MA542 Lecture

Timothy Kohl

Boston University

April 23, 2025

Cyclotomic Extensions

We've discussed the *cyclotomic polynomials*

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1$$

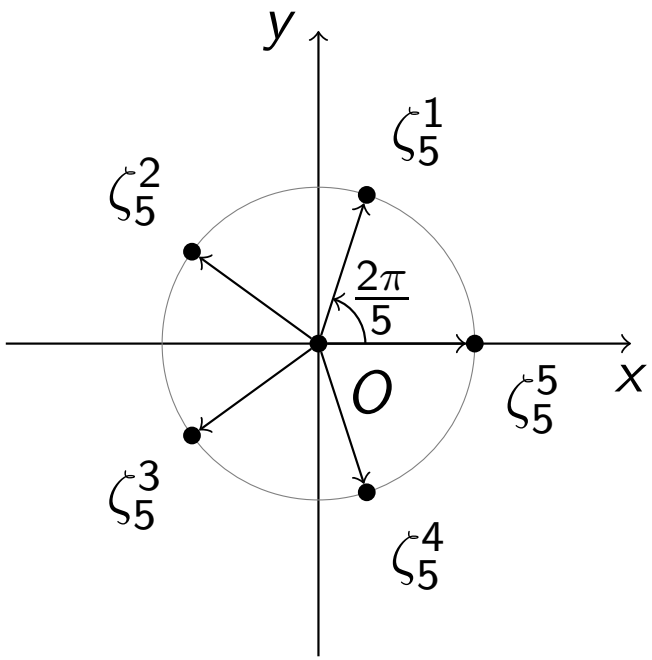
and that the roots are p^{th} roots of unity ζ_p^i where

$$\zeta_p = e^{\frac{2\pi i}{p}} = cos(\frac{2\pi}{p}) + isin(\frac{2\pi}{p})$$

which are distributed equidistantly around the unit circle, dividing it up into equal size arcs.

And this is the origin of the term 'cyclotomy' which is the act of subdividing a circle in such a fashion.

For example, if $p = 5$ we have 5 roots of unity distributed around the circle at multiples of $2\pi/5$ (72 degrees).



And for integers n which are not prime necessarily, we can still define the basic n^{th} root of unity $\zeta_n = e^{\frac{2\pi i}{n}}$ where ζ_n^t for t from 0 to $n-1$ are distributed around the unit circle and are the roots of $x^n - 1$.

In somewhat greater generality, we can define the so-called *circle group*

$$T = \{e^{i\theta} \mid 0 \leq \theta < 2\pi\}$$

where $e^{i\theta} = cos(\theta) + isin(\theta)$ also lie on the unit circle, and indeed T *is* the unit circle since every solution (x, y) of $x^2 + y^2 = 1$ has the form $x = cos(\theta)$ and $y = sin(\theta)$ for $\theta \in [0, 2\pi)$.

What's of greater interest is the fact that T **is** a group under multiplication since

$$e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1 + \theta_2)}$$

where, the sum $(\theta_1 + \theta_2)$ of elements of $[0, 2\pi)$ are added *mod* 2π, which is readily seen to be closed and associative, and where $e^0 = 1$ is the identity and the inverse of $e^{i\theta}$ is $e^{-i\theta}$.

The group T is, of course, uncountably infinite but it is of interest since for every n, the group T contains a cyclic subgroup of order n, namely $\left\langle e^{i\frac{2\pi}{n}} \right\rangle$ and the fact that it is of order n is that

$$(e^{i\frac{2\pi}{n}})^k = e^{ik\frac{2\pi}{n}}$$

which means that $\left|e^{i\frac{2\pi}{n}}\right| = n$ since $k = n$ is the smallest value which makes $\frac{k2\pi}{n}$ an even multiple of 2π.

It's also interesting to note that $\left\langle e^{i\theta} \right\rangle$ is infinite cyclic exactly when θ is an irrational multiple of 2π.

Recall from basic group theory that if $\langle \sigma \rangle$ is a cyclic group of order n that $|\sigma^k| = \frac{n}{gcd(n,k)}$ so that $|\sigma^k| = n$ if and only if $gcd(k, n) = 1$.

