Notes on Cyclotomic Polynomials and the Galois Group of Cyclotomic Extensions

Yang Li **Kee Siong Ng**
School of Computing
Australian National University
Canberra, ACT, 2600

April 13, 2022

1 Cyclotomic Polynomial and Cyclotomic Extension

Cyclotomic polynomials are widely used in the construction of homomorphic encryption schemes based on Ring Learning With Error problems. In this short note, we attempt a self-contained introduction to the cyclotomic polynomials and the Galois groups of cyclotomic extensions.

1.1 Cyclotomic polynomials

Cyclotomic polynomials are polynomials whose roots are the primitive roots of unity.

Roots of unity **Definition 1.1.1.** *For any positive integer n, the n-th roots of unity are the (complex) solutions to the equation $x^n = 1$, and there are n solutions to the equation.*

Theorem 1.1.2. *Let n be a positive integer and define $\zeta_n = e^{2\pi i/n}$. Then the set of all n-th roots of unity is given by*

$$\{\zeta_n^k \mid k = 0, 1, \dots, n-1\}, \tag{1}$$

Proof. By Euler's formula, we have

$$e^{2\pi i} = \cos(2\pi) + i\sin(2\pi) = 1$$

and that $(e^{2\pi i})^k = e^{2k\pi i} = 1$ for all $k \in \{0, 1, \dots, n-1\}$. To solve for $x^n = 1$, note that

$$x^n = 1 = e^0 = e^{2\pi i} = e^{4\pi i} = e^{6\pi i} = \cdots = e^{2k\pi i}.$$

Raising each term to the power of $1/n$ yields

$$x = (x^n)^{1/n} = 1 = e^{2\pi i/n} = e^{4\pi i/n} = e^{6\pi i/n} = \cdots = e^{2k\pi i/n}.$$

Therefore, there are n distinct solutions to $x^n = 1$, each given by ζ_n^k, for $k = 0, 1, \dots, n-1$ □

Example 1.1.3. *The 1st root of unity is 1. The 2nd roots of unity are $\zeta_2^0 = 1$ and $\zeta_2^1 = -1$. The 3rd roots of unity are $\zeta_3^0 = 1$, $\zeta_3^1 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ and $\zeta_3^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$.*

We sometimes drop the subscript to ζ_n if the context is clear.

Geometrically, we can interpret the nth roots of unity as the points that are evenly spread on the unit circle in the complex plane, starting from 1 on the real axis. (The word "cyclotomic" means "circle-dividing".) Equivalently, they are the vertices of a regular n-gon that lie on the unit circle, with the real value 1 as one of the n vertices. Figure 1 illustrates the 3rd roots of unity.

In general, the equation $x^n = 1$ can be defined over different fields. In the real field $\mathbb{R}$, the only possible roots of unity are ± 1. In the complex field $\mathbb{C}$, the nth roots of unity form a cyclic group under multiplication. The generator is $e^{2\pi i/n}$ and the group order is n, as shown in Theorem 1.1.2. In a finite field, for example $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6\}$, the 3rd roots of unity are $\{1, 2, 4\}$, because these are the only numbers equal to 1 modulo 7 when raising to the third power.

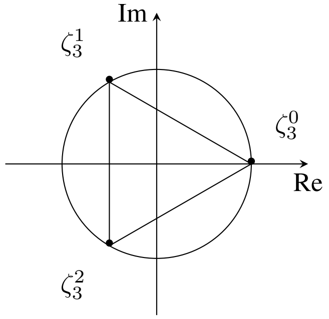

Figure 1: The 3rd roots of unity $\zeta^0 = 1$, $\zeta^1 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ and $\zeta^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$.

Primitive root

Definition 1.1.4. *An n-th root of unity r is called* ***primitive*** *if it is not a d-th root of unity for any integer d smaller than n; i.e. $r^n = 1$ and $r^d \neq 1$ for $d < n$.*

Geometrically, r is primitive if it is a vertex of a regular polygon that lies on the unit circle, but not a vertex of a smaller regular polygon that lies on the unit circle.

