Frobenius Elements, the Chebotarev Density Theorem, and Reciprocity

Dylan Yott

July 30, 2014

1 Motivation

Recall Dirichlet's theorem from elementary number theory.

Theorem 1.1. *For $(a, m) = 1$, there are infinitely many primes $p \equiv a \pmod{m}$.*

The point of this exposition is to present a theorem which generalizes the above result and has many applications that will help us later in the seminar. Then, as always, we will reprove quadratic reciprocity.

Suppose L/K is a (Galois) extension of number fields with Galois group G. Suppose $\mathfrak{P}$ is a prime of L lying over $\mathfrak{p}$ a prime of K. Set $\mathcal{O}_L/\mathfrak{P} = \mathbb{F}_{\mathfrak{P}}$ and $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_{\mathfrak{p}}$. Then recall the following exact sequence:

$$1 \longrightarrow I(\mathfrak{P}/\mathfrak{p}) \longrightarrow D(\mathfrak{P}/\mathfrak{p}) \longrightarrow Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}) \longrightarrow 1$$

Now we remind the reader of these objects and maps. We've defined $D(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G | \sigma(\mathfrak{P}) = (\mathfrak{P})\}$. Given an element $\sigma \in D(\mathfrak{P}/\mathfrak{p})$, this gives an automorphism of $\mathcal{O}_L$ fixing $\mathfrak{P}$, which is an automorphism of $\mathbb{F}_{\mathfrak{P}}$, and fixes $\mathbb{F}_{\mathfrak{p}}$, giving an element of $Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$. It is a standard fact from algebraic number theory that this map is surjective. Then we've chosen to define $I(\mathfrak{P}/\mathfrak{p})$ to be the kernel of this surjection. It turns out that this is equivalent to defining $I(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in D(\mathfrak{P}/\mathfrak{p})| \ \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}}, \ \forall \alpha \in \mathcal{O}_L\}$.

More importantly for us, when $\mathfrak{p}$ is unramified in L, we have $I(\mathfrak{P}/\mathfrak{p}) = 1$. This gives an isomorphism between $D(\mathfrak{P}/\mathfrak{p})$ and $Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$. It is well known that $Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ is cyclic of order $f(\mathfrak{P}/\mathfrak{p})$, and in fact has a **canonical** generator given by $x \mapsto x^{N(\mathfrak{p})}$, where $N(\mathfrak{p}) = |\mathbb{F}_{\mathfrak{p}}| := q$. Lifting this canonical generator along our isomorphism to $D(\mathfrak{P}/\mathfrak{p})$ gives an element which we call $Frob_{\mathfrak{P}}$, which is characterized by the property that $\forall \alpha \in \mathcal{O}_L$, we have $Frob_{\mathfrak{P}}(\alpha) \equiv \alpha^q \pmod{\mathfrak{p}\mathcal{O}_L}$.

Since we're interested in using these Frobenius elements to understand extensions of K in terms of the arithmetic of K, it would be a bit disappointing if these Frobenius elements depended too much on our choice of $\mathfrak{P}/\mathfrak{p}$.

Exercise 1.2. *Show that if $\mathfrak{P}$ and $\mathfrak{P}$‘ are two primes over $\mathfrak{p}$, let $\sigma \in G$ be such that $\sigma(\mathfrak{P}) = \mathfrak{P}$‘. Show $Frob_{\mathfrak{P}‘} = \sigma \circ Frob_{\mathfrak{P}} \circ \sigma^{-1}$.*

By the last exercise, when L/K is abelian, there is no dependence at all on the choice of $\mathfrak{P}$, and we can make sense of $Frob_{\mathfrak{p}}$. In fact, the decomposition groups $D(\mathfrak{P}/\mathfrak{p})$ also only depend on p, which is similarly not hard to show.

2 Examples

Consider $\mathbb{Q}(i)/\mathbb{Q}$. Here, the only ramified prime is 2. Otherwise, p splits $\iff p \equiv 1 \pmod 4$ and p is inert $\iff p \equiv 3 \pmod 4$. Since $D(\mathfrak{p})$ is trivial in the split and ramified case and is equal to G otherwise, it is clear what the Frobenius elements are. If we write $G = \{\pm 1\}$ then $Frob_p = 1$ when $p \equiv 1 \pmod 4$ and $Frob_p = -1$ otherwise. It is very useful to write $Frob_p = \left(\frac{-1}{p}\right)$.

There is a more honest and perhaps more enlightening way to see $Frob_p = \left(\frac{-1}{p}\right)$ that uses the property satisfied by Frobenius. Let $p > 2$ be prime, and suppose we want to know which element $\sigma \in G$ acts like raising to the p^{th} power modulo p. That is, which element is a lift of Frobenius? Well:

$$(a + bi)^p = a + bi^p$$

Since $i^p = \left(\frac{-1}{p}\right)$, we see that when $p \equiv 1 \pmod 4$, then $\sigma = 1$ is the right automorphism, and conversely for the other case.

