Cyclotomic Fields

Sylvan Martin

Goal & Outline

Broadly, the goal of this project is to explore cyclotomic polynomials and try to show how one might naturally come accross them. We will prove the irreducibility of the cyclotomic polynomial, while seeing some neat and useful math along the way, like Gauss's Lemma and Eisenstein's Criterion for Irreducibility.

References

The following is a list of references I'll be using to study this topic.

- "Abstract Algebra," by Dummit and Foote
- "Cyclotomic Fields with Applications," by G. Eric Morehouse
  - `https://ericmoorhouse.org/handouts/cyclotomic_fields.pdf`
- "Minimal Polynomials," by James M. Belk (from Cornell!)
  - `https://e.math.cornell.edu/people/belk/numbertheory/MinimalPolynomials.pdf`

Prerequisites

Truthfully, I intend on trying to explain everything in this project so that anyone with the knowledge of MATH 4340 can understand it without any other prerequisite knowledge. The main math used here is adjoining abstract roots, and polynomial rings, which is comfortably within the MATH 4340 skillset.

Mentions of Relevant Material

In this report, I reference several concepts from lecture, here are some of those:

- Cyclic groups, and their isomorphism with the additive group $\mathbb{Z}/n\mathbb{Z}$
- Reducibility of polynomials
- Ideals, specifically the fact that if P is a prime ideal of R, then R/P is an integral domain.

Introduction

Recall that any cyclic group of order n is isomorphic to the additive cyclic group $\mathbb{Z}/n\mathbb{Z}$. Similarly, it is also isomorphic to the multiplicative cyclic group of the n-th roots of unity, the complex roots of $x^n - 1 = 0$. This is the group

$$\{z \in \mathbb{C} \mid z^n = 1\} = \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\} = \langle \zeta \rangle$$

where ζ_n is the n-th root of unity in $\mathbb{C}$, often written as

$$\zeta_n = e^{2i\pi/n}$$

and we write μ_n to denote the cyclic group of n-th roots of unity, $\mu_n = \langle \zeta_n \rangle$. Note that the only elements in μ_n with order n are those ζ_n^k where k and n are coprime. This is because if k and n are not coprime, then ζ_n^k has order $n/\gcd(k, n) < n$. Importantly, this means that the only *primitive* roots of unity (those of strictly order n) are those where k and n are coprime. Euler's totient function $\phi(n)$ is used to denote the number of integers k less than n such that k and n are coprime. So, there are $\phi(n)$ primitive n-th roots of unity. Geometrically, these roots are vectors spaced evenly about the unit circle, and so their sum is zero.

$$1 + \zeta_n + \zeta_n^2 + \cdots + \zeta_n^{n-1} = 0$$

Now, let's consider polynomials with roots of unity. The above identity tells us that ζ is a root of

$$1 + t + t^2 + \cdots + t^{n-1}$$

with this polynomial being of degree $n - 1$. We also have the neat identity

$$X^n - 1 = (X - 1)(X - \zeta_n)(X - \zeta_n^2) \cdots (X - \zeta_n^{n-1})$$

However, there are more interesting polynomials to be seen here!

Definition-Lemma:[1] Say that F is a field, and for some $\alpha \in F$, there is a nonzero polynomial $f \in F[X]$ such that $f(\alpha) = 0$. (In other words, α is algebraic in F.) We define the ***minimal polynomial*** of α to be the monic polynomial of minimal degree with α as a root.

An important property of such minimal polynomials is that they are irreducible. Why is this? Say that $f \in F[X]$ is the minimal polynomial of α, but it is not irreducible. That is, there are $g, h \in F[X]$, both non-constant, such that $f = gh$. If α is a root of f, then it must be a root of g or of h. However, g and h have degrees less than f, so f could not have been minimal.

So, a natural question is what is the minimal polynomial of ζ? This is the driving question of this project.

1. I am marking this as a lemma, because it is not obvious to me that this minimal polynomial is unique.

Cyclotomic Polynomials

Let us construct a polynomial with roots at the *primitive* n-th roots of unity. Recall that ζ_n^k is a primitive n-th root of unity only if n is coprime to k. So, the natural definiton follows.

Definition The ***n-th cyclotomic polynomial*** is the monic polynomial

$$\Phi_n(X) = \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} \left(X - \zeta_n^k\right)$$

Now whenever we see a gcd hanging around, it's always begging us to consider the case when n is prime, which is

$$\Phi_n(X) = (X - \zeta_n)(X - \zeta_n^2) \cdots (X - \zeta_n^{n-1})$$

Another neat fact about the n-th cyclotomic polynomial is that its degree is $\phi(n)$, where ϕ is again Euler's totient function. This is because it is the product of $\phi(n)$ linear polynomials.