Example 1.1.5. *1 is not primitive. The two real roots ± 1 of the 4th roots of unity are not primitive, because they are also the 2nd roots of unity. Both complex roots of the 3rd roots of unity are primitive. The primitive 6th roots of unity are shown in Figure 2.*

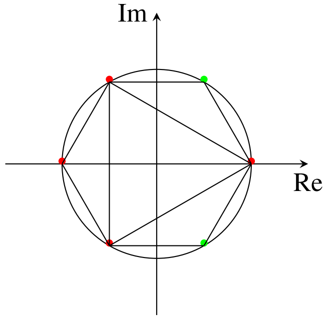

Figure 2: The 6th roots of unity $\zeta^0 = 1, \zeta^1 = \frac{1}{2}+i\frac{\sqrt{3}}{2}, \zeta^2 = -\frac{1}{2}+i\frac{\sqrt{3}}{2}, \zeta^3 = -1, \zeta^4 = -\frac{1}{2}-i\frac{\sqrt{3}}{2}, \zeta^5 = \frac{1}{2} - i\frac{\sqrt{3}}{2}$. The primitive roots are ζ^1, ζ^5 that are coloured in green. $\zeta^0, \zeta^2, \zeta^4$ are not primitive because they are also the 3rd roots of unity. ζ^0, ζ^3 are not primitive because they are also the 2nd roots of unity.

The following theorem provides an easy way to find the n-th primitive roots of unity.

Theorem 1.1.6. *The n-th primitive roots of unity are $\{\zeta_n^k \mid 1 \leq k \leq n-1$ and $\gcd(k,n) = 1\}$.*

If n is prime, then all the n-th roots of unity except 1 are primitive. It follows from Theorem 1.1.6 that the number of n-th primitive roots of unity is equal to the number of natural numbers smaller than n that is coprime with n, which is also known as the **Euler's totient function**

$$\phi(n) = |\{k \mid 1 \leq k \leq n-1 \text{ and } \gcd(k,n) = 1\}|.$$

For example, there are four 12th primitive roots of unity $\{\zeta, \zeta^5, \zeta^7, \zeta^{11}\}$.

We now have the necessary components to define cyclotomic polynomials.

Cyclotomic polynomial

Definition 1.1.7. *The* ***n-th cyclotomic polynomial*** $\Phi_n(x)$ *is the polynomial whose roots are the n-th primitive roots of unity. That is,*

$$\Phi_n(x) = \prod_{\substack{1\leq k<n \\ \gcd(k,n)=1}} (x - \zeta_n^k),$$

where $\zeta_n^k = e^{2k\pi i/n}$ is an nth root of unity (as before in Theorem 1.1.2).

n	$\Phi_n(x)$	roots
1	$x-1$	1
2	$x+1$	$\zeta^1 = -1$
3	x^2+x+1	ζ^1, ζ^2
4	x^2+1	$\zeta^1 = i, \zeta^3 = -i$
5	$x^4+x^3+x^2+x+1$	$\zeta^1, \zeta^2, \zeta^3, \zeta^4$
6	x^2-x+1	ζ^1, ζ^5

Table 1: First few cylotomic polynomials

Example 1.1.8. *The first few cyclotomic polynomials and their roots are listed in Table 1. For $n = 4$, the 4th cyclotomic polynomial is $\Phi_4(x) = (x-i)(x+i) = x^2+1$, because the 4th roots of unity are $\{\pm 1, \pm i\}$ and the primitive roots are $\pm i$.*

Here are two special cases of cyclotomic polynomials.

Remark 1.1.9. *If n is prime, then the n-th cyclotomic polynomial is given by*

$$\Phi_n(x) = x^{n-1} + x^{n-2} + \cdots + 1 = \sum_{t=0}^{n-1} x^t.$$

If $n = p^k$ is a prime power, then the n-th cyclotomic polynomial is given by

$$\Phi_n(x) = \Phi_p(x^{n/p}) = \Phi_p(x^{p^{k-1}}) = \sum_{t=0}^{p-1} x^{tp^{k-1}}.$$

As a special case, when $p = 2$ and $m = 2n = p^k \geq 2$, the m-th cyclotomic polynomial is

$$\Phi_m(x) = x^n + 1.$$

This is directly related to the underlying ring in the ring Learning With Errors problem.

