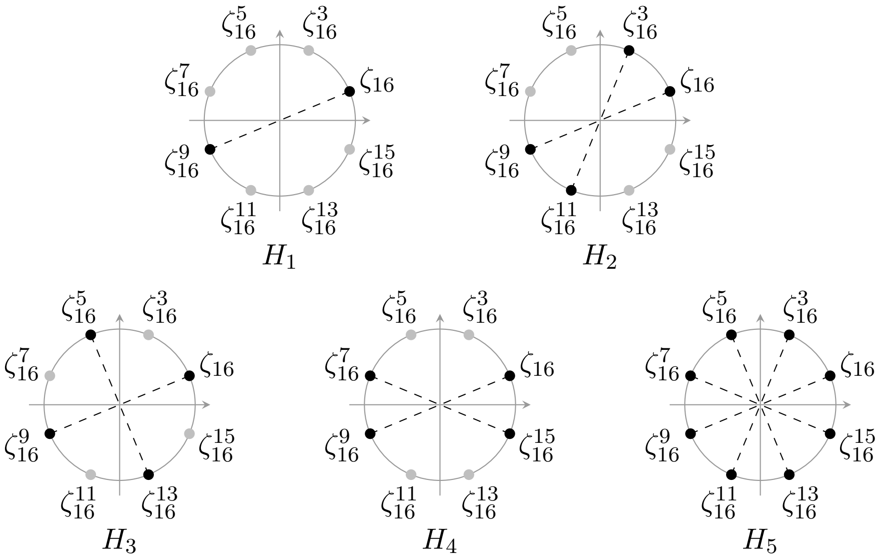

FIGURE 1. the sum $\alpha_{H_i} = \sum_{h\in H_i} \zeta_{16}^h$ for each $i = 1, 2, 3, 4, 5$

For this small example, figure 1 shows that for each subgroup $H_i (1 \leq i \leq 5)$, the sum $\sum_{h\in H_i} \zeta_{16}^h$ equals zero by symmetry.

On the other hand, $(\mathbb{Z}/16\mathbb{Z})^\times$ has exactly three subgroups not containing 9:

$$K_1 = \{1\},\ K_2 = \{1, 7\},\ \text{and } K_3 = \{1, 15\},$$

and obviously, we have

$$\zeta_{16} \neq 0,\ \zeta_{16} + \zeta_{16}^7 \neq 0,\ \text{and } \zeta_{16} + \zeta_{16}^{15} \neq 0 \text{ (See figure 2).}$$

Example 3.3. *Let $n = 9 = 3^2$, $\overline{n} = 3$, and $d = 3$. In this case, we have $C = \{1, 4, 7\}$. Notice that C is a cyclic group of order 3, from which it follows that if $H \cap C \neq \{1\}$, then $H \cap C = C$; in other words, if H contains either 4 or 7, then H contains both 4 and 7. There are exactly two subgroups containing 4 and 7:*

$$H_1 = \{1, 4, 7\}, \qquad H_2 = \{1, 2, 4, 5, 7, 8\} = (\mathbb{Z}/9\mathbb{Z})^\times.$$

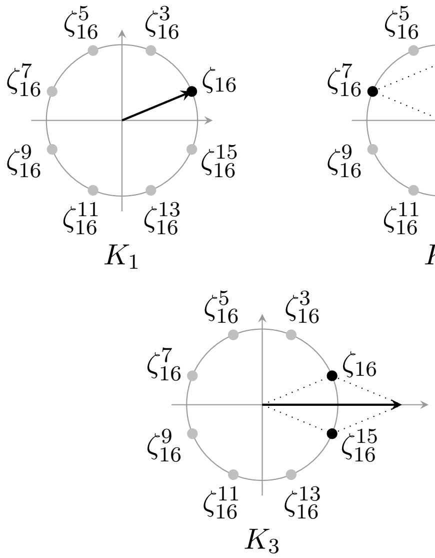

FIGURE 2. the sum $\alpha_{K_i} = \sum_{h \in K_i} \zeta_{16}^h$ for each $i = 1, 2, 3$

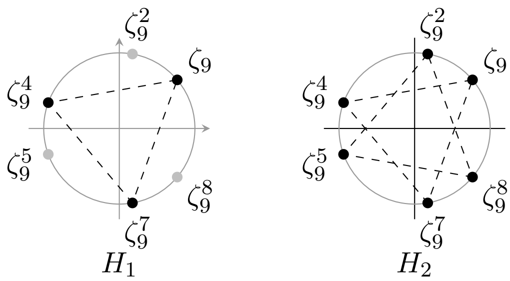

FIGURE 3. The sum $\alpha_{H_i} = \sum_{h \in H_i} \zeta_9^h$ for each $i = 1, 2, 3, 4, 5$

Figure 3 shows

$$\sum_{h \in H_1} \zeta_9^h = \zeta_9 + \zeta_9^4 + \zeta_9^7 = 0, \text{ and}$$
$$\sum_{h \in H_2} \zeta_9^h = \zeta_9 + \zeta_9^2 + \zeta_9^4 + \zeta_9^5 + \zeta_9^7 + \zeta_9^8 = 0$$

by symmetry.