In the previous section, we noted that we can factor $X^n - 1$ as

$$X^n - 1 = (X - 1)(X - \zeta_n)(X - \zeta_n^2) \cdots (X - \zeta_n^{n-1})$$

Where ζ_n is an n-th root of unity, though *not* necessarily a primitive root! We can separate out the roots that *are* primitive by writing

$$X^n - 1 = \prod_{d|n} \prod_{\substack{\zeta_d \in \mu_d \\ \zeta_d \text{ primitive}}} (X - \zeta_d)$$

Since the inner product is Φ_d by definition, that means

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

Using this factorization, we can compute Φ_n for any n. If we know all $\Phi_1(X), \ldots, \Phi_{n-1}(X)$, we can find

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{\substack{d|n \\ d \neq n}} \Phi_d(X)}$$

At the end of this document, I've written a little Sage program that will compute the n-th cyclotomic polynomial. It's quite simple (since Sage implements all the important stuff) but it's a fun thing to write.

Irreducibility of Cyclotomic Polynoials

Eventually, we will prove that the n-th cyclotomic polynomial is the minimal polynomial of ζ_n, but first we will focus on the "easy" case where n is prime. But before we do *that*, we will need *Abel's Irreducibility Theorem* and *Eisenstein's Criterion*.

Theorem: *(Abel's Irreducibility Theorem)* Let F be a field and $K \supseteq F$ be an extension. Let $f \in F[X]$ be a polynomial with a root $\alpha \in K$. Let $g \in F[X]$ be irreducible over F also with the root α. Then, every root of g is also a root of f. (Equivalently, g divides f.)

This gives us a useful corollary, which is that the minimal polynomial of a root α divides every polynomial which has α as a root. To see this, let $g \in F[X]$ be the minimal polynomial of α. As we saw before, g must be irreducible. By the above theorem, if some $f \in F[X]$ has a root α, Then g divides f.

Possibly more important is that if g is irreducible with root α, then it is the minimal polynomial of α. If it weren't the minimal polynomial of α, then it couldn't be irreducible, since it would be divisible by the minimal polynomial of α. So, all we need to prove that Φ_n is the minimal polynomial of ζ_n is that Φ_n is irreducible. (We already know it has a root at ζ_n by construction!)

Let's prove the prime case. We will show that Φ_p (where p is prime) is irreducible, and is therefore the minimal polynomial of the p-th root of unity ζ_p. We will use Eisenstein's Criterion for Irreducibility.

Theorem: *(Eisenstein's Criterion for Irreducibility)* Let P be a prime ideal of the integral domain R, and let

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$$

be a monic polynomial in $R[X]$, with all $a_i \in P$, and $a_0 \notin P^2$ (where P^2 is the set of all products of elements of P). Then, f is irreducible in $R[X]$.

Proof.[2] First, let's introduce some notation. Take $p \in R[X]$. We'll denote $\overline{p} \in (R/P)[X]$ to be the polynomial with the coefficients of p reduced modulo P. Specifically, if

$$p(X) = \sum a_i X^i \in R[X]$$

then

$$\overline{p(X)} := \sum (a_i + P) X^i \in (R/P)[X]$$

Now let's get on with the proof. We will proceed by contradiction. Suppose that f were reducible. So, we can write

$$f = ab$$

for $a, b \in R[X]$ being nonconstant polynomials. Consider reducing f modulo P. Because all coefficients of f are in P (except the first, because 1 cannot be in a prime ideal!) We get

$$\overline{f} = \overline{ab} = X^n$$

Since P is a prime ideal, R/P is an integral domain. Because $\overline{ab}$ then has coefficients in an integral domain, and the "constant" term in the polynomial X^n is zero, that means that the constant term in $\overline{ab}$ is zero, which in turn means that the constant terms in both $\overline{a}$ and

2. From Dummit & Foote, pg. 310

$\overline{b}$ must be zero (if one of them weren't zero, we would see a term with degree less than n appear in their product.) However, the fact that $\overline{a}$ has constant term 0 and $\overline{b}$ has constant term zero means that the constant terms in a and in b must both be in P, which violates the assumption that $a_0 \notin P^2$, since a_0 would be the product of the constant terms in a and b. So, we can conclude that f must be irreducible. □

We will now use the Eisenstein Criterion to show that the p-th cyclotomic polynomial is irreducible for prime p.

