Commun. Korean Math. Soc. **32** (2017), No. 1, pp. 1–6
https://doi.org/10.4134/CKMS.c160003
pISSN: 1225-1763 / eISSN: 2234-3024

GALOIS IRREDUCIBLE POLYNOMIALS

Miyeon Kwon, Ji-Eun Lee, and Ki-Suk Lee

Abstract. In this paper, the fundamental theorem of Galois Theory is used to generalize cyclotomic polynomials and construct irreducible polynomials associated with the n-th primitive roots of unity.

1. Introduction

Let n be a positive integer and w be the n-th primitive root of unity, that is, $w = e^{\frac{2\pi i}{n}}$.

If a monic polynomial $p(x)$ with integer coefficients satisfies that $p(w) = 0$ and is irreuducible over the field of rational numbers, $p(x)$ is called the n-th cyclotomic polynomial, denoted by $\Phi_n(x)$.

It is well-known (see [3]) that the n-th cyclotomic polynomial $\Phi_n(x)$ is equal to

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

where $\mathbb{Z}_n^*$ is the multiplicative group of integers modulo n.

In this paper, we use the fundamental theorem of Galois theory to generalize cyclotomic polynomials and give an algorithm to generate irreducible polynomials associated with the n-th primitive roots of unity.

2. Galois irreducible polynomials

Throughout the paper, we assume that n is a postive integer and $w = e^{\frac{2\pi i}{n}}$ is the n-th primitive root of unity. Following the conventional notations, $\mathbb{Q}$ and $\mathbb{Q}[x]$ denote the field of rational numbers and the polynomial ring over $\mathbb{Q}$, respectively.

Let H be a subgroup of $\mathbb{Z}_n^*$ and $\mathbb{Z}_n^*/H = \{h_1H, h_2H, \ldots, h_lH\}$ be its corresponding quotient group. For each $k = 1, \ldots, l$, define $a_k = \sum_{h \in H} w^{h_k h}$.

We now consider the monic polynomial having $a_1, \ldots, a_l$ as its roots, denoted by $J_{n,H}(x)$. Then $J_{n,H}(x) = (x - a_1)(x - a_2) \cdots (x - a_l)$. Especially, if $H = \{1\}$, then $J_{n,H}(x) = \Phi_n(x)$. This paper concerns irreducible polynomials with

Received January 5, 2016.

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

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

integer coefficients in the form of $J_{n,H}(x)$. Such irreducible polynomials will be called Galois irreducible polynomials.

In this section, we will show that any $J_{n,H}(x)$ is a monic polynomial with integer coefficients. In particular, if n is a prime number, any $J_{n,H}(x)$ is irreducible over $\mathbb{Q}$. We will prove this by showing that $\sigma(J_{n,H}(x)) = J_{n,H}(x)$ for any $\sigma \in Gal(\mathbb{Q}(w)/\mathbb{Q})$, where $\mathbb{Q}(w)$ is the simple extension field of $\mathbb{Q}$ containing w and $Gal(\mathbb{Q}(w)/\mathbb{Q})$ is the Galois group of $\mathbb{Q}(w)$ over $\mathbb{Q}$. We first recall a well-known result (see [1]) about $Gal(\mathbb{Q}(w)/\mathbb{Q})$.

Lemma 2.1. *Let $\mathbb{Q}(w)$ be the simple extension field of $\mathbb{Q}$ containing w. Then the Galois group $Gal(\mathbb{Q}(w)/\mathbb{Q})$ over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}_n^*$ with the mapping $\theta : \mathbb{Z}_n^* \to Gal(\mathbb{Q}(w)/\mathbb{Q})$, defined by $\theta[k](w) = w^k$.*

For a subgroup H of $\mathbb{Z}_n^*$ and $\mathbb{Z}_n^*/H$, if we let $\xi = \Sigma_{h\in H} w^h$, then we can use the mapping θ defined in Lemma 2.1 to express $a_1, \dots, a_l$ in terms of ξ as follows.