h	ζ_{16}^h				h	ζ_{16}^h			
1	ζ_{16}				9	$-\zeta_{16}$			
3		ζ_{16}^3			11		$-\zeta_{16}^3$		
5			ζ_{16}^5		13			$-\zeta_{16}^5$	
7				ζ_{16}^7	15				$-\zeta_{16}^7$

TABLE 1. expressions of ζ_{16}^h for $h \in (\mathbb{Z}/16\mathbb{Z})^\times$

3.3. An expression of $\zeta_n^h \in \mathbb{Q}(\zeta_n)$ $(h \in (\mathbb{Z}/n\mathbb{Z})^\times)$

In fact, the converse of the Lemma 3.1 is true. Before proving this, it is worthwhile to express ζ_n^h for $h \in G = (\mathbb{Z}/n\mathbb{Z})^\times$ as a $\mathbb{Q}$-linear combination of $1, \zeta_n, \cdots, \zeta_n^{\phi(n)-1}$. First notice that every $h \in G = (\mathbb{Z}/n\mathbb{Z})^\times$ can be uniquely expressed as $h = m + \ell d$, where $m \in \{0, 1, \cdots, d-1\}$ and $\ell \in \{0, 1, \cdots, \overline{n}-1\}$. Thus, we obtain $\zeta_n^h = \zeta_n^{m+\ell d} = \zeta_n^m \zeta_n^{\ell d} = \zeta_n^m \zeta_{\overline{n}}^{\ell}$. On the other hand, since $\zeta_{\overline{n}}^{\ell} \in \mathbb{Q}(\zeta_{\overline{n}})$, we can rewrite $\zeta_{\overline{n}}^{\ell}$ as

$$\zeta_{\overline{n}}^{\ell} = a_0 + a_1\zeta_{\overline{n}} + \cdots + a_{\phi(\overline{n})-1}\zeta_{\overline{n}}^{\phi(\overline{n})-1} \qquad (a_0, a_1, \cdots, a_{\phi(\overline{n})-1} \in \mathbb{Q}).$$

Hence, we can express ζ_n^h as follows:

$$\begin{aligned}\zeta_n^h &= \zeta_n^m \left(a_0 + a_1\zeta_{\overline{n}} + \cdots + a_{\phi(\overline{n})-1}\zeta_{\overline{n}}^{\phi(\overline{n})-1}\right) \\ &= \zeta_n^m \left(a_0 + a_1\zeta_n^d + \cdots + a_{\phi(\overline{n})-1}\zeta_n^{(\phi(\overline{n})-1)d}\right) \\ &= a_0\zeta_n^m + a_1\zeta_n^{m+d} + \cdots + a_{\phi(\overline{n})-1}\zeta_n^{m+(\phi(\overline{n})-1)d}.\end{aligned}$$

Since

$$\begin{aligned}m + (\phi(\overline{n}) - 1)d &< d + (\phi(\overline{n}) - 1)d \\ &= \phi(\overline{n})d = (p_1 - 1)p_1^{e_1-1} \cdots (p_r - 1)p_r^{e_r-1} = \phi(n),\end{aligned}$$

only ζ_n^{m+id} terms $(i = 0, 1, \cdots, \phi(\overline{n}) - 1)$ possibly appear in the expression of ζ_n^h as a linear combination of $1, \zeta_n, \cdots, \zeta_n^{\phi(n)-1}$.

Example 3.4. *Let $n = 16 = 2^4$, $\overline{n} = 2$, and $d = 8$. Using the fact $\Phi_{16}(x) = x^8 + 1$ (hence, $\zeta_{16}^8 = -1$), we can easily verify Table 1, which shows an expression of each primitive root ζ_{16}^h of unity as a linear combination.*

Example 3.5. *Let $n = 9 = 3^2$, $\overline{n} = 3$, and $d = 3$. In this case, we have $\Phi_9(x) = x^6 + x^3 + 1$. Table 2 shows an expression of each primitive root ζ_9^h of unity as a linear combination.*

h	ζ_9^h	h	ζ_9^h	h	ζ_9^h
1	ζ_9	4	ζ_9^4	7	$-\zeta_9 \quad - \zeta_9^4$
2	ζ_9^2	5	ζ_9^5	8	$- \zeta_9^2 \quad - \zeta_9^5$

TABLE 2. expressions of ζ_9^h for $h \in (\mathbb{Z}/9\mathbb{Z})^\times$

Theorem 3.6. *Let H be a subgroup of $G = (\mathbb{Z}/n\mathbb{Z})^\times$. Then $\sum_{h\in H} \zeta_n^h = 0$ if and only if H contains an element $\neq 1$ of the form $1 + \ell d$.*

