Lecture 17: Primes in cyclotomic fields

Reminder: Exam on Monday

Special schedule this week: Wed: Scott Hargren, Fri: No class.

Office hours this week:
Me: Mon 10-11, Sun: TBA
Jonah: Tue 3-4, Fri 3-4, Cobol B1.

Thm: $n = \prod p_i^{v_i}$ the prime factorization of $n \in \mathbb{N}$. Then in $\mathbb{Q}(\zeta_n)$,

$$\Phi(p^{v_p}) = (\Phi_1, \ldots, \Phi_r)$$

where the $\Phi_i$ are distinct primes of minimal degree $f_p = \text{order of } p \text{ in } \mathbb{Z}/(n^{v_p} \mathbb{Z})$.

[Recall motivation re: quadratic reciprocity.]

Proof: Let $L = \mathbb{Q}(\zeta_n)$. As $\mathcal{O}_L = \mathbb{Z}[\zeta_n]$ the factorization of $p\mathcal{O}_L$ is determined by that of $\Phi_n(x) \mod p$.

cyclotomic poly. Case $p \nmid n$, i.e., $v_p = 0$. Let $\beta \in \mathcal{O}_L$ be a prime above $p$.

First, observe $(n^{th} \text{ roots of } 1)\mathcal{O}_L \rightarrow \mathcal{O}_L/\beta$ is injective,
since $X^n - 1$ has distinct roots in $\mathbb{Q}_p / \beta$
(Rnote that $X^n - 1$ and $nX^{n-1}$ have no common roots)
since $p \nmid n$.

In particular, $\mathbb{Q}_p / \beta$ is the extension of $\mathbb{F}_p$
gotten by adjoining all of the $n^{th}$ roots of unity.

Now $\mathbb{Q}_p / \beta = \mathbb{F}_{p^f}$ and $n$ divides $|\mathbb{F}_{p^f}| = p^f - 1$.
Thus $p^f \equiv 1 \mod n$, and $f \nmid f$. Since $\mathbb{F}_{p^f}$ is cyclic,
in fact $\mathbb{Q}_p / \beta = \mathbb{F}_{p^{f_1}}$. Thus $\Phi_n \in \mathbb{F}_{p}[x]$ factors
into $\Phi_1(x)^e \cdots \Phi_r(x)^e$ all of degree $f_p$.

As $X^n - 1$ has distinct roots in $\mathbb{Q}_p / \beta$, must
have $e = 1$, completing the proof in this case.

**General Case:** Let $m$ by $n = p^r m$. Consider

$\{\xi_i\}$ - primitive $(p^r m)^{th}$ roots of unity

$\{\xi_j\}$ - primitive $m^{th}$ roots of unity.

Then $\{\xi_i \xi_j\}$ are exactly the primitive $m^{th}$
roots of unity.
Thus \( \Phi_n(x) = \prod_{i,j} (x - \eta_i \xi_j) \)

Now \( x^{p^v} \equiv (x-1)^{p^v} \mod p \), so if \( \beta \) is a prime of \( \mathbb{Q}_L \) above \( p \), we have \( \eta_i \equiv 1 \mod \beta \).

Thus
\[
\Phi_n(x) \equiv \prod_{i,j} (x - \xi_j) \equiv \Phi_m(x)^{\Phi(p^v)} \mod \beta
\]

As this is true for some prime above \( p \), we get
\[
\Phi_n(x) \equiv \Phi_m(x)^{\Phi(p^v)} \mod p \quad \text{②}
\]
and we've reduced to the earlier case.

[② The point is just \( \beta \mathbb{Z} = (p) \).]

Next turn: Quadratic Reciprocity

Special case: \( \left( \frac{2}{p} \right) = (-1)^{\frac{p^2-1}{8}} \)

Proof:
Since \((1+i)^2 = 2i\), we have

\[
(1+i)^p = (1+i)( (1+i)^2 )^{\frac{p-1}{2}} = (1+i) \cdot i^{\frac{p-1}{2}} \cdot 2^{\frac{p-1}{2}}
\]

Now \(\left( \frac{2}{p} \right) \equiv 2^{\frac{p-1}{2}} \mod p\), since \(\mathbb{F}_p^\times \equiv \mathbb{Z}_{p-1}^\times \equiv (\mathbb{F}_p^\times)^2\).

Combining

\[
(1+i)^p \equiv 1 + i^p \equiv 1 + i(-1)^{\frac{p-1}{2}} \equiv (1+i) i^{\frac{p-1}{2}} \left( \frac{2}{p} \right) \mod p
\]

If \(\frac{p-1}{2}\) is even, we have \((1+i) \equiv (1+i) (-1)^{\frac{p-1}{4}} \left( \frac{2}{p} \right) \mod p\).

\[
\Rightarrow \left( \frac{2}{p} \right) = (-1)^{\frac{p-1}{4}}. \quad (\text{Note } (1+i) \text{ is invertible } \mod p; \text{ take } (1+i)^{-1} = (1-i) 2^{-1}.)
\]

A similar calculation shows \(\left( \frac{2}{p} \right) = (-1)^{\frac{p+1}{4}}\) if \(\frac{p-1}{2}\) is odd.

Since

\[
\frac{p^2-1}{8} = \left( \frac{p-1}{4} \right) \left( \frac{p+1}{2} \right) = \left( \frac{p+1}{4} \right) \left( \frac{p-1}{2} \right)
\]

we're done.