

## GALOIS POLYNOMIALS

JI-EUN LEE\* AND KI-SUK LEE\*\*

ABSTRACT. We associate a positive integer  $n$  and a subgroup  $H$  of the group  $G(n)$  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  $\mathbb{Q}$ .

### 1. Introduction

Let  $n$  be a positive integer and  $\zeta_n$  be the  $n$ -th primitive root of unity, that is  $\zeta_n = e^{\frac{2\pi i}{n}}$ . It is well known that the  $n$ -th Cyclotomic polynomial  $\Phi_n(x)$  is equal to

$$\Phi_n(x) = \prod_{k \in G(n)} (x - \zeta_n^k),$$

where  $G(n)$  is the multiplicative group of invertible integers modulo  $n$ .

Suppose  $H$  be a subgroup of  $G = G(n)$  and  $G/H = \{h_1H, h_2H, \dots, h_lH\}$  be its corresponding quotient group. For each  $k = 1, \dots, l$ , define  $a_k = \sum_{h \in H} \zeta_n^{h_k h}$ . We now consider the monic polynomial having  $a_1, \dots, a_l$  as its roots, denoted by  $J_{n,H}(x)$ . Then the polynomial

$$J_{n,H}(x) = (x - a_1)(x - a_2) \cdots (x - a_l)$$

is called Galois polynomial.

In this paper, the irreducibility of Galois polynomials is studied. If  $n$  is square-free,  $J_{n,H}(x)$  is irreducible over  $\mathbb{Q}$  for any subgroup  $H$  ([1], Theorem 3.6). However, it is not always true if  $n$  has a squared factor.

---

Received February 14, 2019; Accepted March 15, 2019.

2010 Mathematics Subject Classification: Primary 12D05, 12E05, 12F05, 12F10.

Key words and phrases:  $n$ -th cyclotomic polynomial, Galois irreducible polynomial, semi-cyclotomic polynomial.

\*\*The corresponding author, Ki-Suk Lee.

Here, we modify Evans' criterion([5]) and prove the condition of  $H$  to get an irreducible Galois polynomial when  $n$  is general.

## 2. Irreducibility of Galois polynomials

Throughout the paper,  $r$  is the product of the distinct prime factors of  $n$ , or twice that, according as  $8 \nmid n$  or  $8 \mid n$ . Let  $H$  be a subgroup of  $G(n)$  and define  $\eta = \sum_{h \in H} \sigma_h(\zeta)$ . Write  $n = p^\alpha \cdot m$  where  $p$  is the largest prime factor of  $n > 1$  with  $p \nmid m$ ,  $\alpha \geq 1$ .

In this section, we study the irreducibility of  $J_{n,H}(x)$  when  $n$  is general. If  $n$  is not square-free, the condition of  $H$  to get an irreducible Galois polynomial is not simple. We will show that if no nontrivial element of  $H \equiv 1 \pmod{r}$ , the Galois polynomial  $J_{n,H}(x)$  is irreducible. First, we prove the following Lemma which will be used proving main Theorem.

**LEMMA 2.1.** *Suppose that  $k \in Z$  with  $p \nmid k$  and that  $p^B \parallel (x-1)$  where  $B \geq 1$ , but  $B > 1$  when  $p = 2$ . Then  $p^{A+B} \parallel (x^{kp^A} - 1)$  for each integer  $A \geq 0$ .*

*Proof.* We can write  $x = mp^B + 1$  with  $p \nmid m$  and prove the Lemma by induction on  $A$ .

When  $A = 0$ ,

$$\begin{aligned} x^k - 1 &= (mp^B + 1)^k - 1 \\ &= (mp^B)^k + {}_k C_1 (mp^B)^{k-1} + \cdots + {}_k C_{k-1} (mp^B) + 1 - 1 \\ &= mp^B \{ (mp^B)^{k-1} + \cdots + {}_k C_{k-2} (mp^B) + {}_k C_{k-1} \} \\ &= mp^B \{ (mp^B)^{k-1} + \cdots + {}_k C_{k-2} (mp^B) + k \}. \end{aligned}$$

Since  $p \nmid k$ ,  $p^B \mid (x^k - 1)$  and  $p^{B+1} \nmid (x^k - 1)$ , that is  $p^B \parallel (x^k - 1)$ .  
When  $A = 1$ ,

$$\begin{aligned} x^{kp} - 1 &= (mp^B + 1)^{kp} - 1 \\ &= (mp^B)^{kp} + kp(mp^B)^{kp-1} + \cdots + kp(mp^B) + 1 - 1 \\ &= \{ (mp^B)^{kp} + kp(mp^B)^{kp-1} \cdots + {}_{kp} C_2 (mp^B)^2 + kmp^{B+1} \}. \end{aligned}$$

Since  $p \nmid km$ ,  $p^{B+1} \parallel kmp^{B+1}$ . Therefore  $p^{B+1} \parallel (x^{kp} - 1)$ .