Lemma: The p-th cyclotomic polynomial is irreducible for prime p.

Proof. Recall from before that

$$X^p - 1 = (X-1)(X-\zeta_p)\cdots(X-\zeta_p^{n-1})$$

Which gives us

$$\Phi_p(X) = \frac{X^p-1}{X-1} = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Z}[X]$$

We cannot immediately apply Eisenstein's criterion, because the coefficients in this polynomial are all 1, which cannot be in any sort of prime ideal. However, we can instead look at

$$\Phi_p(X+1) = \frac{(X+1)^p-1}{X} = X^{p-1} + pX^{p-2} + \cdots + \frac{p(p-1)}{2}X + p \in \mathbb{Z}[X]$$

This polynomial meets exactly the format for Eisenstein's criterion, as the leading coefficient is 1, and the constant coefficient p clearly is not a multiple of p^2, and all other coefficients are in the prime ideal $p\mathbb{Z}$. (They're all integer multiples of p!) So, we know that $\Phi_p(X+1)$ is irreducible in $\mathbb{Z}[X]$. Why must this imply that $\Phi_p(X)$ is irreducible? Well, imagine for a moment that $\Phi_p(X)$ were reducible. Then, we would have some non-constant g and h such that

$$\Phi_p(X) = g(X)h(X)$$

and then

$$\Phi_p(X+1) = g(X+1)h(X+1)$$

which would imply that $\Phi_p(X+1)$ is reducible, which we just proved cannot be the case. So, we can conclude that Φ_p is irreducible. □

This is a useful fact, but of course we wish that the n-th cyclotomic polynomial is irreducible in general. We are now embarking on a quest to prove the irreducibility of Φ_n, but on the way we will need some new definitions and lemmas.

Cyclotomic Fields

Definition: The field $\mathbb{Q}(\zeta_n)$ is called the ***cyclotomic field of n-th roots of unity.***

Let's unpack this definition a bit. We are adjoining the root of Φ_n to $\mathbb{Q}$, giving us

$$\mathbb{Q}(\zeta_n) := {}^{\mathbb{Q}[X]}\!/_{(\Phi_n)}$$

Recall that Φ_n is irreducible, so (Φ_n) is maximal, which means that $\mathbb{Q}(\zeta_n)$ is a field as we would expect. Some properties about $\mathbb{Q}(\zeta_n)$ are immediate. (These are from **Lemma 15** from lecture.)

1. Φ_n has a root in $\mathbb{Q}[X]/(\Phi_n)$.
2. $[{}^{\mathbb{Q}[X]}\!/_{(\Phi_n)} : \mathbb{Q}] = \deg(\Phi_n) = \phi(n)$

Lemma: *(Gauss's Lemma)* Let $f(X) \in \mathbb{Z}[X]$. If f is reducible in $\mathbb{Q}[X]$, then f is reducible in $\mathbb{Z}[X]$.

Another way of viewing what this lemma is saying is that if we have some nonconstant $p(X), q(X) \in \mathbb{Q}[X]$ such that

$$f(X) = p(X)q(X)$$

then p and q have associates[3] $p', q' \in \mathbb{Z}[X]$ such that $f(X) = p'(X)q'(X)$.

In the more general version of Gauss's Lemma, we look at fields of fractions of UFDs instead of just integers inside the rationals. But for our purposes, we only need to look at $\mathbb{Z}[X] \subset \mathbb{Q}[X]$.

Proof. Say we have the rational factorization $f(X) = A(X)B(X)$, with $A, B \in \mathbb{Q}[X]$, and[4]

$$A(X) = A_0 + A_1X + \cdots + A_kX^k, \quad B(X) = B_0 + B_1 + \cdots + B_kX^k$$

Since each $A_i, B_i \in \mathbb{Q}$, then if A_i' is the denominator of A_i, (likewise for B_i'), we can multiply everything by

$$d = \text{lcm}(A_1', B_1', \ldots A_k', B_k')$$

and we get

$$df(X) = a(X)b(X)$$

where $a, b \in \mathbb{Z}[X]$. Now, if d is a unit (just ± 1 since we're in $\mathbb{Z}$) we are done, since we can divide by d and have factored f into two nonconstant integer polynomials. So, assume d is not a unit. Also, assume d is positive for simplicity. (If it's negative, we just divide by -1 on both sides at the end.)