$$
\begin{aligned}
a_1 &= \sum_{h\in H} w^{h_1 h} = \theta[h_1](\xi),\\
a_2 &= \sum_{h\in H} w^{h_2 h} = \theta[h_2](\xi),\\
&\vdots\\
a_l &= \sum_{h\in H} w^{h_l h} = \theta[h_l](\xi).
\end{aligned}
$$

For any $k \in \mathbb{Z}_n^*$, the mapping $\tau_k : \mathbb{Z}_n^*/H \to \mathbb{Z}_n^*/H$, defined by $\tau_k(h_i H) = kh_i H$, is a bijection on $\mathbb{Z}_n^*/H$. Moreover, $\theta[k](\xi) = \theta[k'](\xi)$ for any k and $k' \in h_i H$. This allows us to claim that $\{\theta[kh_1](\xi), \dots, \theta[kh_l](\xi)\} = \{a_1, \dots, a_l\}$ for any $k \in \mathbb{Z}_n^*$ and therefore $J_{n,H}(x) = (x - a_1)(x - a_2)\cdots(x - a_l)$ is in $\mathbb{Q}[x]$ as the following theorem asserts.

Theorem 2.2. *For any subgroup H of $\mathbb{Z}_n^*$, $J_{n,H}(x)$ is in $\mathbb{Q}[x]$.*

Proof. For each $\sigma \in Gal(\mathbb{Q}(w)/\mathbb{Q})$, there is a $k \in \mathbb{Z}_n^*$ such that $\sigma = \theta[k]$.

$$
\begin{aligned}
\theta[k](J_{n,H}(x)) &= (x - \theta[k](a_1))(x - \theta[k](a_2))\cdots(x - \theta[k](a_l))\\
&= (x - \theta[kh_1](\xi))(x - \theta[kh_2](\xi))\cdots(x - \theta[kh_l](\xi))\\
&= (x - a_1)(x - a_2)\cdots(x - a_l) = J_{n,H}(x). \qquad \square
\end{aligned}
$$

In fact, $J_{n,H}(x) \in \mathbb{Z}[x]$, the set of all polynomials with integer coefficients. To see this, note that each coefficient of $J_{n,H}(x)$ can be expressed as $k_0 + k_1 w + \cdots + k_m w^m$, where k_i's are integers.

Let $p(x) = k_0 + k_1 x + \cdots + k_m x^m$. Then $p(x) \in \mathbb{Z}[x]$. Since $\Phi_n(x)$ is a monic polynomial in $\mathbb{Z}[x]$, the long division allows us to rewrite $p(x)$ as $p(x) = \Phi_n(x)g(x) + r(x)$, where $r(x) \in \mathbb{Z}[x]$ is of degree less than $\phi(n)$. Note that $\phi(n)$ is the Euler's totient function that counts the positive integers less than or equal to n that are relatively prime to n.

Letting $x = w$, we get $p(w) = \Phi_n(w)g(w) + r(w) = r(w)$. That is,

$$k_0 + k_1 w + \cdots + k_m w^m = m_0 + m_1 w + \cdots + m_{\phi(n)-1} w^{\phi(n)-1}$$

for some integers $m_0, \ldots, m_{\phi(n)-1}$. Therefore the following theorem suffices to show that $J_{n,H}(x) \in \mathbb{Z}[x]$.

Theorem 2.3. *If A is a rational number in the form $A = m_0 + m_1 w + \cdots + m_{\phi(n)-1} w^{\phi(n)-1}$, where $m_0, \ldots, m_{\phi(n)-1}$ are integers, then A is an integer.*

