Info

This note, that was found here, as a part of a collection
is written (completely with human hands) by Rupadarshi Ray,
was created on March 12, 2026 9:20:31 PM,
was last modified on September 5, 2026 5:11:03 PM, and
was exported on September 7, 2026 3:04:07 PM.

Roots of $X^n - 1$, $\mathbb{Q}(\xi_n)$ and cyclotomic polynomials

Consider

$$X^n - 1$$

in $\mathbb{Q}[X]$. We wish to factorise this polynomial. We know the roots of this polynomial are precisely the **roots of unity**

Definition. Roots of unity and cyclotomic field

Let

$$\begin{aligned} \mu_n &:= \{\xi \in \mathbb{C} | \xi^n = 1\} \\ &= \left\{ \exp\left(\frac{2\pi i k}{n}\right) \middle| 1 \leq k \leq n \right\} \\ &= \{\zeta_n^k | 1 \leq k \leq n\} \\ &\subseteq U(1) \cap \overline{\mathbb{Z}} \end{aligned}$$

where $\zeta_n := \exp(2\pi i/n)$ be the group of all n-th roots of unity under multiplication which lives in the n-th **cyclotomic field**

$$\mathbb{Q}(\zeta_n)$$

Therefore,

$$X^n - 1 = \prod_{\xi \in \mu_n} (X - \xi) \quad \text{in } \mathbb{Q}(\zeta_n)[X]$$

However, we can group together the linear factors $(X - \xi)$ where ξ has order d in μ_n, that is, ξ is a **primitive d-th root of unity**

$$X^n - 1 = \prod_{d|n} \prod_{\substack{\xi \in \mu_d \\ \xi \text{ primitive}}} (X - \xi) \quad \text{in } \mathbb{Q}(\zeta_n)[X]$$

Definition. Cyclotomic polynomials

The n-th **cyclotomic polynomial** is

$$\begin{aligned} \operatorname{cyclo}_n(X) &:= \prod_{\substack{1 \leq k \leq n \\ (k,n)=1}} \left(X - \exp\left(\frac{2\pi k}{n}\right)\right) && \text{in } \mathbb{Q}(\zeta_n)[X] \\ &= \prod_{\substack{\xi \in \mu_n \\ \text{primitive}}} (X - \xi) && \text{in } \mathbb{Q}(\zeta_n)[X] \end{aligned}$$

whose roots are precisely the primitive n-th roots of unity

$$\{\xi \in \mu_n | o(\xi) = n\}$$

is monic and has degree equal to the Euler totient of n

$$\deg \operatorname{cyclo}_n = \operatorname{Euler}(n)$$

Therefore

$$X^n - 1 = \prod_{d|n} \operatorname{cyclo}_d(X) \quad \text{in } \mathbb{Q}(\zeta_n)[X]$$

which gives the identity

$$n = \sum_{d|n} \operatorname{Euler}(d)$$

$$\operatorname{cyclo}_n(X) \in \mathbb{Z}[X]$$

is monic and irreducible in $\mathbb{Q}[X]$ as well as in $\mathbb{Z}[X]$ and thus

$$X^n - 1 = \prod_{d|n} \operatorname{cyclo}_d(X) \quad \text{in } \mathbb{Z}[X]$$

Therefore, the minimal polynomial of ζ_n is cyclo_n and

$$[\mathbb{Q}(\zeta_n), \mathbb{Q}] = \deg \operatorname{cyclo}_n = \operatorname{Euler}(n)$$

As

$$\left\{ \frac{1}{\xi} \middle| \xi \in \mu_n \text{ primitive} \right\} = \{\xi \in \mu_n \text{ primitive}\} = Z(\operatorname{cyclo}_n)$$

we have

$$X^{\operatorname{Euler}(n)} \operatorname{cyclo}_n\left(\frac{1}{X}\right) = \operatorname{cyclo}_n(X)$$

Thus

$$\text{coeff of } X^j \text{ in } \operatorname{cyclo}_n(X) = \text{coeff of } X^{\operatorname{Euler}(n)-j} \text{ in } \operatorname{cyclo}_n(X)$$

which means for $\mathrm{Euler}(n) = 2M$ we have

$$X^{-M}\mathrm{cyclo}_n(X) = (X^M + X^{-M}) + a_1(X^{M-1} + X^{1-M}) + \dots$$

with $a_1, \dots, a_M \in \mathbb{Z}$.

