MATH 225A: LECTURE 17
NOVEMBER 23, 2021
SCRIBE: MICHAEL ZSHORNACK

6.2 Cyclotomic Extensions

We next turn to discussing some of the uses of Frobenius elements in the specific context of cyclotomic fields. First, we recall some facts about these fields from basic Galois theory. For $m \geq 1$, we let ζ_m be a primitive mth root of unity. Then the map

$$\begin{aligned} (\mathbb{Z}/m\mathbb{Z})^\times &\mapsto \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \\ a \pmod{m} &\mapsto (\sigma_a : \zeta_m \mapsto \zeta_m^a) \end{aligned}$$

is an isomorphism. Part of why we care about cyclotomic extensions of $\mathbb{Q}$ is because of the following theorem.

Theorem (Kronecker–Weber)**.** *Let $K/\mathbb{Q}$ be an abelian extension. Then there exists an m such that $K \subseteq \mathbb{Q}(\zeta_m)$.*

We won't discuss the proof of this theorem here, but it is something that can be approached by class field theory.

We note the following facts about cyclotomic extensions. Let $\mathfrak{O}$ denote the ring of integers of $\mathbb{Q}(\zeta_m)$. It's clear that we have the inclusion $\mathbb{Z}[\zeta_m] \subseteq \mathfrak{O}$ (in fact, this inclusion is an equality, but in the discussion that follows, we will only need this direction). Now, we can calculate directly that

$$\Delta(1, \zeta_m, \ldots, \zeta_m^{\varphi(m)-1}) = \prod_{\substack{\zeta \neq \zeta' \\ m\text{th roots of } 1}} (\zeta - \zeta')$$

where φ is the Euler φ-function. To compute this value, we use L'Hôpital's rule and notice that

$$\lim_{x\to 1}\frac{x^m-1}{x-1} = m = \prod_{\substack{\zeta\neq 1\\ m\text{th root of }1}}(1-\zeta).$$

From this then, we see that if $(p) \mid (\zeta - 1)$ as ideals for a prime $p \in \mathbb{Z}$ and $\zeta \neq 1$, then $p \mid m$. Moreover, if p ramifies in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, then $p \mid m$. Also, this tells us that if $p \nmid m$, then the product $\Delta(1, \zeta_m, \dots, \zeta_m^{\varphi(m)-1})$ is not congruent to 0 modulo p and so all the terms in the product must be distinct. Hence, if $p \nmid m$, we have the implication $\zeta \equiv \zeta' \pmod{p} \implies \zeta = \zeta'$.

Next, we will want to look at the Frobenius element associated to the prime p in the following theorem.

Theorem 6.8 (Decomposition in cyclotomic extensions)**.** *Suppose $(m,p) = 1$ and let n denote the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$. Then $n = f$ where f is the residuce class extension degree of p in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$.*

Proof. We write $L = \mathbb{Q}(\zeta_m)$ and we let $\mathfrak{P}$ denote a prime in $\mathfrak{O}_L$ above the prime p. We have the following tower:

$$\begin{tikzcd}
L \arrow[r, dash] \arrow[d, dash] \arrow[d, dash, bend right=60, "\Gamma"'] & \mathfrak{P} \arrow[d, dash] \\
\mathbb{Q} \arrow[r, dash] & p
\end{tikzcd}$$

where $\Gamma = \mathrm{Gal}(L/\mathbb{Q})$ is abelian with $\Gamma \cong (\mathbb{Z}/m\mathbb{Z})^\times$. We set $f = f_{\mathfrak{P}}$ and our goal now is to show that $n = f$. We know that f is the order of the Frobenius element $(\mathfrak{P}, L/\mathbb{Q})$. Furthermore, before we saw that the Frobenius element depended on the choice of prime above p up to conjugation, but here, we have that

$$(\mathfrak{P}^\gamma, L/\mathbb{Q}) = \gamma^{-1}(\mathfrak{P}, L/\mathbb{Q})\gamma = (\mathfrak{P}, L/\mathbb{Q})$$

for any $\gamma \in \Gamma$ because Γ is abelian. Hence, the Frobenius element doesn't depend on the choice of $\mathfrak{P}$ above p either so the Frobenius autmomorphism is uniquely determined by the prime p so we can unambiguously write $(\mathfrak{P}, L/\mathbb{Q})$. Now, we know the Frobenius element acts as raising to the pth power on the residue fields so that we have

$$\zeta_m^{(\mathfrak{P}, L/\mathbb{Q})} \equiv \zeta_m^p \pmod{\mathfrak{P}}.$$

Raising both sides to the nth power then, we get that

$$\zeta_m^{(\mathfrak{P}, L/\mathbb{Q})^n} \equiv \zeta_m^{p^n} \equiv \zeta_m \pmod{\mathfrak{P}}$$

where the first congruence holds by definition of the Frobenius element and the second congruence holds because n is the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$. So the map $(\mathfrak{P}, L/\mathbb{Q})^n$ induces on residue fields is the identity. But recall that since p was unramified, the map $\rho : \Gamma_{\mathfrak{P}} \to \mathrm{Gal}(\ell/\mathbb{F}_p)$ is an isomorphism, in particular, injective, and so if $(\mathfrak{P}, L/\mathbb{Q})^n$ induces the identity on residue fields, we must have that $(\mathfrak{P}, L/\mathbb{Q})^n = 1$ in $\mathrm{Gal}(L/\mathbb{Q})$. Therefore, the order of $(\mathfrak{P}, L/\mathbb{Q})$ divides n and so we have $f \mid n$.

