Section 13.6 Cyclotomic Polynomials

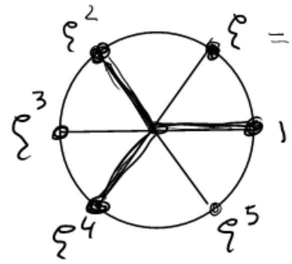
Roots of Unity

Consider $f(x) = x^n - 1$

Roots are $z \in \mathbb{C}$, with $z^n = 1$, that is the n^{th} roots of 1.

Example $x^6 - 1$

Roots are $\{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$



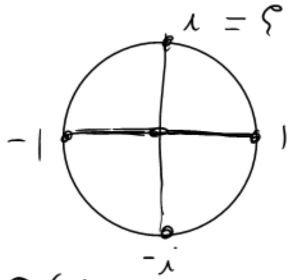
$\zeta = \cos\left(\frac{2\pi}{6}\right) + i\sin\left(\frac{2\pi}{6}\right)$

Note

- $\mu_6 = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\} \cong \mathbb{Z}_6$ is a cyclic group.
- Splitting field of $x^6 - 1$ is $\mathbb{Q}(\zeta)$
- $\zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$, so ζ is root of $x^5 + x^4 + x^3 + x^2 + x + 1$
- Thus $[\mathbb{Q}(\zeta) : \mathbb{Q}] \leq 5$
- However: $\zeta^2 - \zeta + 1 = 0$, $m_\zeta(x) = x^2 - x + 1$, so $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$

Example $x^4 - 1$

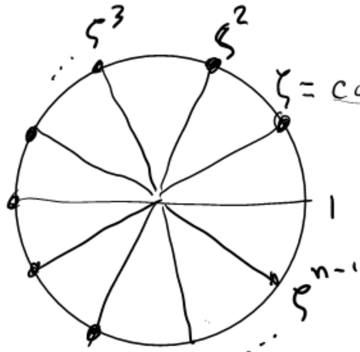
Roots are $\{1, i, i^2, i^3\}$



Note

- $\mu_4 = \{1, i, -1, -i\} \cong \mathbb{Z}_4$
- Splitting field of $x^4 - 1$ is $\mathbb{Q}(i)$
- $\zeta^3 + \zeta^2 + \zeta + 1 = 0$ so $\zeta = i$ is root of $x^3 + x^2 + x + 1$
- Thus $[\mathbb{Q}(\zeta) : \mathbb{Q}] \leq 3$
- However $\zeta^2 + 1 = 0$, so $m_\zeta(x) = x^2 - 1$ and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$

In general $x^n - 1$ has n roots, the n "roots of unity"



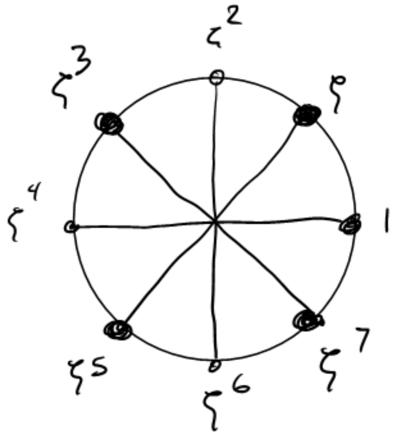
$\zeta = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$

ζ is called the principle n^{th} root of unity

- $\mu_n = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \ldots, \zeta^{n-1}\} \cong \mathbb{Z}_n$
- Splitting field of $x^n - 1$ is $\mathbb{C}(\zeta)$
- $\zeta^{n-1} + \zeta^{n-2} + \cdots + \zeta^1 + 1 = 0$, so ζ is root of $x^{n-1} + x^{n-2} + \cdots + x + 1$
- $[\mathbb{Q}(\zeta) : \mathbb{Q}] \leq n - 1$
- Root of unity z is *primitive* if it generates μ_n.
- ζ^k primitive $\iff \gcd(k, n) = 1$.
- $d \mid n \implies \mu_d \leq \mu_n$

Example Primitive elements of μ_8 are $\zeta, \zeta^3, \zeta^5, \zeta^7$, i.e. $\left\{ \pm\frac{1}{\sqrt{2}} \pm \frac{i}{\sqrt{2}} \right\}$

Also $4 \mid 8$ and indeed $\mu_4 = \{1, i, -1, -i\} \subseteq \mu_8$



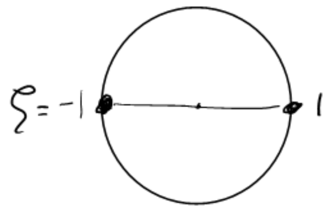
Problem Find minimal polynomial of the principle n^{th} root of unity $\zeta = \cos(2\pi/n) + i\sin(2\pi/n)$

Text If n is prime, $m_\zeta(x) = x^{n-1} + x^{n-2} + \dots + x + 1$.

