Honam Mathematical J. **37** (2015), No. 4, pp. 469–472
http://dx.doi.org/10.5831/HMJ.2015.37.4.469

SEMI-CYCLOTOMIC POLYNOMIALS

Ki-Suk Lee, Ji-Eun Lee and Ji-Hye Kim

Abstract. The n-th cyclotomic polynomial $\Phi_n(x)$ is irreducible over $\mathbb{Q}$ and has integer coefficients. The degree of $\Phi_n(x)$ is $\varphi(n)$, where $\varphi(n)$ is the Euler Phi-function. In this paper, we define Semi-Cyclotomic Polynomial $J_n(x)$. $J_n(x)$ is also irreducible over $\mathbb{Q}$ and has integer coefficients. But the degree of $J_n(x)$ is $\frac{\varphi(n)}{2}$. Galois Theory will be used to prove the above properties of $J_n(x)$.

1. Introduction

Given a positive integer n, the integers between 1 and n which are co-prime to n form a group with multiplication modulo n as the operation. It is denoted by $\mathbb{Z}_n^*$ and is called the multiplicative group of integers modulo n. The Galois group $Gal_{\mathbb{Q}}\mathbb{Q}(\alpha)$ of $x^n - 1$ is isomorphic to $\mathbb{Z}_n^*$, where $\alpha = e^{\frac{2\pi}{n}i}$.

It is well-known that the n-th cyclotomic polynomial $\Phi_n(x)$ is an irreducible polynomial in $\mathbb{Z}[x]$. Here we give the following theorems about the n-th cyclotomic polynomials. Galois Theory will give an easy proof of the irreducibility of $\Phi_n(x)$.

Let U_n be the set consisting of all primitive n-th roots of unity in $\mathbb{C}$, the complex number field.

$$\Phi_n(x) = \prod_{a \in U_n} (x - a)$$

is said to be the n-th cyclotomic polynomial.

Theorem 1.1. *If n is a positive integer, then $\Phi_n(x)$ is in $\mathbb{Q}[x]$.*

Proof. Every Galois map in $Gal_{\mathbb{Q}}\mathbb{Q}(\alpha)$ can be considered as a map from U_n to U_n which is injective and surjective. Since $\Phi_n(x)$ is fixed by every map in $Gal_{\mathbb{Q}}\mathbb{Q}(\alpha)$, all coefficients of $\Phi_n(x)$ are in $\mathbb{Q}$. □

Received September 5, 2015. Accepted November 14, 2015.
2010 Mathematics Subject Classification. 12D05, 12E05, 12F05, 12F10.
Key words and phrases. n-th cyclotomic polynomial, semi-cyclotomic polynomial, irreducible polynomial.

In fact, the coefficients of $\Phi_n(x)$ are integers. [[3], Thoerem 4.1, V]

Theorem 1.2. *If n is a positive integer, then $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.*

Proof. If $\Phi_n(x)$ is reducible in $\mathbb{Q}[x]$, then $\Phi_n(x) = h(x) \cdot k(x)$ in $\mathbb{Q}[x]$ with $\deg h(x) > 0$, $\deg k(x) > 0$. We may assume that $h(x)$ has $(x-\alpha)$ as a factor and misses $(x-\alpha^r)$, with $r \neq 1$, $(n,r) = 1$. Then $h(x) = (x-\alpha) \cdot h^*(x)$ and $k(x) = (x-\alpha^r) \cdot k^*(x)$.

Let ϕ_i in $Gal_{\mathbb{Q}}\mathbb{Q}(\alpha)$ be the map such that $\phi_i(\alpha) = \alpha^i$, for an integer i. There exists ϕ_r in $Gal_{\mathbb{Q}}\mathbb{Q}(\alpha)$ which sends $(x-\alpha)$ to $(x-\alpha^r)$. Then $h(x) \in \mathbb{Q}[x]$ is not fixed by ϕ_r. This is a contradiction. □

2. Semi-cyclotomic polynomial

In this chapter, we define semi-cyclotomic polynomial, $J_n(x)$. We prove that the coefficients of $J_n(x)$ are integers and $J_n(x)$ is irreducible in $\mathbb{Q}$.

If $(n,r) = 1$, then $(n, n-r) = 1$.

So ${Z_n}^*$ can be written as $\{r_1, r_2, \cdots, r_k, -r_k, \cdots, -r_2, -r_1\}$, where $k = \frac{\varphi(n)}{2}$ and $(n, r_j) = 1$, for $j = 1, 2, \cdots, k$.

Let $\alpha = e^{\frac{2\pi}{n}i}$. Then α is a primitive n-th root of unity in $\mathbb{C}$.

Let $a_1 = \alpha^{r_1} + \alpha^{-r_1}$, $\cdots$, $a_k = \alpha^{r_k} + \alpha^{-r_k}$.

We define semi-cyclotomic polynomial as

$$J_n(x) = (x-a_1)(x-a_2)\cdots(x-a_k).$$

Theorem 2.1. *$J_n(x)$ is in $\mathbb{Q}[x]$.*

Proof. We may write the Galois group of $x^n - 1$ as

$$Gal_{\mathbb{Q}}\mathbb{Q}(\alpha) = \{\phi_{r_1}, \phi_{r_2}, \cdots, \phi_{r_k}, \phi_{-r_k}, \cdots, \phi_{-r_1}\} ,$$

where $\phi_{r_j}(\alpha) = \alpha^{r_j}$.