Now, assume that Lemma is true for  $A$ , we will show that it is true for  $A + 1$ .

$$x^{kp^{A+1}} - 1 = (x^{kp^A} - 1)(x^{kp^A(p-1)} + x^{kp^A(p-2)} + \dots + x^{kp^A} + 1)$$

As we assumed,  $p^{A+B} \parallel (x^{kp^A} - 1)$ , we will check if  $p \parallel (x^{kp^A(p-1)} + x^{kp^A(p-2)} + \dots + x^{kp^A} + 1)$ .

$$x^{kp^A(p-1)} = (1 + mp^B)^{kp^A(p-1)} = \dots + kp^A(p-1)mp^B + 1,$$

$$x^{kp^A(p-2)} = (1 + mp^B)^{kp^A(p-2)} = \dots + kp^A(p-2)mp^B + 1,$$

⋮

$$x^{kp^A} = (1 + mp^B)^{kp^A} = \dots + kp^A mp^B + 1.$$

Therefore,

$$\begin{aligned} x^{kp^A(p-1)} + x^{kp^A(p-2)} + \dots + x^{kp^A} + 1 &= \dots + k\left(\frac{(p-1)p}{2}\right)mp^{A+B} + p \\ &= p(\dots + k\left(\frac{(p-1)p}{2}\right)mp^{A+B-1} + 1). \end{aligned}$$

So we get  $p^{A+B+1} \parallel (x^{kp^{A+1}} - 1)$ .

□

**LEMMA 2.2.** *Let  $x \in Z$ ,  $x \equiv 1 \pmod{r}$  and  $x \not\equiv 1 \pmod{n}$ . Then for some  $d > 0$  and some prime  $t$  such that  $t^2 \mid n$ ,  $x^d \equiv 1 \pmod{\frac{n}{t}}$  and  $x^d \not\equiv 1 \pmod{n}$ .*

*Proof.* We proceed by induction on the number of distinct prime factors of  $n$ . Since  $t^2 \mid n$  is a condition, we may assume  $n = p^\alpha$ ,  $\alpha \geq 2$  for the first step of induction. Then  $x = p^{\alpha-1} + 1$  and  $d = 1$  will work. Now, we assume that  $n = p^\alpha \cdot m$  with  $(p, m) = 1$  and consider two cases; when  $p^\alpha \mid (x - 1)$  and  $p^\alpha \nmid (x - 1)$ .

Case 1:  $p^\alpha \mid (x - 1)$

Since  $x \equiv 1 \pmod{r_0}$  and  $x \not\equiv 1 \pmod{m}$ , the induction hypothesis yields some  $d > 0$  and some prime  $t$  such that  $t^2 \mid m$ ,  $x^d \equiv 1 \pmod{m/t}$ , and  $x^d \not\equiv 1 \pmod{m}$ . Thus  $x^d \equiv 1 \pmod{\frac{n}{t}}$  and  $x^d \not\equiv 1 \pmod{n}$ .

Case 2:  $p^\alpha \nmid (x - 1)$

Since  $x \equiv 1 \pmod{r}$ , we have  $p^B \parallel (x - 1)$ . where  $\alpha > B \geq 1$  and  $B > 1$  when  $p = 2$ . Since  $p$  is the largest prime factor of  $n$ ,  $p \nmid \phi(m)$ . Define  $d = \phi(m)p^A$ , where  $A = \alpha - B - 1$ . Note that  $A \geq 0$ . By Lemma 2.1,  $p^{\alpha-1} \parallel (x^d - 1)$ . Also  $x^d \equiv 1 \pmod{m}$  since

$\phi(m)|d$ . Therefore  $x^d \equiv 1 \pmod{\frac{n}{t}}$  and  $x^d \not\equiv 1 \pmod{n}$  holds with  $t = p$ . Finally note that  $p^2|n$  since  $\alpha > B \geq 1$ .