By definition, cyclotomic polynomials are monic and have $\phi(n)$ linear factors. In addition, $\Phi_n(x)$ divides $x^n - 1$ because the roots of the former are also roots of the latter, but not vice versa. This implies an important relationship:

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \tag{2}$$

Here are some special cases of Equation (2).

$$\begin{aligned}
x^2 - 1 &= (x-1)(x+1) \\
x^3 - 1 &= (x-1)(x^2+x+1) \\
x^4 - 1 &= (x^2-1)(x^2+1) = (x-1)(x+1)(x^2+1) \\
x^5 - 1 &= (x-1)(x^4+x^3+x^2+1) \\
x^6 - 1 &= (x^2-1)(x^2+x+1)(x^2-x+1) = (x^3-1)(x+1)(x^2-x+1)
\end{aligned}$$

Note the pattern that if d divides n, then $x^d - 1$ divides $x^n - 1$:

$$x^n - 1 = (x^d - 1)(x^{n-d} + x^{n-2d} + \cdots + x^d + 1).$$

More formally, note that

$$\begin{aligned}
x^n - 1 &= \prod_{1 \leq k \leq n} (x - \zeta_n^k) \\
&= \prod_{d:d|n} \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=d}} (x - \zeta_n^k) \\
&= \prod_{d:d|n} \Phi_{\frac{n}{d}}(x) \\
&= \prod_{d:d|n} \Phi_d(x).
\end{aligned}$$

The second equality is because $d \mid n$ splits $[1, n]$ into $\frac{n}{d}$ mutually exclusive subsets. The third equality uses the definition of cyclotomic polynomial. The last equality is because the subset of integers $\frac{n}{d}$ and d are identical.

Equation (2) says that a number is an n-th root of unity if and only if it is a d-th primitive root of unity for some natural number d that divides n.

Example 1.1.10. *The 6th roots of unity are shown in Figure 2. $\zeta^0 = 1$ is the 1st primitive root. ζ^3 is the 2nd primitive root. ζ^2 and ζ^4 are the 3rd primitive roots. ζ^1 and ζ^5 are the 6th primitive roots. Hence, the product of these four cyclotomic polynomials is a polynomial whose roots are the 6th roots of unity, i.e., $\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) = x^6 - 1$.*

Here are some important properties of cyclotomic polynomials.

Theorem 1.1.11. *The n-th cyclotomic polynomial $\Phi_n(x)$ is a degree $\phi(n)$ polynomial with integer coefficients.*

Minimal polynomial

Theorem 1.1.12. *The n-th cyclotomic polynomial is the minimal polynomial of a n-th primitive root of unity.*

This theorem implies that cyclotomic polynomials are irreducible over the field of rationals $\mathbb{Q}$.

1.2 Cyclotomic extensions

In this subsection, we use Galois theory to study the roots of cyclotomic polynomials and the symmetric structure in their permutations.

To motivate the use of Galois theory, we start with this well-known result.

Theorem 1.2.1. *If $P(x)$ is a polynomial of degree n with leading coefficient 1, then any symmetric polynomial in the roots of $P(x)$ can be written as a polynomial in the coefficients of $P(x)$.*

Example 1.2.2. *Consider a cubic polynomial with roots r, s, t:*

$$\begin{aligned} P(x) &= x^3 + bx^2 + cx + d \\ &= (x - r)(x - s)(x - t) \end{aligned}$$

Expanding out the second line, we get

$$x^3 - (r + s + t)x^2 + (rs + rt + st)x - rst.$$

Equating coefficients, we get the so-called elementary symmetric polynomials

$$\begin{aligned} -b &= r + s + t \\ c &= rs + rt + st \\ -d &= rst \end{aligned}$$

Let $Q(r, s, t) = r^3 + s^3 + t^3$ be a symmetric polynomial, which means switching any pair of variables results in the same polynomial. Then one can show that $Q(r, s, t) = -b^3 - 3bc - 9d$.