Proof. Let $p(x) = (m_0 - A) + m_1 x + \cdots + m_{\phi(n)-1} x^{\phi(n)-1}$. Then $p(x) \in \mathbb{Q}[x]$ with $p(w) = 0$. Since $\Phi_n(x)$ is the minimal polynomial of w over $\mathbb{Q}$ (i.e., the irreducible polynomial over $\mathbb{Q}$ having w as one of its zeros), $\Phi_n(x)$ divides $p(x)$. By noting that the degree of $p(x)$ is less than $\phi(n)$, we can conclude that $p(x) = 0$, equivalently $m_0 = A, m_1 = 0, \ldots, m_{\phi(n)-1} = 0$. $\square$

We here recall the Möbius function defined on the set of positive integers. For any positive integer n, the Möbius function, denoted by $\mu(n)$, is defined to be the sum of the primitive n-th roots of unity, that is, $\mu(n) = \sum_{k \in \mathbb{Z}_n^*} w^k$. It is known (see [2]) that $\mu(n)$ has values in $\{-1, 0, 1\}$ depending on the factorization of n into prime factors:

- $\mu(n) = 1$ if n is a square-free integer with an even number of prime factors.
- $\mu(n) = -1$ if n is a square-free integer with an odd number of prime factors.
- $\mu(n) = 0$ if n has a squared prime factor.

This enables us to identify $J_{n,H}(x)$ when $\xi = \sum_{h \in H} w^h$ is in $\mathbb{Q}$ as stated below.

Corollary 2.4. *Let H be a proper subgroup of $\mathbb{Z}_n^*$. If $\xi = \sum_{h \in H} w^h \in \mathbb{Q}$, then $\xi = 0$ and hence $J_{n,H}(x) = x^l$, where $l = |\mathbb{Z}_n^*/H|$.*

Proof. If $\xi = \sum_{h \in H} w^h \in \mathbb{Q}$, then $\xi = N$ for some integer N and $a_1 = a_2 = \cdots = a_l = N$. Therefore $Nl = a_1 + a_2 + \cdots + a_l = \Sigma_{k \in \mathbb{Z}_n^*} w^k$. Since $\sum_{k \in \mathbb{Z}_n^*} w^k = \mu(n)$ and $\mu(n)$ has values in $\{-1, 0, 1\}$, we can conclude that $N = 0$ as $l \geq 2$. This completes the proof that $J_{n,H}(x) = (x - a_1) \cdots (x - a_l) = x^l$. $\square$

For example, let us look at the case of $n = 8$. Then $w = e^{2\pi i/8}$ and $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$. If we choose $H = \{1, 5\}$, then we get $a_1 = w + w^5 = 0$ and $a_2 = w^3 + w^7 = 0$, leading to $J_{8,H}(x) = x^2$. However, this oocurs only when $\mu(n) = 0$, that is, n has a squared prime factor. In fact, if $\mu(n) \neq 0$, then any polynomial in the form of $J_{n,H}(x)$ is irreducible over $\mathbb{Q}$. We will prove it in Theorem 3.6. The following theorem proves its special case when n is a prime number.

Theorem 2.5. *If p is a prime number, then $J_{p,H}(x)$ is the minimal polynomial of $\xi = \sum_{h \in H} w^h$ over $\mathbb{Q}$ for any subgroup H of $\mathbb{Z}_p^*$.*

Proof. Let $P(x)$ be the minimal polynomial of ξ over $\mathbb{Q}$. Then for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(w)/\mathbb{Q})$, $\sigma(\xi)$ is a zero of $P(x)$. Since $\{1, w, \ldots, w^{p-1}\}$ is a basis of $\mathbb{Q}(w)$ over $\mathbb{Q}$, it is clear that $\sum_{h\in H} w^h \neq \sum_{h'\in H'} w^{h'}$ whenever H and H' are disjoint subsets of $\mathbb{Z}_p^*$. Hence $a_1, \ldots, a_l$ are distinct zeros of $P(x)$. As a result, we have that $J_{n,H}(x) = (x-a_1)\cdots(x-a_l)$ divides $P(x)$. This completes the proof. □

For example, let us look at the case of $p = 7$. Then $w = e^{2\pi i/7}$ and $\mathbb{Z}_7^*$ has 4 subgroups: $H_1 = \{1\}$, $H_2 = \{1, 6\}$, $H_3 = \{1, 2, 4\}$, and $H_4 = \mathbb{Z}_7^*$.