□

LEMMA 2.3. *If no nontrivial element of  $H$  is  $\equiv 1 \pmod{r}$  and  $H = G(n)$ , then  $\eta = \pm 1$ .*

*Proof.* If no nontrivial element of  $H$  is  $\equiv 1 \pmod{r}$  and  $H = G(n)$ ,  $n$  is square free. The Ramanujan's sum  $\sum_{x \in G} \zeta_n^x$  equals  $\mu(n)$ , where  $\mu$  is the Möbius function. Since  $n$  is square free,  $\mu(n) = \pm 1$ , so  $\eta = \pm 1$ . □

THEOREM 2.4. *Suppose that no nontrivial element of  $H$  is  $\equiv 1 \pmod{r}$ . Then  $\eta \neq \sigma_c(\eta)$  for all  $c \in G - H$ .*

*Proof.* We proceed by induction on the number of distinct prime factors of  $n$ . For the first step, let  $p$  be any prime number. If  $n = p$ , we get  $\eta \neq \sigma_c(\eta)$  since Galois polynomial  $J_{n,H}(x)$  is always irreducible since all roots of  $J_{n,H}(x)$  are distinct ([1], Theorem2.5). If  $n = p^k$ , with  $k \geq 2$ , we get  $\eta \neq \sigma_c(\eta)$  ([4], Theorem3.7).

Now, we consider when  $n$  has more than one prime factor. We may write  $n = p^\alpha \cdot m$ , where  $(p, m) = 1$ . Let the subgroup  $I \subset H$  defined by

$$I = \{x \in H : x \equiv 1 \pmod{p^\alpha}\}.$$

Reduction  $(\text{mod } m)$  maps  $I$  isomorphically onto a subgroup  $J \subset G_m$ . Write

$$H = \bigcup_{i=1}^k x_i I,$$

a disjoint union of cosets with  $x_1 = 1$ . Then

$$R := \sigma_{m+p^\alpha}(\eta) = \sum_{h \in H} \zeta_m^h \zeta_{p^\alpha}^h = \sum_{i=1}^k \sigma_{x_i} \{ \zeta_{p^\alpha} \sum_{x \in I} \sigma_x(\zeta_m) \} = \sum_{i=1}^k \sigma_{x_i} (\delta \zeta_{p^\alpha}),$$

where  $\eta = \sum_{h \in H} \sigma_h(\zeta_n)$  and  $\delta = \sum_{x \in I} \sigma_x(\zeta_m)$ .

Since  $\delta = \sum_{x \in I} \sigma_x(\zeta_m) = \sum_{x \in J} \sigma_x(\zeta_m)$ , and  $m$  has one less distinct prime factors than  $n$ , by induction hypothesis,  $\tau_w(\delta) \neq \delta$  for all  $w \in G_m - J$ .

For  $1 \leq i \leq k$ , write

$$x_i = ps_i + r_i, \quad cx_i = ps'_i + r'_i \quad (0 < r_i, r'_i < p).$$

We proceed to show that

$$r_1, \dots, r_k \text{ are distinct and } r'_1, \dots, r'_k \text{ are distinct.}$$

If  $x_i \equiv x_j \pmod{p}$  with  $i \neq j$ , then  $x := x_i x_j^{-1} \equiv 1 \pmod{p}$ . Since the cosets are different,  $x \not\equiv 1 \pmod{p^\alpha}$ . Thus

$$p^B \parallel (x - 1) \text{ with } 1 \leq B < \alpha.$$

By Lemma 2.1,

$$x^{p^{\alpha-B}} \equiv 1 \pmod{p^\alpha}.$$

Since  $x^{\varphi(r)} \equiv 1 \pmod{r}$  and  $x^{\varphi(r)} \in H$ ,  $x^{\varphi(r)} \equiv 1 \pmod{n}$ . Therefore  $x^{\varphi(r)} \equiv 1 \pmod{p^\alpha}$ . Since the exponents  $p^{\alpha-B}$  and  $\varphi(r)$  are relatively prime,  $x \equiv 1 \pmod{p^\alpha}$ . This is a contradiction. So, similarly we can prove that  $r'_1, \dots, r'_k$  are different. If  $cx_i \equiv cx_j \pmod{p}$ , then  $x_i \equiv x_j \pmod{p}$ .