Now, consider the prime factorization of $d = p_1p_2 \cdots p_n$, where $p_i \in \mathbb{Z}$ is a prime that can be repeated throughout the product. Since p_1 is prime, $(p_1) \subset \mathbb{Z}$ is a prime ideal, so $(\mathbb{Z}/(p_1))[X]$ is an integral domain. We can look the reduction map $\mathbb{Z}[X] \to (\mathbb{Z}/(p_1))[X]$ which consists

3. That is, there exist $r, s \in \mathbb{Q}$ (the units of $\mathbb{Q}[X]$) such that $p' = rp$ and $q' = sq$

4. A and B may be of different degree, but I'm just writing k coefficients for simplicity. We could have any of the coefficients be zero.

of just reducing each coefficient of a polynomial modulo p_1. If we reduce both sides of $df(X) = a(X)b(X)$, we get

$$df(X) + (p_1) = (a(X) + (p_1))(b(X) + (p_1))$$

Now, since $p_1 \mid d$, we know $d \in (p_1)$, and so $df(X) + (p_1) = 0$. Since $(\mathbb{Z}/(p_1))[X]$ is an integeral domain, we know that one of $a(X) + (p_1)$ or $b(X) + (p_1)$ is also zero. Assume WLOG that $a(X) + (p_1) = 0$, or that $a(X) \in (p_1)$. This means that all coefficients in $a(X)$ are divisible by p_1, which means we divide both sides by p_1 and still end up with polynomials in $\mathbb{Z}[X]$ on both sides.

$$\begin{aligned} df(X) &= a(X)b(X) \\ p_1 p_2 \cdots p_n f(X) &= a(X)b(X) \\ p_2 \cdots p_n f(X) &= \left(\frac{1}{p_1} a(X)\right) b(X) \end{aligned}$$

Now, we can repeat this process for all remaining $p_2, \ldots, p_n$, each time being able to divide either $a(X)$ or $b(X)$ and still remain inside $\mathbb{Z}[X]$. So, there will exist $a'(X), b'(X) \in \mathbb{Z}[X]$ so that

$$f(X) = a'(X)b'(X)$$

□

Corollary: Let $f(X) \in \mathbb{Z}[X]$ be monic, and factor into $f(X) = g(X)h(X)$ with $g, h \in \mathbb{Q}[X]$. Then, if g and h are monic, then $g, h \in \mathbb{Z}[X]$.

Proof. Gauss's Lemma tells us that there must exist nonzero $r, s \in \mathbb{Q}$ such that $rg(X), sh(X) \in \mathbb{Z}[X]$. So,

$$f(X) = rsg(X)h(X)$$

Now, the leading coefficient of $g(X)h(X)$ must be 1, as is the leading coefficient of $f(X)$. So, we'll have $1 = rs \cdot 1$, and so both $r, s = 1$, which means $g, h \in \mathbb{Z}[X]$ all along. □

This has an awesome application! We can use this to show that $\Phi_n(X)$ must have integer coordinates.

Lemma: $\Phi_n(X) \in \mathbb{Z}[X]$ and is monic.

Proof.[5] We will induct on n. The base cases are given in the introductory section, and those clearly have integer coordinates and are monic. Assume that for all $1 \leq d < n$, $\Phi_d(X) \in \mathbb{Z}[X]$. As we showed in the introduction,

$$X^n - 1 = f(X)\Phi_n(X)$$

Where $f(X) = \prod_{\substack{d \mid n \\ d<n}} \Phi_d(X) \in \mathbb{Z}[X]$ by our inductive hypothesis. Since $\zeta_d \in \mathbb{Q}(\zeta_n)$ is a root of both $X^n - 1$ and $f(X)$, $f(X)$ must divide $X^n - 1$ in the ring $\mathbb{Q}(\zeta_n)[X]$. However, since

5. From Dummit & Foote, pg. 554

both $X^n - 1$ and $f(X)$ have coefficients in $\mathbb{Q}$, $f(X)$ must divide $X^n - 1$ in $\mathbb{Q}[X]$. By the corollary to Gauss's Lemma above, since $X^n - 1$ is monic and are $f(X)$ and $\Phi_n(X)$, we will have that $\Phi_n(X) \in \mathbb{Z}[X]$. □

Fun Observation:[6] Take p^n to be any prime power. Then, the p^n-th cyclotomic polynomial $\Phi_{p^n}(X)$ will have exactly p terms, with the degrees of all the terms summing to $p^n(n-1)/2$.