That is $k \in U(n)$ the group of units mod n, and since $|U(n)| = \phi(n)$ where ϕ is the Euler ϕ-function we have that $\langle \sigma \rangle$ has $\phi(n)$ generators.

Definition

For $\langle \zeta_n \rangle$ where $\zeta_n = e^{i\frac{2\pi}{n}}$ we call such a generator ζ_n^k (for $k \in U(n)$) a primitive n^{th} root of unity.

The importance of the definition of primitive n^{th} roots of unity lies in how it's used to define cyclotomic polynomials in general.

Definition

For $n \geq 1$ an integer, the n^{th} cyclotomic polynomial is

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

which is of degree $|U(n)| = \phi(n)$.

We note, that for $n = p$ (prime) we have that $U(p) = \{1, \ldots, p-1\}$ which yields

$$\Phi_p(x) = (x - \zeta_p)(x - \zeta_p^2) \cdots (x - \zeta_p^{p-1}) = x^{p-1} + \cdots + x + 1$$

which is our original set of examples.

So what if n isn't prime?

- $\zeta_1 = e^{\frac{2i\pi}{1}} = 1$ so $\Phi_1(x) = (x-1)$
- $\zeta_2 = e^{\frac{2i\pi}{2}} = e^{i\pi} = -1$, $U(2) = \{1\}$ so $\Phi_2(x) = (x+1)$
- $\Phi_3(x) = x^2 + x + 1$
- $\zeta_4 = e^{\frac{2i\pi}{4}} = e^{\frac{i\pi}{2}} = i$, $U(4) = \{1, 3\}$ so $\Phi_4(x) = (x-i)(x+i) = x^2 + 1$
- $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$
- $\zeta_6 = e^{\frac{i\pi}{3}} = \frac{1+\sqrt{-3}}{2}$, $U(6) = \{1, 5\}$ where $\zeta_6^5 = \frac{1-\sqrt{-3}}{2}$ so $\Phi_6(x) = x^2 - x + 1$ (Exercise!)

So from the example $\Phi_p(x) = \frac{x^p-1}{x-1}$ and the fact that the roots of $x^n - 1$ are exactly $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$ it's clear that $\Phi_n(x) \mid x^n - 1$ but, in fact, we can say more.

Observe, for example, that given $\zeta_{12} = e^{\frac{i2\pi}{12}}$, the primitive 12-th roots of unity are $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$ and the remaining 12-th roots of unity are

$$1, \zeta_{12}^2, \zeta_{12}^3, \zeta_{12}^4, \zeta_{12}^6, \zeta_{12}^8, \zeta_{12}^9, \zeta_{12}^{10}$$

and we notice some interesting facts about these *non*-primitive roots.

- $\zeta_{12}^2 = e^{\frac{i2\pi}{6}} = \zeta_6$
- $\zeta_{12}^3 = e^{\frac{i2\pi}{4}} = \zeta_4 = i$
- $\zeta_{12}^4 = e^{\frac{i2\pi}{3}} = \zeta_3$
- $\zeta_{12}^6 = e^{\frac{i2\pi}{2}} = \zeta_2 = -1$
- $\zeta_{12}^8 = \zeta_3^2$
- $\zeta_{12}^9 = \zeta_4^3 = -i$
- $\zeta_{12}^{10} = \zeta_6^5$

This leads to a rather interesting observation when one factors $x^{12} - 1$.

$$x^{12}-1=$$
$$(x-1)(x-\zeta_{12})(x-\zeta_{12}^2)(x-\zeta_{12}^3)(x-\zeta_{12}^4)(x-\zeta_{12}^5)(x-\zeta_{12}^6)(x-\zeta_{12}^7)(x-\zeta_{12}^8)(x-\zeta_{12}^9)(x-\zeta_{12}^{10})(x-\zeta_{12}^{11})$$
$$=$$
$$\underbrace{(x-1)}_{\Phi_1(x)}\underbrace{(x-\zeta_{12})(x-\zeta_{12}^5)(x-\zeta_{12}^7)(x-\zeta_{12}^{11})}_{\Phi_{12}(x)}\underbrace{(x-\zeta_{12}^2)(x-\zeta_{12}^{10})}_{\Phi_6(x)}\underbrace{(x-\zeta_{12}^3)(x-\zeta_{12}^9)}_{\Phi_4(x)}\underbrace{(x-\zeta_{12}^4)(x-\zeta_{12}^8)}_{\Phi_3(x)}\underbrace{(x-\zeta_{12}^6)}_{\Phi_2(x)}$$

