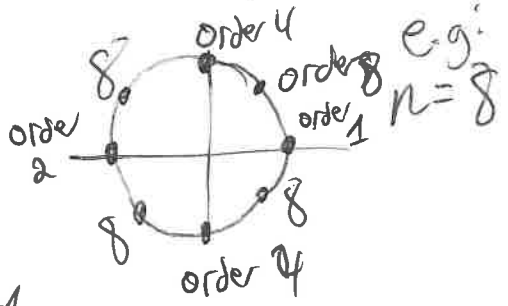
Cyclotomic fields:

$x^{n-1}/\mathbb{Q}$ splitting field: $\mathbb{Q}(e^{2\pi i/n})$, a cyclotomic field

Sol^{ns} / $\mathbb{C}$: ζ_n^h, $h \in \mathbb{Z}$; $\zeta_n := e^{2\pi i/n}$, all powers of ζ_n.

these form the set of order $d \mid n$ roots of unity.



e.g. $n=8$

Consider the gp of n-th roots of unity (sol^{ns} to $\zeta^n = 1$), called $\mu_n \cong \mathbb{Z}_n$.

isomorphism $\zeta_n^a \mapsto a$

A generator is called a primitive n^{th} r.o.u.

One choice is always ζ_n. The other choices are all ζ_n^h where $(h,n) = 1$.

Thus, the # of primitive n-th r.o.u. is $\varphi(n)$.

Note: $\zeta \in \mu_d \Rightarrow \zeta^d = 1 \Rightarrow \zeta^{dm} = 1 \ \forall\, m \in \mathbb{N} \Rightarrow \zeta \in \mu_n \ \forall\, d \mid n$.

$\Rightarrow \mu_d \subseteq \mu_n$.

Given an n-th $\zeta \in \mu_n$, its order is some $d \mid n$, ζ primitive of order $d \mid n$.

Def^n: The n-th cyclotomic polynomial, $\Phi_n(x)$,

is $\Phi_n(x) := \prod_{\substack{\zeta \in \mu_n \\ \text{primitive}}} (x - \zeta) = \prod_{\substack{1 \le h \le n \\ (h,n)=1}} (x - \zeta_n^h)$.

Clearly, $\deg(\Phi_n(x)) = \varphi(n)$.

Roots of $x^n - 1$ are all of μ_n, so

$$(*)\quad x^n - 1 = \prod_{\zeta \in \mu_n} (x - \zeta) = \prod_{d \mid n} \prod_{\zeta \in \mu_d \text{ prim.}} (x - \zeta) = \prod_{d \mid n} \Phi_d(x).$$

(organize by order)

Cor: $n = \sum_{d \mid n} \varphi(d)$. (Of course, there are more direct pfs of this!)

Ex: If $n = p$ is prime,

$$\varphi(p) = p - 1, \text{ and}$$

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

$\Phi_1(x)$ $\Phi_p(x)$

We already saw (Eisenstein + shift) $\Phi_p(x)$ is irred. / $\mathbb{Q}$

$\Rightarrow [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1 = \varphi(p)$.

- More generally, $(*)$ lets us recursively compute $\Phi_n(x)$.

E.g.: $x^6 - 1 = \Phi_1(x) \cdot \Phi_2(x) \cdot \Phi_3(x) \cdot \Phi_6(x)$

$= (x-1)(x+1)(x^2+x+1)\,\Phi_6(x)$ ($x^3 - 1$)

~~$(x^3-1)(x^3+1)$~~

~~$\rightsquigarrow \Phi_6(x) = \frac{x^6 - 1}{(x-1)(x+1)(x^2+x+1)}$~~ $= \Phi_1 (x^3 - 1)(x+1)\,\Phi_6(x)$

$x^3 + 1 = (x+1)\,\Phi_6(x) \rightsquigarrow \Phi_6(x) = \frac{x^3+1}{x+1} = x^2 - x + 1$.

This is irred. / $\mathbb{Q}$ as it has no rational roots

$\Rightarrow \Phi_6(x)$ is the min. poly of $\zeta_6 \Rightarrow [\mathbb{Q}(\zeta_6) : \mathbb{Q}] = 2 = \varphi(6)$.

More generally, $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n)$.

This follows from

Lemma: $\Phi_n \in \mathbb{Z}[x]$.

Theorem (Gauß, Kronecker)

$\Phi_n(x)$ is irreducible / $\mathbb{Q}$

($\Leftrightarrow$ it is the min. poly of ζ_n).

Pf of Lemma: We use strong induction on n.

$n=1$: $\Phi_1 = x-1$ ✓.

Assume true $\forall\, m<n$. Then

$$x^n - 1 = \prod_{d\mid n} \Phi_d(x) = \Phi_n(x) \cdot \prod_{\substack{d\mid n \\ d<n}} \Phi_d(x) =: \Phi_n(x)\cdot h(x).$$

Induction hypothesis $\Rightarrow h \in \mathbb{Z}[x]$.

By long division, $\Phi_n(x) \in \mathbb{Q}[x]$.

Gauß' Lemma $\Rightarrow \Phi_n(x) \in \mathbb{Z}[x]$. ∎

Pf of theorem: If Φ_n reducible, so $\exists$ monic $g, f \in \mathbb{Z}[x]$,

$\Phi_n = f\cdot g$. Further assume f is an irred. factor of Φ_n.

Let ζ be a primitive n-th r.o.u. which is a root of f,

and take a prime $p \nmid n$. Then ζ^p is also of order n,

and a root of either f or g.

Case 1: $g(\zeta^p) = 0$.

then ζ is a root of $g(x^p)$ and $f(x)$ is the min. poly. of $\zeta \Rightarrow f(x) \mid g(x^p)$ in $\mathbb{Z}[x]$, i.e.

$$g(x^p) = f(x) \cdot h(x), \text{ some } h \in \mathbb{Z}[x].$$

Reducing mod p, we get an eq^n

$$\bar{g}(x^p) = \bar{f}(x)\bar{h}(x) \quad \text{in } \mathbb{F}_p[x].$$

But mod p, $\bar{g}(x^p) = (\bar{g}(x))^p$

$$\Rightarrow (\bar{g}(x))^p = \bar{f}(x) \cdot \bar{h}(x).$$

This eq^n is in the UFD $\mathbb{F}_p[x]$.

Thus, $\bar{f}, \bar{g}$ have a common factor in $\mathbb{F}_p[x]$

Recalling $\Phi_n = f \cdot g$, $\overline{\Phi_n} = \bar{f} \cdot \bar{g} \Rightarrow \overline{\Phi_n}$ has a mult. root mod p. But $\Phi_n \mid x^n - 1$, so this $\Rightarrow$ $x^n - 1$ has a mult. root mod p.

But $(x^n - 1)' = nx^{n-1}$, and $p \nmid n$, so $(x^n-1)' \neq 0$, only root is $x = 0$, not a root of $x^n - 1$

$\rightsquigarrow *$.

Case 2: $\forall f(\zeta^p) = 0$.

This argument works $\forall$ roots ζ of $f(x)$.

But then taking any $(h, n) = 1$, write $h = \prod p_i$, p_i primes not dividing n.

$\Rightarrow \zeta^{p_1}$ is a root of f, $(\zeta^{p_1})^{p_2}$ is too, etc. $\Rightarrow \zeta^h$ is a root of f.

$\Rightarrow$ all primitive n-th roots are roots of $f \Rightarrow f = \Phi_n$

$\Rightarrow \Phi_n$ is irreducible.