Group theory is the study of symmetries and Theorem 1.2.1 leads us to the study of the set of permutations of the roots of a polynomial, which is known as the Galois group of the polynomial.

Splitting field

Definition 1.2.3. *Let $P(x)$ be a polynomial with rational coefficients. The splitting field K of $P(x)$ is the smallest field that contains the roots of $P(x)$. (K is called the splitting field because we can split $P(x)$ into linear factors in K. Also, by the properties of a field, K can be understood as the set of multi-variate polynomial expressions in the roots of $P(x)$ with rational coefficients.)*

We want to understand the symmetricity of the elements of splitting field K of $P(x)$ with respect to permutations of the roots of $P(x)$. These permutations of roots are obtained via automorphisms.

Automorphism

Definition 1.2.4. *An automorphism α of the splitting field K of a polynomial $P(x)$ is a bijection from K to K such that*

$$\begin{aligned} \alpha(a + b) &= \alpha(a) + \alpha(b) \\ \alpha(ab) &= \alpha(a)\alpha(b). \end{aligned}$$

Note that for all $a \in K$ that is a rational number, $\alpha(a) = a$ by the property of α. It then follows that for all polynomials $Q(r_1, \ldots, r_n) \in K$, where each r_i is a root of $P(x)$, we have

$$\alpha(Q(r_1, \ldots, r_n)) = Q(\alpha(r_1), \ldots, \alpha(r_n)).$$

Now consider $P(r_i)$, which is a polynomial in a root of $P(x)$ so $P(r_i) \in K$. Since

$$P(\alpha(r_i)) = \alpha(P(r_i)) = \alpha(0) = 0,$$

we can see that an automorphism always send a root of $P(x)$ to another root of $P(x)$; further, given automorphisms are bijections, each automorphism can be identified with a permutation of the roots of $P(x)$.

A collection of permutations is a group if it is closed under composition of permutations. Since automorphisms compose, the set of permutations of the roots of a polynomial $P(x)$ that correspond to an automorphism is a group, called the Galois Group of the polynomial $P(x)$, or equivalently the Galois Group $Gal(K(\zeta)/K)$ of the field extension $K(\zeta)/K$, where the cyclotomic extension $K(\zeta)$ is the splitting field of $P(x)$.

For most polynomials $P(x)$, every permutation of the roots induces an automorphism so the Galois Group of $P(x)$ is the set of all permutations of the roots. But for some polynomials, the Galois Group is a strict subset of the permutations of the roots because some permutations do not induce an automorphism. This is the case for cyclotomic polynomials.

Let G be the Galois group of the n-th cyclotomic polynomial, where n is prime. The roots of the polynomial are $\{\zeta, \zeta^2, \ldots, \zeta^{n-1}\}$. Each $\alpha \in G$ maps ζ by $\alpha(\zeta) = \zeta^a$ for some $a \in \{1, \ldots, n-1\}$. Since

$$\alpha(\zeta^k) = \alpha(\zeta)^k = \zeta^{ak},$$

the number a completely determines where all the other roots go. In general, the Galois group of a polynomial can permute the roots arbitrarily, but the Galois group of cyclotomic polynomials only allow permutations of the form

$$(\zeta, \zeta^2, \ldots, \zeta^{n-1}) \mapsto (\zeta^a, \zeta^{2a \bmod n}, \ldots, \zeta^{(n-1)a \bmod n})$$

for all $a \in \{1, \ldots, n-1\}$.

Example 1.2.5. *For $n = 5$, these are the only permutations induced by automorphisms:*

$$\begin{aligned}
&(\zeta^1, \zeta^2, \zeta^3, \zeta^4) \ \text{ for } a = 1\\
&(\zeta^2, \zeta^4, \zeta^1, \zeta^3) \ \text{ for } a = 2\\
&(\zeta^3, \zeta^1, \zeta^4, \zeta^2) \ \text{ for } a = 3\\
&(\zeta^4, \zeta^3, \zeta^2, \zeta^1) \ \text{ for } a = 4
\end{aligned}$$

The above chain of reasoning can be more formally stated in the following theorem, where $(\mathbb{Z}/n\mathbb{Z})^*$ is the multiplicative integer modulo n group.