Clearly, $J_{7,H_1}(x) = \Phi_7(x)$ and $J_{7,H_4}(x) = x - 1$. Elementary calculations give $J_{7,H_2}(x)$ and $J_{7,H_3}(x)$ as follows.

$$\begin{aligned} J_{7,H_2}(x) &= (x - (w + w^6))(x - (w^2 + w^5))(x - (w^3 + w^4)) \\ &= x^3 + x^2 - 2x - 1; \\ J_{7,H_3}(x) &= (x - (w + w^2 + w^4))(x - (w^3 + w^5 + w^6)) \\ &= x^2 + x + 2. \end{aligned}$$

3. Irreducibilty of $J_{n,H}(x)$

In this section, we study the irreducibility of $J_{n,H}(x)$ when n is not necessarily prime. First of all, it is clear that $J_{n,H}(x)$ is irreducible over $\mathbb{Q}$ if and only if $a_1, \ldots, a_l$ are distinct: Let $\xi = \sum_{h\in H} w^h$ and $P(x)$ be the minimal polynomial of ξ over $\mathbb{Q}$. Since $\mathbb{Q}(w)$ is a normal extention of $\mathbb{Q}$, $P(x)$ is separable in $\mathbb{Q}(w)$ with $P(\sigma(\xi)) = 0$ for all $\sigma \in Gal(\mathbb{Q}(w)/\mathbb{Q})$. In other words, $P(x)$ is a product of linear factors over $\mathbb{Q}(w)$ that includes all distinct factors of $(x - a_1), \ldots, (x - a_l)$.

The fundamental theorem of Galois theory (see [1]) allows us to obtain another equivalent condition on H for irreducible polynomials $J_{n,H}(x)$.

Theorem 3.1. *Let H be a subgroup of $\mathbb{Z}_n^*$ and $\mathbb{Z}_n^*/H = \{h_1H, \ldots, h_lH\}$. Let $a_k = \sum_{h\in H} w^{h_k h}$, $k = 1, \ldots, l$ and $\mathbb{Q}(w)_H$ be the subfield of $\mathbb{Q}(w)$ fixed by $\{\theta[h] : h \in H\}$. Then $J_{n,H}(x) = (x-a_1)\cdots(x-a_l)$ is irreducible over $\mathbb{Q}$ if and only if $\mathbb{Q}(\xi) = \mathbb{Q}(w)_H$, where $\xi = \sum_{h\in H} w^h$.*

Proof. For any $h^* \in H$, $\theta[h^*](\xi) = \sum_{h\in H} w^{h^* h} = \sum_{h\in H} w^h = \xi$, since H is a subgroup of $\mathbb{Z}_n^*$. This implies that $\xi \in \mathbb{Q}(w)_H$ and hence $\mathbb{Q}(\xi)$ is a subfield of $\mathbb{Q}(w)_H$ with $[\mathbb{Q}(w)_H : \mathbb{Q}(\xi)]\,[\mathbb{Q}(\xi) : \mathbb{Q}] = l$.

Let $P(x)$ be the minimal polynomial of ξ over $\mathbb{Q}$. Then $P(x)$ is a polynomial in $\mathbb{Q}[x]$ of degree equal to $[\mathbb{Q}(\xi) : \mathbb{Q}]$ and divides $J_{n,H}(x)$. Putting together, we can conclude that

$$\begin{aligned} \mathbb{Q}(\xi) = \mathbb{Q}(w)_H \quad &\Leftrightarrow \quad [\mathbb{Q}(\xi) : \mathbb{Q}] = l \\ &\Leftrightarrow \quad \deg(P(x)) = l \\ &\Leftrightarrow \quad P(x) = J_{n,H}(x). \end{aligned}$$
□

Theorem 3.1 leads us to several corollaries as follows.