Because

$$X^k + X^{-k} = \left(X + \frac{1}{X}\right)(X^{k-1} + X^{1-k}) - (X^{k-2} + X^{2-k})$$

shows

$$X^k + X^{-k} \in \mathbb{Z}\left[X + \frac{1}{X}\right]$$

we conclude

For $n > 2, M := \mathrm{Euler}(n)/2$. We have a monic, irreducible

$$\mathrm{ccyclo}_n \in \mathbb{Z}[X]$$

of degree M such that

$$X^{-M}\mathrm{cyclo}_n(X) = \mathrm{ccyclo}_n\left(X + \frac{1}{X}\right)$$

Moreover, for $(k, n) = 1$ we have

$$\mathrm{ccyclo}_n\left(2\cos\left(\frac{2\pi k}{n}\right)\right) = 0$$

implying $2\cos(2\pi k/n) \in \overline{\mathbb{Z}}$ has degree $\mathrm{Euler}(n)/2$.

Suppose ccyclo_n is not irreducible. Then

$$\mathrm{ccyclo}_n(X) = h_1(X)h_2(X)$$

where h_1 say is of degree $1 < r < M$. Then

$$\begin{aligned}\mathrm{cyclo}_n(X) &= X^M\mathrm{ccyclo}_n\left(X + \frac{1}{X}\right)\\ &= X^M h_1\left(X + \frac{1}{X}\right)h_2\left(X + \frac{1}{X}\right)\\ &= X^r h_1\left(X + \frac{1}{X}\right) \cdot X^{M-r}h_2\left(X + \frac{1}{X}\right)\end{aligned}$$

which contradicts

$$\mathrm{cyclo}_n(X) \in \mathbb{Z}[X]$$

is monic and irreducible in $\mathbb{Q}[X]$ as well as in $\mathbb{Z}[X]$ and thus

$$X^n - 1 = \prod_{d|n}\mathrm{cyclo}_d(X) \quad \text{in } \mathbb{Z}[X]$$

Therefore, the minimal polynomial of ζ_n is cyclo_n and

$$[\mathbb{Q}(\zeta_n), \mathbb{Q}] = \deg\mathrm{cyclo}_n = \mathrm{Euler}(n)$$

Current note has 0 direct children and 0 total descendants.

- stretchy
  - $\mathbb{Q}(\xi_n)$

And it has 62 siblings.

- stretchy
  - Trefoil 3_1 knot
  - The only compact connected Lie group that can act faithfully on a torus is itself
  - Hecke algebras
  - $\overline{B^n}$
  - $\mathrm{BS}(1, 2)$
  - $(\mathbb{C}, +, \times)$
  - $D^* := D \setminus \{0\}$
  - Cantor set
  - Configuration space of N rigid points in $\mathbb{R}^3$
  - Free groups
  - $GL(2)(\mathbb{Z}) \curvearrowright T^2$
  - H_2^3
  - $[a, b]$
  - Figure 8 knot
  - Lamplighter group on $\mathbb{Z}_2$
  - $\beta\mathbb{N}$
  - $\#_2\mathbb{R}P^2$
  - $\prod_{i\in\mathbb{N}}\{1, \dots, n_i\}$
  - $\mathbb{R}P^n$
  - $(\mathbb{Q}, +, \times, <)$
  - $\mathbb{Q}_{\hat{p}}$
  - $\overline{\mathbb{Q}}$
  - $\mathbb{Q}_{\mathrm{constr}}$
  - $\mathbb{Q}(\xi_n)$
  - $\mathcal{O}_{\overline{\mathbb{Q}}}$
  - $(\mathbb{R}, +, \times, <, \sup)$
  - Homeomorphism of $\mathbb{R}^2$ that sends $\mathbb{N}$ to a countable closed discrete subset
  - $\mathbb{R}^2 \times S^1$
  - $\mathbb{R}^n$

- $\mathbb{R} \times S^1$
- $\mathbb{R} \times S^2$
- S^1
- $S^1 \wedge S^1$
- $S^1 \times S^n$
- S^2 and $\mathbb{C}\boldsymbol{P}^1$
- Mapping torus of the antipodal map of S^2
- S^3
- S^n
- I-bundle
- Symmetric group
- $\mathbb{T}$
- T^2
- T_g^2
- $T_{0,0,3}^2$
- $\mathbb{R}^2 \setminus \{0\}$
- Three $T_{1,0,1}^2$ glued at their boundaries
- $T_{1,1,0}^2$
- T_2^2
- $T_g^2 \times [0,1]$
- $\#_{\mathbb{N}} T^2$
- Thompson's group
- T^n
- 3-valent tree
- 4-valent tree
- $[0,1]^{\mathbb{N}}$ with product topology
- Whitehead manifolds
- $\mathbb{Z}$
- $\mathbb{Z}[\sqrt{m}]$
- $\mathbb{Z}[X]$
- $\mathbb{Z}^{\mathbb{N}}$
- $\mathbb{Z}[i]$
- $\mathbb{Z}[i\sqrt{5}]$