On Monday, in midst of exploring "cyclotomic extensions" $\mathbb{Q}(\zeta_n)$ ζ_n: n^{th} rt. of 1. (primitive)

INTRO

So far: if $n = p^r$, then $[\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}] = \varphi(p^r)$ $= p^{r-1}(p-1)$

with minimal polynomial $\phi_n(x) = \prod_{\zeta:\text{ prim } n^{th}\text{ root}} (x - \zeta)$

with $p \cdot \mathcal{O}_K = ((1-\zeta)\mathcal{O}_K)^{\varphi(p^r)}$

i.e. for p: $e = \varphi(p^r)$, $f = 1$, $r = 1$.

in $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$
$\quad\quad \backslash|/$
$\quad\quad\; p$

and we had claimed $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^r}]$ but not finished pf.

(calculated $d(1, \zeta_{p^r}, \dots) = N_{K/\mathbb{Q}}(\phi'_{p^r}(\zeta_{p^r})) = \pm p^c$ $\quad c = p^{r-1}(pr - r - 1)$

which implied $p^c \cdot \mathcal{O}_K \subseteq \mathbb{Z}[\zeta_{p^r}] \subseteq \mathcal{O}_K$.)

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

since $1-\xi$ has minimal poly.

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

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

$$N_{\mathbb{Q}(\xi^{p^s})/\mathbb{Q}}(1-\xi^{p^s}) = \pm p.$$

But N is well-behaved in towers,

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

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

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

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

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

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

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

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

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

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

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

But $p^l \mathcal{O}_K \subset \mathbb{Z}[\zeta]$ for some l. (e.g. $l = c$.)

so in fact $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

From here, not hard to prove analogous facts for primitive n-th roots (n not nec. prime power)

<u>Theorem</u>: (a) $\mathbb{Q}(\zeta_n)$ is degree $\varphi(n)$ extension of $\mathbb{Q}$

(b) $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$

(c) if $n = p^r \cdot m$ with $\gcd(m,p) = 1$, then

$$(p) = (\mathfrak{P}_1 \cdots \mathfrak{P}_s)^{\varphi(p^r)}$$

(and these prime divisors of n are only ones that ramify)

<u>pf</u>: By induction. Write $n = p^r m$. By induction, we may assume true for m, then use fact that $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_{p^r})\mathbb{Q}(\zeta_m)$ $\quad \zeta_{p^r} := \zeta^m$, $\zeta_m := \zeta^{p^r}$

$$\begin{tikzcd}[column sep=small] & \mathbb{Q}(\zeta) = K \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\zeta_{p^r}) \arrow[dr, dash] & & \mathbb{Q}(\zeta_m) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

From our prior results, know p is totally ramified in $\mathbb{Q}(\zeta_{p^r})$ and unramified in $\mathbb{Q}(\zeta_m)$ (made up of primes away from m, and these prime divisors of m are only ramified primes)

$$\begin{tikzcd}[column sep=small] & ? \arrow[dl, dash] \arrow[dr, dash] & \\ \mathfrak{p}^{\varphi(p^r)} \arrow[dr, dash] & & \mathfrak{P}_1 \cdots \mathfrak{P}_s \arrow[dl, dash] \\ & p & \end{tikzcd}$$

Now $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta_m)] \leq \varphi(p^r)$ since since it is obtained from $\mathbb{Q}(\zeta_m)$ by adjoining ζ_{p^r} which has order $\varphi(p^r)$ over $\mathbb{Q}$.

$$(\mathcal{O}_K \mathfrak{p})^{\varphi(p^r)} = \mathcal{O}_K \mathfrak{P}_1 \cdots \mathfrak{P}_s \Rightarrow [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_m)] = \varphi(p^r)$$

$$\underset{\text{by induction}}{\Rightarrow} [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(p^r)\varphi(m) = \varphi(n)$$

and proves (c).

To show $\mathcal{O}_k = \mathbb{Z}[\xi_n]$, write $n = p_1^{t_1} \cdots p_r^{t_r}$ with $\xi_i = \xi_n^{n/p_i^{t_i}}$

All discriminants $d(1, \xi_i, \ldots, \xi_i^{\varphi(p_i^{t_i})-1}) = \pm p_i^{c_i}$ and so are rel. prime.

so set $\xi_1^{j_1} \cdots \xi_r^{j_r}$ $j_i \in [0, \varphi(p_i^{t_i})-1]$

give integral basis of $\mathbb{Q}(\xi) | \mathbb{Q}$. In particular each $\alpha \in \mathcal{O}_K$

is expressible as $\alpha = f(\xi)$ coeffs. in $\mathbb{Z}$. degree $\leq \varphi(n)-1$.