Theorem 1.2.6. *The mapping*

$$\begin{gathered}
\varphi : Gal(K(\zeta_n)/K) \to (\mathbb{Z}/n\mathbb{Z})^*\\
\varphi(\sigma) = a_\sigma \bmod n
\end{gathered}$$

Injective homomorphism

that is given by $\sigma(\zeta) = \zeta^{a_\sigma}$ for all n-th roots of unity ζ is an injective group homomorphism.

Proof. For any automorphisms $\sigma, \tau \in Gal(K(\zeta_n)/K)$, a primitive root $\zeta_n \in \mu_n$ satisfies $\sigma\tau(\zeta_n) = \sigma(\zeta_n^{a_\tau}) = \zeta_n^{a_\sigma a_\tau}$ by applying the automorphism one after the other. In addition, the two automorphisms gives another automorphism in the Galois group by composition, so $\sigma\tau(\zeta_n) = \zeta_n^{a_{\sigma\tau}}$. Hence, we have $\zeta_n^{a_\sigma a_\tau} = \zeta_n^{a_{\sigma\tau}}$. This implies $a_\sigma a_\tau \equiv a_{\sigma\tau} \bmod n$, because ζ_n has order n. Therefore, we have $\varphi(\sigma\tau) = a_{\sigma\tau} \equiv a_\sigma a_\tau \bmod n = \varphi(\sigma)\varphi(\tau)$ which entails φ is a homomorphism. The injectivity is not difficult to see either. □

We know the group $(\mathbb{Z}/n\mathbb{Z})^*$ is abelian. The map φ embeds the Galois groups of cyclotomic extensions to this abelian group, so the Galois group is also abelian. For a general base field K, the group homomorphism need not be surjective. There are two special cases, $K = \mathbb{Q}$ and $K = \mathbb{F}_p$, for a prime p, that are of most interest for building lattice cryptosystems. We will look at the property of the map φ in each special case one by one.

Isomorphism when $K = \mathbb{Q}$

Theorem 1.2.7. *The Galois group of the cyclotomic extension $\mathbb{Q}(\zeta_n)$ is isomorphic to the multiplicative integer modulo n group. That is,*

$$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*.$$

For each automorphism $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, there is an integer $i \in (\mathbb{Z}/n\mathbb{Z})^*$ such that the automorphism $\sigma \mapsto [i]$ is mapped to the equivalent class of i if and only if $\sigma(\zeta_n) = \zeta_n^i$.

The automorphisms in the Galois group are functions on the roots of unity. We can think of the equivalent class $[i]$ as a function too given by $[i] : \zeta \mapsto \zeta^i$ for all roots $\zeta \in \mu_n$. The theorem says each automorphism in the Galois group is uniquely mapped to an integer in the multiplicative group (or a function). Theorem 1.2.7 is useful for proving the pseudorandomness of the ring LWE distribution as we will see in a later section.

Observe that the order of the Galois group is equal to the degree of the Galois extension over $\mathbb{Q}$, which is equal to the degree $\phi(n)$ of the n-th cyclotomic polynomial. The order of the multiplicative group is equal to the number of integers in $[0, n-1]$ that are coprime with n. The two numbers are obviously equal.

When K is a field with non-zero prime characteristic $char(K) = p$ (e.g., $K = \mathbb{F}_p$), as is often the case in cryptography, the homomorphism φ is not necessarily surjective. Theorem 1.2.8 caters for this case. For our purpose, we are primarily interested in the cyclotomic polynomials $\Phi_d(x)$ where $\gcd(d, p) = 1$.