Suppose now for sake of contradiction that $f < n$. We still have the congruences

$$\zeta_m^{(\mathfrak{P}, L/\mathbb{Q})^f} \equiv \zeta_m^{p^f} \equiv \zeta_m \pmod{\mathfrak{P}}$$

by definition of the Frobenius element and as $(\mathfrak{P}, L/\mathbb{Q})$ has order f. Thus these congruences then imply that $\zeta^{p^f-1} - 1 \equiv 0 \pmod{\mathfrak{P}}$ and hence $\zeta_m^{p^f-1} - 1 \in \mathfrak{P}$. But, as $f < n$, $p^f \not\equiv 1 \pmod{m}$ and so $\zeta_m^{p^f-1} - 1$ can be chosen to be nonzero. But the only divisors of $\zeta_m^{p^f-1} - 1$ divide m by our earlier note and hence we reach a contradiction as $(m, p) = 1$. Therefore, we must indeed have that $f = n$ as desired. □

This theorem then leads to a nice proof of the law of quadratic reciprocity.

Theorem 6.9 (Quadratic reciprocity)**.** *Let p and q be distinct odd primes. Then we have*

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

Proof. Let $q^* = \left(\frac{-1}{q}\right) q$. Then first, we claim that the field $L := \mathbb{Q}(\sqrt{q^*})$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_q)$. There are at least two ways we can see this:

(1) Consider $\Gamma = \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \cong (\mathbb{Z}/q\mathbb{Z})^\times$. This group has a unique subgroup of index 2 and hence by the Galois correspondence, $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ has a unique quadratic subfield L.

Next, we ask what this subfield L is. We can identify it by noting that q is the unique prime which ramifies in L (as it's the unique prime which ramifies in $\mathbb{Q}(\zeta_q)$). Hence to determine L, we just need to determine a quadratic subfield where q is the unique prime which ramifies. This is enough then to determine that $L = \mathbb{Q}(\sqrt{q^*})$.

(2) We can also show this using Gauss sums (which are covered in the problem sheet). Namely, we can let $\chi : \Gamma \to \mathbb{C}^\times$ be the unique character of Γ of order 2. Then we consider the Gauss sum associated to χ:

$$\tau(\chi, \zeta_q) := \sum_{\gamma \in \Gamma} \chi(\gamma)\zeta_q^\gamma \in \mathbb{Q}(\zeta_q).$$

We also have that

$$\tau(\chi, \zeta_q)^2 = \left(\frac{-1}{q}\right) q = q^*$$

(by a formula for Gauss sums derived in the exercises) and hence $\mathbb{Q}(\sqrt{q^*})$ is a subfield of $\mathbb{Q}(\zeta_q)$. Thus it is indeed a quadratic subfield of $\mathbb{Q}(\zeta_q)$, and the fact that it's the unique such one follows by the same reasoning as before.

Now, we'll exploit this fact to derive the formula for quadratic reciprocity. As p is distinct from q, then p doesn't ramify in $L/\mathbb{Q}$ (by noting that p doesn't divide the discriminant of L). So as p is not ramified, it either splits or is inert in $L/\mathbb{Q}$, and we can determine which of these it is by using Kummer's criterion and reducing it to a question about the Legendre symbols. Namely, by Kummer's criterion (Theorem 4.10), p splits or is inert in $L/\mathbb{Q}$ precisely whether or not $x^2 - q^* \equiv 0 \pmod{p}$ has two distinct solutions or no solutions respectively, which happens exactly depending on if $\left(\dfrac{q^*}{p}\right) = +1$ or $\left(\dfrac{q^*}{p}\right) = -1$ respectively.

Next, we will determine another way to characterize whether p is split or inert in $L/\mathbb{Q}$. We fix a prime $\mathfrak{p} \subseteq \mathfrak{O}_L$ above p and a prime $\mathfrak{P} \subseteq \mathfrak{O}_{\mathbb{Q}(\zeta_q)}$ above $\mathfrak{p}$ so that we have the following tower:

$$\begin{tikzcd}
\mathbb{Q}(\zeta_q) \arrow[r, dash] \arrow[d, dash] \arrow[dd, dash, bend right=60, "\Gamma\cong(\mathbb{Z}/q\mathbb{Z})^\times"'] & \mathfrak{P} \arrow[d, dash] \\
L \arrow[r, dash] \arrow[d, dash] & \mathfrak{p} \arrow[d, dash] \\
\mathbb{Q} \arrow[r, dash] & p
\end{tikzcd}$$