Let $S = \{a_1, ..., a_k\}$. Since $H = \{r_1, -r_1\} = \{1, -1\}$ is a subgroup of $\mathbb{Z}_n^*$ and $\{r_k, -r_k\} = r_k\{1, -1\}$ are cosets of H, every Galois map ϕ_{r_j} can be considered as a function from S to S, which is injective and surjective. This implies $J_n(x)$ is fixed by $Gal_{\mathbb{Q}}\mathbb{Q}(\alpha)$. Therefore $J_n(x)$ is in $\mathbb{Q}[x]$. □

Theorem 2.2. *$J_n(x)$ is in $\mathbb{Z}[x]$.*

Proof. Every coefficients of $J_n(x)$ can be written as $k_0 + k_1\alpha + \cdots + k_m\alpha^m$, where k_i's are integers. Since the coefficients of $J_n(x)$ are rational, they are integers because of the following Lemma. □

Lemma 2.3. *If A is a rational number which can be written as $k_0 + k_1\alpha + \cdots + k_m\alpha^m$ (where k_i's are integers), then A is an integer.*

Proof. $\mathbb{Q}(\alpha)$ is a vector space over $\mathbb{Q}$ with dimension $\varphi(n)$. We may choose

$$\left\{1, \alpha, \alpha^2, \cdots, \alpha^{\varphi(n)-1}\right\}$$

as a basis. Then $\Phi_n(x)$ is a monic polynomial in $\mathbb{Z}[x]$ and α is a root of $\Phi_n(x)$. Since degree of $\Phi_n(x)$ is $\varphi(n)$, we can replace $\alpha^{\varphi(n)}$ with lower power terms. So A can be written as

$$A = m_0 + m_1\alpha + m_2\alpha^2 + \cdots + m_t\alpha^t,$$

where $t = \varphi(n)-1$ and m_i's are integers. Since $\left\{1, \alpha, \alpha^2, \cdots, \alpha^{\varphi(n)-1}\right\}$ is a basis, the above expression of A is unique. Therefore if A is a rational number, every m_i's must be zero except m_0. So A is an integer. □

Theorem 2.4. *$J_n(x)$ is irreducible over $\mathbb{Q}$.*

Proof. Note that $a_j = 2\cos(\frac{2\pi}{n}r_j)$ for $j = 1, 2, \cdots, k$. This implies $a_1, \cdots, a_k$ are all distinct.

If $J_n(x)$ is reducible, then $J_n(x) = h(x)\cdot k(x)$ in $\mathbb{Q}[x]$ with $\deg h(x) > 0$, $\deg k(x) > 0$. We may assume that $h(x)$ has $(x - a_1)$ as a factor and misses $(x - a_j)$, with $j \neq 1$. Then $h(x) = (x - a_1)\cdot h^*(x)$ and $k(x) = (x - a_j)\cdot k^*(x)$. There exists ϕ_{r_j} in $Gal_{\mathbb{Q}}\mathbb{Q}(\alpha)$, which sends $(x - a_1)$ into $(x - a_j)$. Then $h(x) \in \mathbb{Q}[x]$ is not fixed by ϕ_{r_j}, which is a contradiction. □

3. Applications

We may use $J_n(x)$ to prove the irrationality of some cosine function values. Also impossibility of trisection of 60° will be proved.

Theorem 3.1. *If $\varphi(n) > 2$ and $(n, k) = 1$, then $\cos(\frac{2\pi k}{n})$ is not a rational number.*

Proof. Let $a_k = \alpha^k + \alpha^{-k}$ for $(n, k) = 1$, then $a_k = 2\cos(\frac{2\pi k}{n})$. Since the irreducible polynomial $J_n(x)$ has a_k as a root, $J_n(x)$ is the minimal polynomial of $2\cos(\frac{2\pi k}{n})$ over $\mathbb{Q}$.
If $\varphi(n) > 2$, the degree of $J_n(x)$ is greater than 1. This implies $\cos(\frac{2\pi k}{n})$ is not a rational number. □

Theorem 3.2. *An angle of 60° cannot be trisected by straight edge and compass.*

Proof. $2\cos 20^\circ$ is a root of $J_{18}(x)$. The degree of $J_{18}(x)$ is $\frac{\varphi(18)}{2} = 3$. Since 3 is not a power of 2, $2cos20^\circ$ is not a constructible number. [[2], Theorem 15.9] □

References

[1] J. R. Bastida and R. Lyndon, *Field Extensions and Galois Thory*, Encyclopedia of Mathmatics and Its Application, Addison-Wesley Publishing Company (1984).
[2] T. W. Hungerford, *Abstract Algebra An Introduction*, Brooks/Cole, Cengage Learning (2014).
[3] S. Lang, *Algebra*, Addison-Wesley Publishing Company (1984).
[4] P. Ribenboim, *Algebraic Numbers*, John Wiley *and* Sons Inc (1972).

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

Ji-Eun Lee
Myogok Elementary School,
Gangdonggu, Seoul 134-805, Republic of Korea.
E-mail: dlwldms818@gmail.com

Ji-Hye Kim
Department of Mathematics Education, Korea National University of Education,
Cheongjusi, Chungbuk 363-791, Republic of Korea.
E-mail: hyekj83@naver.com