In general the degree of $m_\zeta(x)$ is smaller than $n-1$.

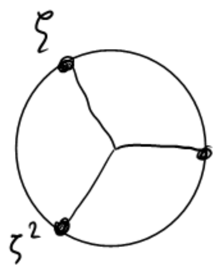
Examples

$n=2$



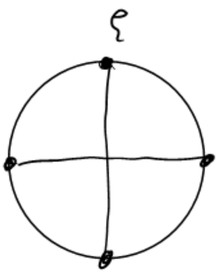
$m_\zeta(x) = x + 1 \qquad = \Phi_2(x)$

$n=3$



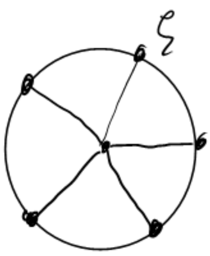
$m_\zeta(x) = x^2 + x + 1 \qquad = \Phi_3(x)$

$n=4$



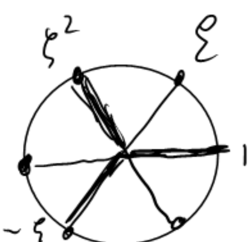
$m_\zeta(x) = x^2 + 1 \qquad = \Phi_4(x)$

$n=5$



$m_\zeta(x) = x^4 + x^3 + x^2 + x + 1 \qquad = \Phi_5(x)$

$n=6$



$m_\zeta(x) = x^2 - x + 1 \qquad = \Phi_6(x)$

These $m_\zeta(x)$ are all over the map. What's the general pattern?

The answer involves the Euler φ-function $\varphi : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$.

$\varphi(n) = \#$ of integers $1 \le a \le n$ with $\gcd(a,n) = 1$.

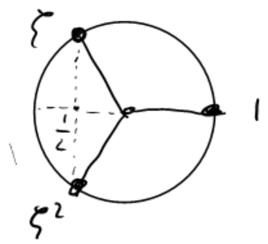
Ex
$\varphi(2) = 1 \quad a = 1$
$\varphi(3) = 2 \quad a = 1,2$
$\varphi(4) = 2 \quad a = 1,3$
$\varphi(5) = 4 \quad a = 1,2,3,4$
$\varphi(6) = 2 \quad a = 1,5$

Definition The n^{th} cyclotomic polynomial, which has degree $\varphi(n)$, is

$$\Phi_n(x) = \prod_{\substack{\alpha \in \mu_n \\ |\alpha| = n}} (x - \alpha) = \prod_{\substack{0 \le k < n \\ \gcd(k,n)=1}} (x - \zeta^k) \leftarrow \left\{ \zeta = \cos\left(\tfrac{2\pi}{n}\right) + i \sin\left(\tfrac{2\pi}{n}\right) \right\}$$

Examples
$$\Phi_1(x) = \prod_{\substack{\alpha \in \{1\} \\ |\alpha| = 1}} (x-\alpha) = x - 1 \qquad \Phi_2(x) = \prod_{\substack{\alpha \in \{-1,1\} \\ |\alpha| = 2}} (x-\alpha) = x - 1$$

$$\Phi_3(x) = \prod_{\substack{\alpha \in \mu_3 \\ |\alpha| = n}} (x - \alpha) = (x-\zeta)(x-\zeta^2)$$
$$= x^2 - (\zeta + \zeta^2)x + \zeta^3$$
$$= x^2 + x + 1$$



Theorem For each $n \in \mathbb{Z}^+$, $\Phi_n(x)$ is a monic irreducible polynomial in $\mathbb{Z}[X]$. It is the minimal polynomial for any primitive nth root of unity ζ. Thus $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg \Phi_n = \varphi(n)$.

Computation of $\Phi_n(x)$:

$$x^n - 1 = \prod_{\alpha^n = 1} (x - \alpha) = \prod_{d \mid n} \prod_{\substack{\alpha \in \mu_d \\ |\alpha| = d}} (x - \alpha) = \prod_{d \mid n} \Phi_d(x).$$

Example Find $\Phi_4(x)$

$$x^4 - 1 = \Phi_1(x)\, \Phi_2(x)\, \Phi_4(x)$$
$$x^4 - 1 = (x-1)(x+1)\, \Phi_4(x)$$
$$= (x^2 - 1)\, \Phi_4(x)$$

$$\begin{array}{r} x^2 + 1 \\ x^2 - 1 \,\big)\, \overline{x^4 + 0x^3 + 0x^2 + 0x - 1} \\ \underline{x^4 \qquad - x^2} \\ x^2 - 1 \\ \underline{x^2 - 1} \\ 0 \end{array}$$

$$\Phi_4(x) = \frac{x^4 - 1}{x^2 - 1} = x^2 + 1 \quad \text{(by long division)}$$