Lecture 18: Quadratic Reciprocity — the thrilling conclusion

- Collect HW, put in Bamrod Yattan's box.
- Reminder: No class Friday
  Exam Monday.

Quadratic Reciprocity: If p, q are odd primes, then

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \text{ or } q \text{ is } 1 \bmod 4 \\ \left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \bmod 4 \end{cases}$$

[Also have rules for $\left(\frac{-1}{p}\right)$ ← on HW and $\left(\frac{2}{p}\right)$ ← monday's class]

[↑ Denotes things I wouldn't write if I were lecturing]

On Friday, we saw Quad Recip is equiv. to

Thm $\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$ given that $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

We also know [From last Wed + Friday.]

Lemma: $p \neq q$ odd rat'l primes.

① $\left(\frac{p}{q}\right) = 1 \iff q$ splits in $\mathbb{Q}(\sqrt{p})$

② p splits in $\mathbb{Q}(\sqrt{q^*}) \iff p$ splits into an even number of primes in $\mathbb{Q}(\zeta_q)$

Proof of Q.R.: By the lemmas, we have

$$\left(\frac{q^*}{p}\right) = 1 \iff p \text{ splits in } \mathbb{Q}(\sqrt{q^*})$$

$$\iff p \text{ splits into an even \# of primes in } \mathbb{Q}(\zeta_q)$$

Now p is unramified in $\mathbb{Q}(\zeta_q)$, and

$$p\mathcal{O}_{\mathbb{Q}(\zeta_q)} = \mathfrak{p}_1 \cdots \mathfrak{p}_r \text{ where the } \mathfrak{p}_i \text{ have inertial degree } f_p = \text{order of } p \text{ in } \mathbb{F}_q^\times$$

By the Fund. Identity, $r = \frac{q-1}{f_p}$.

So r is even $\iff f_p \mid \frac{q-1}{2} \iff p^{\frac{q-1}{2}} \equiv 1 \bmod q$

$$\iff \left(\frac{p}{q}\right) = 1,$$

proving the theorem. ▨

[Mentioned last time, but to review:]

$$\left(\frac{p}{q}\right) = 1 \iff p \in \underbrace{\left(\mathbb{F}_q^\times\right)^2} \iff p^{\frac{q-1}{2}} \equiv 1 \bmod q$$

- has order $\frac{q-1}{2}$
- contains all elts of order dividing $\frac{q-1}{2}$ since $\mathbb{F}_q^\times$ is cyclic.

Euler's criterion

Generalizations:

[Quad Rec. was discovered by Euler and proved by Gauss in 1796. The quest for generalizations lead directly to Math 530; e.g. Kummer introduced ideals to study such laws. Much of the 19th century was spent on this.]

Cubic Reciprocity: For the cleanest statement, we work in $\mathbb{Z}[\omega] = \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ where $\omega = \frac{-1+\sqrt{3}i}{2}$

[cube root of 1.]

Def: $\alpha \in \mathbb{Z}[\omega]$ is primary if it is coprime to 3 and $\equiv 2 \bmod 3$.

[Point: each prime ideal is gen by a unique primary elt.]

Define $\left(\frac{\alpha}{\beta}\right)_3 = \begin{cases} +1 \text{ if } \alpha \text{ is a cube mod } \beta \\ -1 \text{ otherwise.} \end{cases}$

Thm: If α and $\beta \in \mathbb{Z}[\omega]$ are primary, then $\left(\frac{\alpha}{\beta}\right)_3 = \left(\frac{\beta}{\alpha}\right)_3$.

Eventually, study of these laws lead to class field theory, in particular to

Artin Reciprocity: L/K a normal ext. of # fields

Then $\mathrm{Gal}(L/K)^{ab} \cong C_K / N_{L/K}(C_L)$

[idèlic class group, closely related to the class group; defined using adèlic methods (p-adic #s) that we'll talk about later in the term]