Corollary 3.2. *Let p be a prime number and $w = e^{2\pi i/p}$. Then any subfield F of $\mathbb{Q}(w)$ over $\mathbb{Q}$ can be expressed as $F = \mathbb{Q}(\xi)$, where $\xi = \sum_{h\in H} w^h$ for some subgroup H of $\mathbb{Z}_p^*$.*

Proof. For each subfield F of $\mathbb{Q}(w)$ over $\mathbb{Q}$, $\mathrm{Gal}(\mathbb{Q}(w)/F)$ is a subgroup of $\mathrm{Gal}(\mathbb{Q}(w)/\mathbb{Q})$, which is isomorphic to $\mathbb{Z}_n^*$ with the correspondence $k \mapsto \theta[k](w) = w^k$. Let H be the subgroup of $\mathbb{Z}_n^*$ corresponding to $\mathrm{Gal}(\mathbb{Q}(w)/F)$. By Theorem 2.5, $J_{p,H}(x)$ is irreducible and therefore $F = \mathbb{Q}(\xi)$, where $\xi = \sum_{h\in H} w^h$. □

Corollary 3.3. *If H is a maximal subgroup of $\mathbb{Z}_n^*$ and $\xi = \sum_{h\in H} w^h \notin \mathbb{Q}$, then $J_{n,H}(x)$ is irreducible over $\mathbb{Q}$.*

Proof. Suppose that H is a maximal subgroup of $\mathbb{Z}_n^*$. Then $\mathbb{Z}_n^*/H$ is a cyclic group of order p, where p is prime. From the proof of Theorem 3.1, we get $[\mathbb{Q}(w)_H : \mathbb{Q}(\xi)]\,[\mathbb{Q}(\xi) : \mathbb{Q}] = p$. Since $\xi \notin \mathbb{Q}$, $[\mathbb{Q}(\xi) : \mathbb{Q}] = p$ and therefore $[\mathbb{Q}(w)_H : \mathbb{Q}(\xi)] = 1$, completing the proof. □

Lee and Kim in [4] proved the following corollary by showing that the zeros of the polynomial are distinct. We are going to use Theorem 3.1 to prove it.

Corollary 3.4. *For any positive integer $n > 2$,*

$$P(x) = \prod_{k\in\mathbb{Z}_n^*;\, k\le\phi(n)/2} (x - (w^k + w^{-k}))$$

is irreducible over $\mathbb{Q}$.

Proof. Consider the subgroup $H = \{1, -1\}$ of $\mathbb{Z}_n^*$ and let $\xi = w + w^{-1}$. Then note that $P(x) = J_{n,H}(x)$. We will show that $\mathbb{Q}(w)_H$, the subfield of $\mathbb{Q}(w)$ fixed by $\{\sigma \in \mathrm{Gal}(\mathbb{Q}(w)/\mathbb{Q}) : \sigma(w) = w \text{ or } w^{-1}\}$, is equal to $\mathbb{Q}(\xi)$.

Let α be any element in $\mathbb{Q}(w)_H$. Then $\alpha = \sum_{k=0}^m c_k w^k$ for some nonnegative integer m and $\sum_{k=0}^m c_k w^{-k} = \sum_{k=0}^m c_k w^k$. 2α can be expressed as $2\alpha = \sum_{k=0}^m c_k(w^k + w^{-k})$. Note that for each $k \ge 0$,

$$w^{(k+1)} + w^{-(k+1)} = (w^k + w^{-k})(w + w^{-1}) - (w^{(k-1)} + w^{-(k-1)}).$$

By the mathematical induction, it is clear that each $w^k + w^{-k} \in \mathbb{Q}(\xi)$ and hence $\alpha \in \mathbb{Q}(\xi)$. This implies that $\mathbb{Q}(w)_H \subseteq \mathbb{Q}(\xi)$. By recalling $\mathbb{Q}(\xi) \subseteq \mathbb{Q}(w)_H$, we can conclude that $\mathbb{Q}(w)_H = \mathbb{Q}(\xi)$ and therefore $J_{n,H}(x)$ is irreducible. □