Image of Galois group when $K = \mathbb{F}_p$

Theorem 1.2.8. *Let $\mathbb{F}_q$ be a finite field with a prime power order q and $\gcd(q, n) = 1$, the Galois group of a cyclotomic extension $\mathbb{F}_q(\zeta_n)$ of the finite field is mapped by the homomorphism φ to the cyclic group $\langle q \bmod n \rangle$ in $(\mathbb{Z}/n\mathbb{Z})^*$. That is,*

$$\varphi(Gal(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q)) = \langle q \bmod n \rangle \subseteq (\mathbb{Z}/n\mathbb{Z})^*.$$

In particular, the dimension of the cyclotomic extension is the order of q modulo n.

To prove Theorem 1.2.8, we need this next result.

Power map

Theorem 1.2.9. *For a prime p and prime power $q = p^n$, the pth power map $\varphi_p : x \mapsto x^p$ on $\mathbb{F}_q$ generates the Galois group $Gal(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q)$.*

Proof. (of Theorem 1.2.8 for the special case when $q = p$ for a prime p) Theorem 1.2.9 implies that the Galois group $Gal(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q)$ is generated by the pth power map $\varphi_p : x \mapsto x^p$ for all $x \in \mathbb{F}_q(\zeta_n)$. In addition, by Theorem 1.2.6 the group homomorphism φ associates to φ_p an non-negative integer $a \bmod n$ such that $\varphi_p(\zeta) = \zeta^a$ for all nth roots of unity $\zeta \in \mu_n$. This entails $\zeta^p = \zeta^a$, which is true if $a \equiv p \bmod n$. Hence, the homomorphism φ maps the pth power map φ_p in the Galois group to $p \bmod n$ in the group $(\mathbb{Z}/n\mathbb{Z})^*$. Since $Gal(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q) = \langle \varphi_p \rangle$, its image is the cyclic group $\langle p \bmod n \rangle \in (\mathbb{Z}/n\mathbb{Z})^*$.

The assumption $char(\mathbb{F}_q) = p$ implies the polynomial $x^n - 1$ is separable in $\mathbb{F}_q[x]$, so $\mathbb{F}_q(\zeta_n)$ is an Galois extension given that it is also the splitting field of $x^n - 1$. Hence, we have $[\mathbb{F}_q(\zeta_n) : \mathbb{F}_q] = |Gal(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q)| = |\langle p \bmod n \rangle|$, which is the order of p modulo n. □

Knowing cyclotomic polynomials are irreducible over $\mathbb{Q}$, we would like to know whether they are also irreducible in a finite field $\mathbb{F}_q$ of prime power order q. This brings out the following theorem and corollary. Denote $\bar{\Phi}_n(x)$ as reducing the coefficients of $\Phi_n(x)$ modulo q.

Factor $\Phi_n(x)$ in F_p

Theorem 1.2.10. *Let q be prime power and $\gcd(q, n) = 1$, the monic irreducible factors of the polynomial $\bar{\Phi}_n(x) \in \mathbb{F}_p[x]$ are distinct and each has a degree equal to the order of q modulo n.*

Corollary 1.2.11. *The polynomial $\bar{\Phi}_n(x)$ is irreducible in $\mathbb{F}_q[x]$ if $\gcd(q, n) = 1$ and $\langle q \bmod n \rangle = (\mathbb{Z}/n\mathbb{Z})^*$. That is, $q \bmod n$ is a generator of the group $(\mathbb{Z}/n\mathbb{Z})^*$.*

Example 1.2.12. *For $n = 5$, the polynomial*

$$\bar{\Phi}_5(x) = x^4 + x^3 + x^2 + x + 1$$

can be factored in $\mathbb{F}_{11}$ as

$$(x - 3)(x - 4)(x - 5)(x - 9)$$

because the order of 11 modulo 5 is 1. Similarly, it can be factored in $\mathbb{F}_{19}$ *as*

$$(x^2 + 5x + 1)(x^2 + 15x + 1)$$

because the order of 19 modulo 5 is 2. Similarly, it can be factored in $\mathbb{F}_3$ *as*

$$x^4 + x^3 + x^2 + x + 1$$

because the order of 3 modulo 5 is 4. The last case is an example of the corollary where the cyclic group $\langle 3 \bmod 5\rangle$ *is a generator of the group* $(\mathbb{Z}/5\mathbb{Z})^*$.