We will prove that  $\eta \neq \sigma_c(\eta)$  if  $c \in G - H$ . Suppose that  $\eta = \sigma_c(\eta)$ . We want to show that  $c \in H$ . If  $\eta = \sigma_c(\eta)$ , then  $R$  is  $\sigma_c(R)$ .

$$\begin{aligned} \sum_{i=1}^k \sigma_{x_i}(\delta) \zeta_{p^\alpha}^{x_i} &= R = \sigma_c(R) = \sum_{i=1}^k \sigma_{cx_i}(\delta) \zeta_{p^\alpha}^{cx_i}. \\ \sum_{i=1}^k (\zeta_{p^\alpha}^{ps_i} \sigma_{x_i}(\delta)) \zeta_{p^\alpha}^{r_i} &= \sum_{i=1}^k (\zeta_{p^\alpha}^{ps'_i} \sigma_{cx_i}(\delta)) \zeta_{p^\alpha}^{r'_i}. \end{aligned}$$

Since  $\zeta_{p^\alpha}, \zeta_{p^\alpha}^2, \dots, \zeta_{p^\alpha}^{p-1}$  comprise a part of a basis for  $\mathbb{Q}(\zeta_n)$  over  $\mathbb{Q}(\zeta_n^p)$ ,  $r'_i = r_1 = 1$  for some  $i$ , and

$$\zeta_{p^\alpha}^{ps_1} \sigma_{x_1}(\delta) = \zeta_{p^\alpha}^{ps'_i} \sigma_{cx_i}(\delta).$$

Note that  $x_1 = 1, r_1 = 1$ , and  $s_1 = 0$ . Then we get  $\delta = \zeta_{p^\alpha}^{d-1} \sigma_d(\delta)$ , where

$$d := cx_i = ps'_i + 1.$$

So,  $\sigma_d(\delta) = \zeta_{p^\alpha}^{1-d} \delta$ .

Assume for the purpose of contradiction that  $d \not\equiv 1 \pmod{p^\alpha}$ . Then  $p^B \parallel (1 - d)$  for some  $B$  with  $1 \leq B < \alpha$ , and  $B > 1$  when  $p = 2$ . Define

$$d_A = d^{\varphi(m)p^A}, \text{ where } A = \alpha - B - 1.$$

By Lemma 2.1,

$$(2.1) \quad p^{\alpha-1} \parallel (d_A - 1).$$

Since  $d^{\varphi(m)} \equiv 1 \pmod{m}$ ,  $m$  divides  $d_A - 1$ . Consequently  $mp^{\alpha-1} \parallel (d_A - 1)$ . Applying  $\sigma_d$  successively to  $\sigma_d(\delta) = \zeta_{p^\alpha}^{1-d} \delta$ , we get  $\sigma_{d^A}(\delta) = \delta \zeta_{p^\alpha}^{1-d^A}$ .

Therefore,  $\delta \equiv \delta \zeta_{p^\alpha}^{1-d^A}$ , and  $\delta(1 - \zeta_{p^\alpha}^{1-d^A}) = 0$ . This implies that  $1 - d^A \equiv 0 \pmod{p^\alpha}$ , which contradicts to (2.1). So we have that  $d \equiv 1 \pmod{p^\alpha}$ .

Reduction (mod  $m$ ) maps  $d$  to an element  $y \in G_m$ . Since  $y \equiv d \pmod{m}$  and  $\delta \in \mathbb{Q}(\zeta_m)$ , we get

$$\tau_y(\delta) = \sigma_d(\delta).$$

Also,  $d \equiv 1 \pmod{p^\alpha}$  implies that  $\sigma_d(\delta) = \zeta_{p^\alpha}^{1-d}\delta$  is equal to  $\delta$ . Therefore  $\tau_y\delta = \delta$  and  $m$  has one less prime factors than  $n$ , we get by induction assumption,  $y \in J$ . Since  $I$  and  $J$  are isomorphic, there exists  $h \in I$  such that  $h \equiv y \pmod{m}$ . This implies that  $d \equiv h \pmod{m}$ . Also have  $h \equiv 1 \pmod{p^\alpha}$  because  $h \in I$ . Since  $d \equiv h \equiv 1 \pmod{p^\alpha}$  and  $d \equiv h \pmod{m}$ , we get  $d \equiv h \pmod{n}$ . Therefore  $d = h$  in  $G_n$  and  $d$  is in  $H$ , since  $h$  is in  $I$ . Finally we get  $c \in H$ , because  $d = cx_i$  and  $x_i \in H$ .  $\square$

**THEOREM 2.5.** *No nontrivial element of  $H$  is  $\equiv 1 \pmod{r}$  if and only if  $\eta \neq 0$ .*

*Proof.*

$\implies$  If  $G = H$ , then  $\eta \neq 0$  by Lemma2.3. If  $G \neq H$ , then  $\eta \neq 0$  by Theorem2.4.