Proof. In lemma 3.1, we showed "if" direction, so we prove "only if" direction here. Suppose that H has no element of the form $1 + \ell d$ except for the identity 1. As we have seen, for any $h \in H \setminus \{1\}$, ζ_n term never appear in the expression of ζ_n^h as a linear combination of $1, \zeta_n, \cdots, \zeta_n^{\phi(n)-1}$. Since $1 \in H$, apparently, ζ_n appears in the sum $\sum_{h\in H} \zeta_n^h$, *i.e.*,

$$\sum_{h\in H} \zeta_n^h = \zeta_n + (\text{a linear combination of the others } 1, \zeta_n^2, \cdots, \zeta_n^{\phi(n)-1}),$$

from which it follows that the sum $\sum_{h\in H} \zeta_n^h$ never equals zero. □

3.4. Main result

Now we are ready to prove our main result on irreducibility of Galois polynomials.

Theorem 3.7. *Let H be a subgroup of $G = (\mathbb{Z}/n\mathbb{Z})^\times$ which has no element of the form $1 + \ell d$ except for the identity 1, i.e., $H \cap C = \{1\}$. Then the Galois polynomial $J_{n,H}(x)$ associated with n and H is irreducible over $\mathbb{Q}$.*

Proof. Thanks to lemma 2.4, it suffices to show that for any $k \in G\backslash H$, two sums $\sum_{h\in H} \zeta_n^h$ and $\sum_{h\in H} \zeta_n^{kh}$ are different. Assume to the contrary that for some $k \in G \setminus H$, we have $\sum_{h\in H} \zeta_n^h = \sum_{h\in H} \zeta_n^{kh}$. In the proof of theorem 3.6, we have seen

$$\left(\sum_{h\in H} \zeta_n^h\right) - \zeta_n = (\text{a linear combination of } 1, \zeta_n^2, \cdots, \zeta_n^{\phi(n)-1}), \tag{5}$$

which implies that the coset kH should contain at least one element of the form $1 + \ell d$. Let $x = 1 + \ell d$ denote such an element of kH. On the other hand, since H and kH are disjoint and $1 \in H$, we have $x \neq 1$, which implies $\zeta_n^x \neq \zeta_n$. Thus, ζ_n^x should be either a scalar multiple of ζ_n which is not equal to ζ_n or of the form

$$\zeta_n + \left(\text{nonzero linear combination of } \zeta_n^{1+d}, \cdots, \zeta_n^{1+(\phi(\overline{n})-1)d}\right).$$

Since the terms ζ_n^{1+id} $(i = 1, \cdots, \phi(\overline{n})-1)$ never appear in the expression 5, we can conclude that kH also contain another element $y = 1 + \ell' d$ with $x \neq y$ in both case. It follows that the element $1 + (\ell - \ell')d = (1 + \ell d)(1 - \ell' d) = xy^{-1}(\neq 1)$ belongs to H, which is absurd. $\square$

From lemma 2.4 and the theorem above, we directly see:

Corollary 3.8. *For any subgroup H of $G = (\mathbb{Z}/n\mathbb{Z})^\times$, the stabilizer*

$$\mathrm{Stab}_{G/H}(a_H) = \mathrm{Stab}_{G/H}\left(\sum_{h\in H} \zeta_n^h\right)$$

is either $\{1\}$ or G/H. Hence, the Galois polynomial is either irreducible over $\mathbb{Q}$ or equal to $x^{|G/H|}$.

3.5. Future research

First of all, we are still interested in characterizing subgroups which produce irreducible Galois polynomials for general n to find a complete answer to the question which was mentioned in the introduction.

Second, since all coefficients of Galois polynomials are integers, we would like to study those mysterious coefficients in a combinatorial way. For example, motivated by the fact

$$\Phi_n(1) = \begin{cases} p & \text{if } n = p^k, \\ 1 & \text{if } n \text{ is divisible by two or more distinct prime numbers,} \end{cases}$$

possible questions are what the integer $J_{n,H}(1)$ is and how it can be related with n and H.

References

[1] M. Y. Kwon, J. E. Lee and K. S. Lee, *Galois Irreducible Polynomials*, Commun. Korean Math. Soc. 32(2017), No. 1, 1-6.

[2] K. S. Lee, J. E. Lee and J. H. Kim, *Semi-cyclotomic polynomials*, Honam Mathematical J. 37(2015), No. 4, 469-472.

[3] K. S. Lee and J. E. Lee, *Classification of Galois Polynomials*, Honam Mathematical J. 39(2017), No. 2, 259-265.

Gicheol Shin
Department of Mathematics, University of California Davis,
One Shields Ave, Davis, CA 95616-8633, U.S.A.
E-mail: gshin@math.ucdavis.edu

Jae Yun Bae
Department of Mathematics Education, Korea National University of Education,
Cheongjusi, Chungbuk 28173, Republic of Korea.
E-mail: baejaeyun@hanmail.net

Ki-Suk Lee
Department of Mathematics Education, Korea National University of Education,
Cheongjusi, Chungbuk 28173, Republic of Korea.
E-mail: ksleeknue@gmail.com