Lecture 15: Primes in cyclotomic fields

Goal: ① Understand exactly how rat'l primes split in $\mathbb{Q}(\zeta_n)$.
② Use explain quadratic reciprocity.

Recall: **Thm:** $p \in \mathbb{Z}$ an odd prime.
Then $p = a^2 + b^2$ for $a, b \in \mathbb{Z}$ iff $p \equiv 1 \bmod 4$.

Alt. Proof: Suppose $p \equiv 1 \bmod 4$. Need to show $\mathfrak{p} = p\mathbb{Z}[i]$ is not prime. If it were, we have

$$\begin{array}{ccc} \mathbb{Z}[i] & \longrightarrow & \mathbb{Z}[i]/\mathfrak{p} \cong \mathbb{F}_{p^2}, \text{ where } \bar{i} \text{ is a primitive elt} \\ | & & | \quad \text{for the right-hand extension.} \\ \mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \end{array}$$

But $\mathbb{F}_p$ already contains the square roots of -1 a contradiction. ∎

Understanding $p\mathcal{O}_L$ in general: L/K extension of number fields.
$\mathfrak{p}$ a prime in $\mathcal{O}_K$,
Suppose $\mathcal{O}_L = \mathcal{O}_K[\theta]$ and $\mathfrak{p}\mathcal{O}_K = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$ with $\mathfrak{q}_i$ distinct primes with inertial degree f_i. Now

$$\begin{array}{ccc} \mathcal{O}_L & \longrightarrow & \mathcal{O}_L/\mathfrak{q}_i = K(\mathfrak{q}_i) \\ | & & | \\ \mathcal{O}_K & \longrightarrow & \mathcal{O}_K/\mathfrak{p} = K(\mathfrak{p}) \end{array}$$

and so $\bar{\theta}$ is a primitive element of the right-hand extension.

Thus if $p(x) \in \mathcal{O}_K[x]$ is the min poly of θ, the poly $\bar{p}(x) \in k(\mathfrak{p})[x]$ has the min poly $\bar{p}_i$ of $\bar{\theta}$ as one of its irreducible factors. ($\bar{p}_i$: degree f_i)

By the Chinese Remainder Thm

$$\mathcal{O}_L \longrightarrow k(\mathfrak{P}_i) \oplus k(\mathfrak{P}_j) \text{ is onto} \Rightarrow \bar{p}_i \neq \bar{p}_j$$

Turns out $\bar{p}(x) = \prod \bar{p}_i(x)^{e_i}$, and so determines the factorization of $\mathfrak{p}\mathcal{O}_L$.

In general, let $\theta \in \mathcal{O}_L$ be a primitive element of L/K. The conductor of $\mathcal{O}_K[\theta]$ largest ideal of $\mathcal{O}_L$ contained in $\mathcal{O}_K[\theta]$. Let $p \in \mathcal{O}_K[x]$ be the min. poly of θ.

Thm: Suppose $\mathfrak{p}$ in $\mathcal{O}_K$ is rel prime to (cond of $\mathcal{O}_K[\theta]$). If $\bar{p}(x) = \prod \bar{p}_i(x)^{e_i}$ in $k(\mathfrak{p})[x]$, then

($\bar{p}_i$: irreducible, degree f_i; p_i: monic lift of $\bar{p}_i$ to $\mathcal{O}_K[x]$)

$$\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{P}_i^{e_i} \text{ where } \mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + p_i(\theta)\mathcal{O}_L$$

is prime with inertial degree f_i.

Pf: See text.

Cor: An odd prime p splits in $\mathbb{Q}(\sqrt{d})$ iff d is a square mod p. (Σ rel prime to p)

Pf: We have $2\,\mathcal{O}_{\mathbb{Q}(\sqrt{d})} \subseteq \mathbb{Z}[\sqrt{d}]$, so the conductor is coprime to $p\mathcal{O}_L$. Thus the thm applies, and p splits iff $x^2 - d$ factor in $\mathbb{Z}/p\mathbb{Z}$. ▨

Quadratic Residues: p an odd prime.

$a \in \mathbb{Z}$ is a *quadratic residue* mod p if $x^2 \equiv a \bmod p$ has a solution, i.e. $\bar{a}$ has a square root in $\mathbb{F}_p$. Henceforth assume $a \not\equiv 0 \bmod p$.

Exactly half of the elts of $\mathbb{F}_p^\times$ are quad. residues.

Legendre symbol: $\left(\frac{a}{p}\right) = \begin{cases} +1 & a \text{ is a Q.R. mod } p \\ -1 & \text{otherwise.} \end{cases}$

Note: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Alt Pf: Consider $\mathbb{F}_p^\times \to \mathbb{F}_p^\times / (\mathbb{F}_p^\times)^2$

Pf: $QR \times QR = QR$ ✓
$NR \times QR = NR$ ✓
$NR \times NR = QR$ — apply the pigeon-hole principle to $\mathbb{F}_p^\times \to \mathbb{F}_p^\times$, $x \mapsto ax$ where a is a NR.

Gauss's Quadratic Reciprocity:

Suppose p and q are odd primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$