$\Rightarrow$ $[1, \xi, \ldots, \xi^{n-1}]$ is desired integral basis // since each of $\xi_1^{j_1} \cdots \xi_r^{j_r}$ is a power of $\xi := \xi_n$

Other basic ingredients — class number/gp and fund. units remain hard problems.

For example, some wacky facts about class #'s of $\mathbb{Q}(\xi_n)$:

if $n < 23$, then $h(n)$: class # is 1. $h(23) = 3$.

$h(101) \sim 3.54 \times 10^{12}$

mention Kronecker-Weber theorem:

Every abelian ext'n of $\mathbb{Q}$ is contained in $\mathbb{Q}(\xi_n)$ for some n.

What if we change the base field? (Kronecker's Jugendtraum)

Finally, we give a more precise characterization of how primes (any prime) decompose in a cyclotomic extension.

This may be viewed as a "reciprocity law" for cyclotomic extensions.

Proposition : Write ~~$n = p_1^{e_1} \cdots p_m^{e_m}$~~. For any prime q (may be in list, may not)

find smallest integer f_q such that

$$q^{f_q} \equiv 1 \mod n/q^{\mathrm{ord}_q(n)}$$

Then $$q\,\mathcal{O}_K = (\mathfrak{q}_1 \cdots \mathfrak{q}_r)^{\varphi(q^{\mathrm{ord}_q(n)})}$$ with residue degrees $[\mathcal{O}_K/\mathfrak{q}_i : \mathbb{Z}/q\mathbb{Z}] = f_q$.

pf: $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$, so our earlier results about factoring min poly. over finite fields apply for $\underline{\underline{\text{all}}}$ primes. (indeed conductor is 1)

Factor $\phi_n(x)$: min. poly for ζ_n, mod q.

if $q \mid n$, say $\mathrm{ord}_q(n) = e \geq 0$, write $n = q^e \cdot m$

$$\phi_n(x) = \prod_{i,j} (x - \zeta_i \eta_j)$$ ζ_i : prim m^{th} rt. η_j : prim. q^e rt.

But $x^{q^e} - 1 \equiv (x-1)^{q^e} \mod \mathfrak{q}$, so $\eta_j \equiv 1$ $\mathfrak{q}$ with $\mathfrak{q} \mid q$.

so $$\phi_n(x) \equiv \prod_i (x - \zeta_i)^{\varphi(q^e)} = \phi_m(x)^{\varphi(q^e)} \mod \mathfrak{q}$$ and hence mod q.

want to show ϕ_m factors into irred. polys of degree f_q, the order of q mod $\underline{\underline{m}}$.

Consider $\phi_m(x)$ where $\gcd(m, q) = 1$.

$x^m - 1$ has no multiple roots, else $x^m - 1$, $\frac{d}{dx}(x^m - 1) = mx^{m-1}$ would have common root
in $\mathcal{O}_K/\mathfrak{q}$

which is impossible since $\mathrm{char}(\mathcal{O}_K/\mathfrak{q}) = q \nmid m$.

so $\mathcal{O}_K/\mathfrak{q}$ contains all n distinct n^{th} roots of unity.

and in particular prim. roots remain primitive.
in projection $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{q}$.

Over $\mathbb{F}_q$, smallest extension containing prim. m^{th} root is $\mathbb{F}_{q^{f_q}}$
whose mult. gp is cyclic of order $q^{f_q} - 1 \equiv 0 \ (m)$

so $\overline{\phi}_n(x)$ factors completely over this extension.
(reduction of ϕ_n mod q) and has no multiple roots since $\phi_n \mid x^n - 1$.

so if $\overline{\phi}_n(x) \equiv \overline{p}_1(x) \cdots \overline{p}_r(x)$ mod q is factorization into irreducibles,

each $\overline{p}_i$ is min poly. of prim. m^{th} rt. of unity in $\mathbb{F}_{q^{f_q}}^\times$

so of degree f_q. //

Example: $\mathbb{Q}(\zeta_5)$ $\quad x^5 - 1 = (x-1)(x^4 + x^3 + \cdots + 1)$

mod 7, since $7 \equiv 2 \ (5)$ which has order 4 $\quad f_p = 4$. Expect $x^4 + \cdots + 1$ is irred. mod 7.

mod 11, $\equiv 1 \ (5)$, expect linear factors

$(x+2)(x+6)(x+7)(x+8) \pmod{11}$

mod 29 $\quad \equiv -1 \ (5)$ $\quad (x^2 + 6x + 1)(x^2 + 24x + 1) \pmod{29}$