That is

$$x^{12}-1=\Phi_1(x)\cdot\Phi_2(x)\cdot\Phi_3(x)\cdot\Phi_4(x)\cdot\Phi_6(x)\cdot\Phi_{12}(x)$$

and the significance of the numbers $1,2,3,4,6,12$ is that these are all the divisors of $n=12$.

Moreover,

$$\begin{aligned}12=deg(x^{12}-1)&=deg(\Phi_1(x))+deg(\Phi_2(x))+deg(\Phi_3(x))+deg(\Phi_4(x))+deg(\Phi_6(x))+deg(\Phi_{12}(x))\\&=\phi(1)+\phi(2)+\phi(3)+\phi(4)+\phi(6)+\phi(12)\end{aligned}$$

which is not a coincidence.

Theorem

For $n \geq 1$, a positive integer

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

where $d \mid n$ means all the positive divisors of n.

Proof.

First, observe that any d^{th} root of unity (for $d \mid n$) is a power of *exactly one* n^{th} root of unity.

This implies that $\Phi_d(x)$ has distinct linear factors from $\Phi_{d'}(x)$ for d' some other divisor of n, i.e.

$$gcd(\Phi_d(x), \Phi_{d'}(x)) = 1 \text{ for } d \neq d'$$

Lastly, the roots of $x^n - 1$ are exactly all the n distinct powers $1, \zeta_n, \ldots, \zeta_n^{n-1}$ which, by the above observation, are roots of distinct $\Phi_d(x)$ i.e. both polynomials have the same roots and since both are monic, they must be identical. □

As a bonus, we get the following nice formula:

$$n = \sum_{d|n} \phi(d)$$

which can be viewed as follows. If we let $U(1) = \{0\}$ then for each $d \mid n$ we have $\frac{n}{d} U(d) = \{\frac{n}{d} u \mid u \in U(d)\}$ and we have that

$$\mathbb{Z}_n = \bigcup_{d|n} \frac{n}{d} U(d)$$

and so $|\mathbb{Z}_n| = \sum_{d|n} |\frac{n}{d} U(d)| = \sum_{d|n} |U(d)| = \sum_{d|n} \phi(d)$.

For example, with $n = 12$ we have

$$\begin{aligned} U(1) = \{0\} &\implies 12U(1) = \{0\} \\ U(2) = \{1\} &\implies 6U(2) = \{6\} \\ U(3) = \{1, 2\} &\implies 4U(2) = \{4, 8\} \\ U(4) = \{1, 3\} &\implies 3U(4) = \{3, 9\} \\ U(6) = \{1, 5\} &\implies 2U(6) = \{2, 10\} \\ U(12) = \{1, 5, 7, 11\} &\implies 1U(12) = \{1, 5, 7, 11\} \end{aligned}$$

where one can see that the union of all these is $\mathbb{Z}_{12}$.

And we know that $\Phi_p(x) = x^{p-1} + \cdots + x + 1 \in \mathbb{Z}[x]$, but what about $\Phi_n(x)$ for composite n?

Theorem

$\Phi_n(x) \in \mathbb{Z}[x]$ for each $n \geq 1$.

PROOF: The proof is by induction on n. Consider first the fact that $\Phi_1(x) = x - 1$ which is obviously in $\mathbb{Z}[x]$.
For $n > 1$ we have $x^n - 1 = \prod_{d|n} \Phi_d(x)$ which includes the factor for $d = n$ so that

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

where

$$f(x) = \prod_{d|n \text{ and } d<n} \Phi_d(x)$$

where inductively we can assume $\Phi_d(x) \in \mathbb{Z}[x]$ which implies $f(x) \in \mathbb{Z}[x]$ and is monic, since each $\Phi_d(x)$ is monic.

