Cyclotomic fields — $\mathbb{Q}(\zeta)$ ζ: primitive n^{th} root of unity.

In particular this extension is Galois over $\mathbb{Q}$, as the splitting field of $X^n - 1$.

The action of the Galois gp takes prim roots to prim roots, thus we have injection $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ ← order is $\phi(n)$: Euler phi function.

$n = p_1^{e_1} \cdots p_r^{e_r}$, then $\phi(n)$ multiplicative and $\phi(p^e) = (p-1)p^{e-1}$

What is minimal polynomial?

claim: It is $\phi_n(X) := \prod_{m \in \mathbb{Z}/n\mathbb{Z}^\times} (X - \zeta^m)$ for any ζ: primitive n^{th} rt.

(or more properly reps in $\mathbb{Z}$ for these residue classes)

$= \prod_{\zeta : prim} (X - \zeta)$

Since G permutes prim roots, $\phi_n(X)$ in fixed field of G, $\mathbb{Q}[X]$.

with ζ as root of course. So ϕ_n is minimal poly. iff ϕ_n irreducible.

(then we know $[\mathbb{Q}(\zeta):\mathbb{Q}] = \varphi(n)$ so $G \simeq (\mathbb{Z}/n\mathbb{Z})^\times$)

We show this by reducing to prime powers. Let $n = p^r$ some prime p, $r \geq 1$.

Given two primitive rts. of unity ζ, ζ' then $\zeta = (\zeta')^t$ $\zeta' = \zeta^s$ some t, s

Thus consider $\frac{1-\zeta'}{1-\zeta} = 1 + \zeta + \cdots + \zeta^{s-1} \in \mathbb{Z}[\zeta]$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \|$

$\frac{1-\zeta}{1-\zeta'} = 1 + \zeta' + \cdots + (\zeta')^{t-1} \in \mathbb{Z}[\zeta']$

so these are units in the order $\mathbb{Z}[\zeta] \subseteq \mathcal{O}_K$

$\phi_{p^r}(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = 1 + X^{p^{r-1}} + \cdots + X^{p^{r-1}(p-1)}$ ← since $X^n - 1 = \prod_{d|n} \phi_d(X)$

In particular $\phi_{p^r}(1) = p$

But $\phi_{p^r}(1) = \prod_{\xi' \text{ prim}} (1-\xi') = \prod_{\xi' \text{ prim.}} \frac{1-\xi'}{1-\xi}(1-\xi)$ $\quad \xi$: fixed primitive

$$= u \cdot (1-\xi)^{\varphi(p^r)}$$

$\Rightarrow \quad p \cdot \mathcal{O}_K = \langle (1-\xi)^{\varphi(p^r)} \rangle = \langle 1-\xi \rangle^{\varphi(p^r)}$ so $(1-\xi)$ is ideal in $\mathcal{O}_K$

p ramifies with index $e = \varphi(p^r)$. for each prime dividing $(1-\xi)$

$\Rightarrow \quad [\mathbb{Q}(\xi_{p^r})/\mathbb{Q}] \geq \varphi(p^r)$. (Already knew reverse ineq. so we have equality...)

$\Rightarrow \quad (1-\xi)$ prime ideal, else wouldn't have "$e \cdot f \cdot r = n$" for primes above p.

and p "totally ramified" in K

$(f = r = 1)$

so in particular $f=1$ implies $\mathcal{O}_K/_{(1-\xi)} \simeq \mathbb{Z}/p\mathbb{Z}$.

(we use this fact in determining $\mathcal{O}_K$).

To calculate $\mathcal{O}_K$, see how much we need to enlarge $\mathbb{Z}[\xi]$.

Compute $\operatorname{disc}(1, \xi, \dots, \xi^{\varphi(p^r)-1}) = \operatorname{disc.}(\phi_{p^r}(x)) = \prod_{i<j} (\xi_i - \xi_j)^2$

$$= \pm \prod_{i=1}^{\varphi(p^r)} \phi'_{p^r}(\xi_i) = \pm N(\phi'_{p^r}(\xi)) \qquad \pm = (-1)^{d \cdot d-1/2}$$

d: deg. of ext'n

General identity for any sep. ext'n.

The value $\phi'_{p^r}(\xi)$ is computed from identity $\phi_{p^r}(x) = \frac{x^{p^r}-1}{x^{p^{r-1}}-1}$, diff. both sides,

to get $\phi'_{p^r}(\xi) = p^r \cdot \xi^{p^r-1} / (\xi^{p^{r-1}}-1)$

Left to calculate

know $N(p^r) = (p^r)^{\varphi(p^r)}$, $N(\xi) = \pm 1$. $\quad N(\xi^{p^{r-1}}-1)$

write $r-1=s$: To compute: $N(\zeta^{p^s}-1)$. If $s=0$, just $N(\zeta-1) = \pm N(1-\zeta)$
$= \pm p$.

since $1-\zeta$ has minimal poly.

$\phi_{p^r}(1-X)$ whose constant term is $\phi_{p^r}(1) = p$.

Now for any $0 \le s < r$, ζ^{p^s} is a primitive $(p^{r-s})^{th}$ root of unity. So same computation gives (since $\phi_{p^{r-s}}(1) = p$) that

$$N_{\mathbb{Q}(\zeta^{p^s})/\mathbb{Q}}(1-\zeta^{p^s}) = \pm p.$$ But N is well-behaved in towers,

so $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\zeta^{p^s}) = \pm p^d$ where $d = [\mathbb{Q}[\zeta] : \mathbb{Q}[\zeta^s]]$
$= \varphi(p^r)/\varphi(p^{r-s}) = p^s$

Putting it all together, $N_{K/\mathbb{Q}} \phi'_{p^r}(\zeta)$
$= \pm p^c$ with $c = p^{r-1}(pr-r-1)$

Now we know $\operatorname{disc}(\mathcal{O}_K) \cdot [\mathcal{O}_K : \mathbb{Z}(\zeta)]^2 = \operatorname{disc}(1, \zeta, \dots, \zeta^{\varphi(p^r)-1})$
$\qquad = \pm p^c$

so $[\mathcal{O}_K : \mathbb{Z}(\zeta)]$ is power of p, and $p^c \cdot \mathcal{O}_K \subseteq \mathbb{Z}[\zeta] \subseteq \mathcal{O}_K$.

clever trick: $\mathcal{O}_K/(1-\zeta) \simeq \mathbb{Z}/p\mathbb{Z}$ so as abelian gps,
$\mathcal{O}_K = (1-\zeta)\mathcal{O}_K + \mathbb{Z}$

and so $\mathcal{O}_K = (1-\zeta)\mathcal{O}_K + \mathbb{Z}[\zeta]$ (*)

mult. by $(1-\zeta)$ in (*): $(1-\zeta)\mathcal{O}_K = \underbrace{(1-\zeta)^2\mathcal{O}_K + (1-\zeta)\mathbb{Z}[\zeta]}$

substitute in (*) for $(1-\zeta)\mathcal{O}_K$ noting $(1-\zeta)\mathbb{Z}[\zeta] + \mathbb{Z}[\zeta] = \mathbb{Z}[\zeta]$

Get $\mathcal{O}_K = (1-\zeta)^2\mathcal{O}_K + \mathbb{Z}[\zeta]$

repeating m times: $\mathcal{O}_K = (1-\zeta)^m\mathcal{O}_K + \mathbb{Z}[\zeta]$

Since $(1-\zeta)^{\varphi(p^r)} = p \cdot \text{unit}$, get $\mathcal{O}_K = p^l\mathcal{O}_K + \mathbb{Z}[\zeta]$ for any l.