$\impliedby$  If there exists a nontrivial element of  $H$  which is  $\equiv 1 \pmod{r}$ , then by Lemma2.2, there exist integers  $d, t$  with  $t$  prime such that  $t^2 \mid n$ ,  $x^d \equiv 1 \pmod{\frac{n}{t}}$  and  $x^d \not\equiv 1 \pmod{n}$ . Define  $K = \{h \in H \mid h \equiv 1 \pmod{\frac{n}{t}}\}$ . And express  $\eta$  by using the cosets of  $K$  in  $H$ . Then we can show that  $\eta = 0$ .  $\square$

**THEOREM 2.6.** *If  $\eta \neq 0$ , then  $\eta$  has degree  $e = |G \setminus H|$  over  $\mathbb{Q}$ .*

*Proof.* Suppose that  $\eta \neq 0$ . By Theorem2.5, no nontrivial elements of  $H$  is  $\equiv 1 \pmod{r}$ . Then by Theorem2.4,  $\eta \neq \sigma_c(\eta)$  for  $c \in H$ . Thus  $\eta$  is fixed by exactly  $|H|$  automorphisms  $\sigma_c$  in  $Gal(\mathbb{Q}(\zeta))$  so  $\eta$  has degree  $e$  over  $\mathbb{Q}$ .  $\square$

Note: This means that Galois polynomial is irreducible if and only if  $\eta \neq 0$ , or equivalently if and only if no nontrivial element of  $H$  is  $\equiv 1 \pmod{r}$ .

### References

[1] M. Kwon, J. E. Lee, and K. S. Lee , *Galois irreducible polynomials*, Communications of the Korean Mathematics Society, **32** (2017), no. 1, 1-6.  
 [2] K. S. Lee, J. E. Lee and J. H. Kim , *Semi-cyclotomic polynomials*, Honam Mathematical Journal, **37** (2015), no. 4, 469-472.

- [3] K. S. Lee and J. E. Lee, *Classification of Galois Polynomials*, Honam Mathematical Journal, **39** (2017), no. 2, 259-265.
- [4] G. C. Shin, J. Y. Bae, and K. S. Lee, *Irreducibility of Galois Polynomials*, Honam Mathematical Journal, **40** (2018), no. 2, 281-291.
- [5] Ronald J. Evnas, *Period polynomials for generalized cyclotomic periods*, Manuscripta math. **40** (1982), 217-243.
- [6] J. R. Bastida and R. Lyndon, *Field Extensions and Galois Theory*, Encyclopedia of Mathematics and Its Application, Addison-Wesley Publishing Company, 1984.
- [7] T. W. Hungerford, *Abstract Algebra An Introduction*, Brooks/Cole, Cengage Learning, 2014.
- [8] S. Lang, *Algebra*, Addison-Wesley Publishing Company, 1984.
- [9] P. Ribenboim, *Algebraic Numbers*, John Wiley and Sons Inc. 1972.
- [10] G. H. Hardy and Wright, E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford: Oxford University Press, 1980.
- [11] Harold G. Diamond, Frank Gerth III, and Jeffrey D. Vaaler, *Guass Sums and Fourier Analysis on Multiplicative subgroups of  $Z_q$* , Transactions of the American Mathematical Society, **277** (1983), no. 2, 711-726.
- [12] Yim su bin, *Semi-cyclotomic polynomial*, Master degree thesis paper, Korea National University of Education (2017).
- [13] Lim sang a, *The coefficients of Galois polynomial*, Master degree thesis paper, Korea National University of Education (2018).
- [14] Bae Jae Yun, *Irreducibility of Galois polynomials when  $n$  has positive square factor*, Master degree thesis paper, Korea National University of Education (2018).

\*\*

Department of Mathematics Education  
 Korea National University of Education  
 Chungbuk 363-791, Republic of Korea  
*E-mail:* dlwldms818@gmail.com

\*

Department of Mathematics Education  
 Korea National University of Education  
 Chungbuk 363-791, Republic of Korea  
*E-mail:* ksleeknue@gmail.com