For example, consider the subgroup $H = \{1, 8\}$ of $\mathbb{Z}_9^*$. Then we get $a_1 = w + w^{-1}$, $a_2 = w^2 + w^{-2}$, $a_3 = w^4 + w^{-4}$ and

$$J_{9,H}(x) = (x - a_1)(x - a_2)(x - a_3) = x^3 - 3x + 1.$$

As a result of Corollary 3.4, it can be shown that $\cos(\frac{2\pi k}{n})$ is irrational whenever k is relatively prime to n.

Theorem 3.5. *If $k \in \mathbb{Z}_n^*$ and $n > 2$, then $\cos\left(\frac{2\pi}{n}k\right) \notin \mathbb{Q}$.*

Proof. In the proof of Corollary 3.4, we showed that $J_{n,\{1,-1\}}(x)$ is an irreducible polynomial over $\mathbb{Q}$ whose zeros are $w^k + w^{-k}$ for $k \in \mathbb{Z}_n^*$. This implies that none of $w^k + w^{-k}$ is in $\mathbb{Q}$. Therefore $\frac{1}{2}(w^k + w^{-k}) = \cos\left(\frac{2\pi}{n}k\right) \notin \mathbb{Q}$. $\square$

We will conclude the section with the following theorem asserting that $J_{n,H}(x)$ is irreducible over $\mathbb{Q}$ whenever n has no squared prime factor.

Theorem 3.6. *Let n be a square-free integer, meaning that n does not have any squared prime factor. Then $J_{n,H}(x)$ is irreducible over $\mathbb{Q}$ for any subgroup H of $\mathbb{Z}_n^*$.*

Proof. Let H be a subgroup of $\mathbb{Z}_n^*$ and $\xi = \sum_{h \in H} w^h$. Suppose that $P(x)$ is the minimal polynomial of ξ over $\mathbb{Q}$. Note that $P(x)$ is also the minimal polynomial of a_i, $i = 1, \ldots, l$, since each a_i can be expressed as $a_i = \sigma(\xi)$ for some $\sigma \in Gal(\mathbb{Q}(w)/\mathbb{Q})$. Hence, $J_{n,H}(x) = (x - a_1) \cdots (x - a_l)$ divides $(P(x))^l$. This allows us to express $J_{n,H}(x)$ as $J_{n,H}(x) = (P(x))^k$ for some positive integer k. Then k times the sum of all zeros of $P(x)$ is equal to $\sum_{k \in \mathbb{Z}_n^*} w^k$ whose value is 1 or -1. We proved in Theorem 2.3 that the sum of all zeros of $P(x)$ is an integer. Therefore k must be 1, implying that $J_{n,H}(x)$ is the miminal polynomial of ξ over $\mathbb{Q}$. $\square$

References

[1] J. R. Bastida and R. Lyndon, *Field Extensions and Galois Theory*, Encyclopedia of Mathematics and Its Application, Addison-Wesley Publishing Company, 1984.

[2] G. H. Hardy, Wright, and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford: Oxford University Press, 1980.

[3] S. Lang, *Algebra*, Addison-Wesley Publising Company, 1984.

[4] K. S. Lee, J. E. Lee, and J. H. Kim, *Semi-cyclotomic polynomials*, Honam Math. Soc. **37** (2015), no. 4, 469–472.

Miyeon Kown
Department of Mathematics
University of Wisconsin-Platteville
Platteville, WI 53818, USA
E-mail address: kwonmi@uwplatt.edu

Ji-Eun Lee
Department of Mathematics Education
Korea National University of Education
Chungbuk 363-791, Korea
E-mail address: dlwldms818@gmail.com

Ki-Suk Lee
Department of Mathematics Education
Korea National University of Education
Chungbuk 363-791, Korea
E-mail address: ksleeknue@gmail.com