PROOF (continued): So we have that $x^n - 1 = \Phi_n(x)f(x)$ where $x^n - 1$, $\Phi_n(x)$ and $f(x)$ (being a product of monic polynomials) is monic, and $x^n - 1, f(x) \in \mathbb{Z}[x]$, so why is $\Phi_n(x) \in \mathbb{Z}[x]$?

This is actually an easy exercise in polynomial multiplication.

If we have $x^n - 1 = (\sum_{i=0}^{p} a_i x^i)(\sum_{j=0}^{q} b_j x^j)$ where $a_i \in \mathbb{Z}$ and $a_q = b_p = 1$ then the degree $n - 1 = p + q - 1$ coefficient of $x^n - 1$ is 0 so

$$a_{p-1}b_q + a_p b_{q-1} = 0$$
$$\downarrow$$
$$a_{p-1} + b_{q-1} = 0$$
$$\downarrow$$
$$b_{q-1} = -a_{p-1} \in \mathbb{Z}$$

PROOF (continued)

And similarly the degree $n-2 = p+q-2$ coefficient is 0 and so

$$\begin{aligned} a_p b_{q-2} + a_{p-1} b_{q-1} + a_{p-2} b_q &= 0 \\ &\downarrow \\ b_{q-2} + a_{p-1} b_{q-1} + a_{p-2} &= 0 \\ &\downarrow \\ b_{q-2} &= -a_{p-1} b_{q-1} - a_{p-2} \in \mathbb{Z} \end{aligned}$$

and continuing this way we deduce that all the coefficients b_j are integers, so $\Phi_n(x) \in \mathbb{Z}[x]$. □

We saw earlier that for each prime p the p-th cyclotomic polynomial $\Phi_p(x)$ is irreducible. In general we have.

Theorem

For each $n \geq 1$, $\Phi_n(x)$ is irreducible (over $\mathbb{Z}$) and therefore over $\mathbb{Q}$ too.

Before we prove this, we need a small technical fact.

Lemma

Let $n > 1$ be an integer and let $p \nmid n$ be prime. Then $\overline{\Phi_n(x)} \in \mathbb{Z}_p[x]$ has no repeated factors.

Proof.

Since $\Phi_n(x) \mid x^n - 1$ and $\frac{d}{dx} x^n - 1 = nx^{n-1}$ then $gcd(x^n - 1, nx^{n-1}) = 1$ mod p since $p \nmid n$.
Ergo, $\overline{x^n - 1}$ has no repeated factors, so neither does $\overline{\Phi_n(x)}$. □

PROOF (of Theorem)
Let $\zeta_n = e^{\frac{2\pi i}{n}}$ and let $f(x) = irr(\zeta_n, \mathbb{Q}) \in \mathbb{Z}[x]$. We have then $\Phi_n(x) = f(x)g(x)$ for some $g(x) \in \mathbb{Z}[x]$.

The roots of $\Phi_n(x)$ are ζ_n^k for $k \in U(n)$ and every such k is a product of prime numbers p where $p \nmid n$, so we will show that for any root μ of $f(x)$ and any $p \nmid n$ that μ^p is a root of $f(x)$.

(We note that μ^p is a root of $\Phi_n(x)$ so it's either a root of $f(x)$ or $g(x)$.)

PROOF (continued): Let μ be a root and let $p \nmid n$ be prime and suppose $g(\mu^p) = 0$ then μ is a root of $g(x^p)$ and so $f(x) \mid g(x^p)$ in $\mathbb{Z}[x]$.

So now $\overline{f(x)}$ divides $\overline{g(x^p)} = \overline{g(x)}^p$ in $\mathbb{Z}_p[x]$ (which, recall is a UFD) so $\overline{f(x)}$ and $\overline{g(x)}$ have a common factor $h(x) \in \mathbb{Z}_p[x]$.

So $h(x)^2 \mid \overline{\Phi_n(x)}$ in $\mathbb{Z}_p[x]$ contradicting the lemma.

Thus $g(\mu^p) = 0$ is a contradiction, so $f(\mu^p) = 0$.

i.e. The roots of $f(x)$ are the roots of $\Phi_n(x)$ so $f(x) = \Phi_n(x)$ and so $\Phi_n(x)$ is irreducible, i.e. $\Phi_n(x) = irr(\zeta_n, \mathbb{Q})$. □