For example, if we look at 2^n-th cyclotomic polynomials, we see

$$\Phi_{2^6}(X) = X^{32} + 1, \quad \Phi_{2^8} = X^{128} + 1$$

And if we look at 3^n-th cyclotomic polynomials...

$$\Phi_{3^3}(X) = X^{18} + X^9 + 1, \quad \Phi_{3^8}(X) = X^{4374} + X^{2187} + 1$$

$2^6 = 64$, and the degrees in $\Phi_{2^6}(X)$ sum to 2^{6-1}, likewise with 2^8. If we look at $\Phi_{7^3}(X)$, we get

$$\Phi_{7^3}(X) = X^{294} + X^{245} + X^{196} + X^{147} + X^{98} + X^{49} + 1$$

The sum of the degrees of these terms is $3 \cdot 7^3$. Similarly, the degree-sum of $\Phi_{7^2}(X)$ is $3 \cdot 7^2$, and the degree-sum of $\Phi_{7^7}(X) = 3 \cdot 7^7$.

In my revised report I had noticed this pattern with no real explanation. (If you're curious, you can re-create this pattern with the Sage program I provide at the end!) Though now, I believe I have an explanation. The trick here is realizing this interesting identity.

$$\Phi_{p^n}(X) = \Phi_p(X^{p^{n-1}})$$

Let's convince ourselves this is true. The roots of the polynomial $\Phi_p(X^{p^{n-1}})$ are precisely the values so that when raised to the power p^{n-1} they are a p-th root of unity. In otherwords, ω is a such a root if

$$(\omega^{p^{n-1}})^p = \omega^{p \cdot p^{n-1}} = \omega^{p^n} = 1$$

Hey look! These are just the p^n-th roots of unity, which means they are also precisely the roots of $\Phi_{p^n}(X)$. Since the roots of $\Phi_{p^n}(X)$ are also the roots of $\Phi_p(X^{p^{n-1}})$, $\Phi_{p^n}(X)$ divides $\Phi_p(X^{p^{n-1}})$ in $\mathbb{Z}[X]$ since $\Phi_{p^n}(X)$ is irreducible. Now, let's look at the degrees of these polynomials. Above, we know that $\deg(\Phi_{p^n}(X)) = \phi(p^n) = p^n - p^{n-1}$, since everything except for multiples of p are coprime to p^n. Also, $\deg(\Phi_p(X^{p^{n-1}}))$ is just $\phi(p) \cdot (p^{n-1})$

$$\begin{aligned} deg(\Phi_p(X^{p^{n-1}})) &= \phi(p) \cdot (p^{n-1}) \\ &= (p-1)(p^{n-1}) \\ &= p^n - p^{n-1} \end{aligned}$$

So, these polynomials have the same degree, and therefore must be equal.[7]

6. I haven't actually seen this specific observation in any literature, but I'm sure it's already known.

7. Technically they could differ by a scalar, but both of these polynomials are monic, so that scalar would just be 1.

Now, the "neat observation" becomes a bit more obvious. We can just list out the terms of $\Phi_{p^n}(X)$ by listing out the terms of $\Phi_p(X^{p^{n-1}})$, which is just

$$\Phi_p(X^{p^{n-1}}) = (X^{p^{n-1}})^{p-1} + (X^{p^{n-1}})^{p-2} + \cdots + X^{p^{n-1}} + 1$$

This already gives us the first part of the neat observation. There will clearly be exactly p terms in this polynomial. As for the sum of the degrees of each term, we can use Gauss's Summation formula.

$$\sum_{k=0}^{p-1} p^{n-1} \cdot k = p^{n-1} \sum_{k=0}^{p-1} k = p^{n-1} \frac{p(p-1)}{2} = p^n(n-1)/2$$

Attachments

Program for Computing Cyclotomic Polynomials

If you have the Sage computer algebra library, (which is awesome!) you can try running this code to compute different cyclotomic polynomials!

```
Phi_1(X) = X - 1
Phi_2(X) = X + 1

def cyclotomic_poly(n): # Computes the n-th cyclotomic polynomial
    if n == 1:
        return Phi_1
    elif n == 2:
        return Phi_2
    else:
        # compute product of previous ones!
        prod = Phi_1
        for d in range(2, n):
    if n % d == 0:
                prod *= cyclotomic_poly(d)
        return ((X^n - 1)/prod).full_simplify()
```

Example Outputs

n	n-th cyclotomic polynomial
3	$X^2 + X + 1$
50	$X^{20} - X^{15} + X^{10} - X^5 + 1$
2^{16}	$X^{32768} + 1$