Now by Proposition 6.7 part 2, $(\mathfrak{P}, \mathbb{Q}(\zeta_q)/\mathbb{Q})|_L = (\mathfrak{p}, L/\mathbb{Q})$. Then, p is split or inert in L according to whether the residue class extension of $\mathfrak{p}$, $f_\mathfrak{p}$ is 1 or 2 respectively (because $[L : \mathbb{Q}] = 2$ and since p is unramified). Hence, p is split or inert in L according to if $(\mathfrak{p}, L/\mathbb{Q}) = 1$ or $\neq 1$ respectively since this Frobenius element generates $\Gamma_\mathfrak{p}$ and $|\Gamma_\mathfrak{p}| = f_\mathfrak{p}$. This occurs exactly according to if p is a square or non square modulo q respectively. We can see this since if $(\mathfrak{p}, L/\mathbb{Q}) = 1$, then L is the fixed field of $\Gamma_\mathfrak{p}$ and hence $\Gamma_\mathfrak{p}$ is the unique subgroup of Γ of index 2 and hence $\Gamma_\mathfrak{p}$ is the subgroup generated by squares of elements in $(\mathbb{Z}/q\mathbb{Z})^\times$ and hence p is a square modulo q. Therefore, p is split or inert in $L/\mathbb{Q}$ precisely whether $\left(\dfrac{p}{q}\right) = +1$ or $\left(\dfrac{p}{q}\right) = -1$ respectively.

Now, comparing our two methods for characterizing whether or not p is split or inert in L, we have that

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

where the alst equality above follows by Euler's criterion. Multiplying both sides of the above by $\left(\dfrac{q}{p}\right)$, we then get the formula for quadratic reciprocity.

□

The good thing about this proof is that in some sense, it also tells us why quadratic reciprocity is true, which other methods don't. Next, we will present another proof of this same fact.

Alternative proof of Theorem 6.9. We work in $\overline{\mathbb{F}_p}$, a fixed algebraic closure of $\mathbb{F}_p$. We let η denote a qth root of unity in $\overline{F_p}$ and consider the following sum:

$$\tau := \sum_{x=1}^{q-1} \eta^x \left(\frac{x}{q}\right).$$

raising both sides to the power p and as the field has characteristic p, we get

$$\tau^p = \sum_{x=1}^{q-1} \eta^{xp} \left(\frac{x}{q}\right) = \sum_{x=1}^{q-1} \eta^{xp} \left(\frac{xp^2}{q}\right),$$

where in the first equality, we use the fact that $\left(\dfrac{x}{q}\right)^p = \left(\dfrac{x}{q}\right)$ as p is odd, and in the second equality, we use the fact that we can use the fact that since p^2 is a quadratic residue, it won't change affect whether or not x is. Next, we make the substitution $y = xp$ in this sum which then gives that

$$\tau^p = \sum_{y=1}^{q-1} \eta^y \left(\frac{y}{q}\right)\left(\frac{p}{q}\right) = \tau\left(\frac{p}{q}\right).$$

By the linear independence of characters, $\tau \neq 0$ and therefore, we can cancel out τ in the above equality, thus we have:

$$\tau^{p-1} = \left(\frac{p}{q}\right). \tag{A}$$

Next, we consider τ^2:

$$\tau^2 = \sum_{x,y} \eta^{x+y}\left(\frac{xy}{q}\right).$$

Making the substitution $y = xz$ yields:

$$\tau^2 = \sum_{x,z} \eta^{x(1+z)}\left(\frac{z}{q}\right) = \sum_{z}\left(\frac{z}{q}\right)\left[\sum_{x}\eta^{x(1+z)}\right].$$

Now, we consider the inner sum. If $z \neq -1$, $\eta^{(1+z)} \neq 1$ and hence

$$\sum_{x}\eta^{x(1+z)} = -1.$$

Hence, if we split up the sum in the formula for τ^2 to the terms where $z = -1$ and $z \neq -1$, we get

$$\tau^2 = \underbrace{\left(\frac{-1}{q}\right)(q-1)}_{z=-1} + \sum_{z\neq -1}(-1)\left(\frac{z}{q}\right).$$

But we know that $\sum_{z}\left(\frac{z}{q}\right) = 0$ and so simplifying the above, we have

$$\tau^2 = \left(\frac{-1}{q}\right)(q-1) + \left(\frac{-1}{q}\right) = \left(\frac{-1}{q}\right)q. \tag{B}$$

Using what we've derived then, we see that by (A),

$$\left(\frac{p}{q}\right) = 1 \iff \tau \in \mathbb{F}_p$$

because $\mathbb{F}_p$ is the splitting field of $x^p - x$ and by (B),

$$\tau \in \mathbb{F}_p \iff \left(\frac{q\left(\frac{-1}{q}\right)}{p}\right) = 1.$$

And so we have that

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

which, as with the first proof, is exactly quadratic reciprocity. □

There are many natural questions we could look at next. For instance, we could look at the generalized quadratic reciprocity law for totally real number fields à la Hecke, but this would require the theory of theta functions which can't be covered in the remaining two lectures. So instead, the last two lectures of the course will either cover the Dedekind zeta function or a basic introduction to class field theory.