Exercise 2.1. *Generalize the above to $Q(\sqrt{d})$, d squarefree.*

Now consider $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Then it is well known that the primes that ramify are precisely those dividing n. Another well known fact is that G can be canonically identified with $(\mathbb{Z}/n\mathbb{Z})^\times$, with an element m being given by the automorphism determined by $\zeta_n \mapsto \zeta_n^m$. So for $(p, n) = 1$, we want to compute $Frob_p$. It is straightforward to check that the automorphism which lifts Frobenius in this case is $p \in (\mathbb{Z}/n\mathbb{Z})^\times$. Cyclotomic fields are very nice in the sense that their ramification and Frobenius elements are very explicit, which will be very handy in what follows.

3 Quadratic Reciprocity

We can now give a very conceptual and clean proof of quadratic reciprocity.

Theorem 3.1. *For p, q distinct odd primes, we have $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.*

Proof. It is straightforward to check that this is equivalent to $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$, where $p^* = \left(\frac{-1}{p}\right)p$. Next, using either ramification theory and basic Galois theory, or using the theory of Gauss sums, we have the following tower of fields and Frobenius elements.

$$\begin{tikzcd}
Q(\zeta_p) \arrow[d, dash] \arrow[dd, dash, bend right=60, "Frob_q = q"'] \\
Q(\sqrt{p^*}) \arrow[d, dash] \arrow[d, dash, bend left=40, "Frob_q = \left(\frac{p^*}{q}\right)"] \\
\mathbb{Q}
\end{tikzcd}$$

□

If we know that $Frob_q \in (\mathbb{Z}/p\mathbb{Z})^\times$ restricts to the Frobenius element in $\{\pm 1$, then we would be done, because q restricts to $\left(\frac{q}{p}\right)$. Showing that Frobenius elements restrict correctly is not difficult since Frobenius elements were defined canonically, and as such behave in a functorial way.

4 Chebotarev Density Theorem

We can rephrase Dirichlet's theorem about primes in arithmetic progressions in terms of Frobenius elements in an obvious way.

$$p \equiv a \pmod{m} \iff Frob_p = a \in \mathbb{Z}/m\mathbb{Z}$$

Thus, proving Dirichlet's theorem comes down to understanding the distribution of Frobenius elements. As such it is natural to study the distribution of Frobenius elements for arbitrary abelian extensions, and hopefully obtain results similar to Dirichlet's theorem. This is precisely what the Chebotarev density theorem tells us.

Theorem 4.1. *For L/K an abelian extension of number fields, $Frob_{\mathfrak{p}}$ are equally distributed in $G = Gal(L/K)$.*

Remark 4.2. *The term equally distributed has a meaning which we will not make precise.*

We have created a machine that given arithmetic data of K (primes), produces elements of a galois group $G = Gal(L/K)$. Now we're going to put these Frobenius elements together to construct the Artin map. Suppose now for simplicity of expoisiton that all the primes of K are unramified in L, and that L/K is abelian as usual. Then we have the following:

$$Art_{L/K} I_K :\rightarrow Gal(L/K)$$

This map is defined by $Art_{L/K}(p) = Frob_p$ and extended to I_K by multiplicativity. By the Chebotarev density theorem, this map is surjective, and as such $I_K/Ker(Art_{L/K}) \cong Gal(L/K)$. This is interesting because the left hand side is purely arithmetic data of K

and the right is information about the extensions of K. This suggests that we might be able to understand extensions of K by studying subgroups (possible kernels of the Artin maps) of I_K. This will be covered in later lectures where we discuss Artin reciprocity. Before we finish we present a theorem.

Theorem 4.3. *For K a number field, there exists L, the maximal unramified abelian extension of K with $Ker(Art_{L/K}) = P_K$, the subgroup of principal ideals. L is called the Hilbert class field of K.*

Let K be a number field, and L its Hilbert class field. Then $C(\mathcal{O}_K) \cong Gal(L/K)$. Thus, the prime ideals of K are equally distributed in the ideal classes.

5 Proof of Dirichlet's Theorem

Rather than prove the Chebotarev density theorem, we prove Dirichlet's theorem, since the general proof of the Chebotarev density theorem ends up reducing to Dirichlet's theorem in some sense, and the ideas present in Dirichlet's theorem already demonstrate the general theory very well.

Let $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ be a character which we extend to $\mathbb{Z}$ by 0. Define an L-function as follows.

$$L(s, \chi) = \sum_n \frac{\chi(n)}{n^s}$$

For $m = 0$, and χ the trivial character we obtain $L(s, chi) = \zeta(s)$, the Riemann zeta function. For $m > 0$ and χ trivial, we get a slightly deficient Riemann zeta function $\zeta(s) \cdot \frac{1}{1-m^{-s}}$. Now we present a general fact about L-functions without proof:

Lemma 5.1. *Let $L(s, \chi) = \sum \frac{a_n}{n^s}$, and suppose $A_n = \sum_{k=1}^n a_k$ is bounded as a function of n. Then $L(s, \chi)$ converges for $Re(s) > 0$.*

The L-functions as in the above lemma arise when χ is a non-trivial character. Whenever χ is trivial, we only get convergence for $Re(s) > 1$. Now we use the Euler product for these L-functions to manipulate them into a more useful form before we proceed with the proof.

$$\begin{aligned}
L(s,\chi) &= \prod_p \frac{1}{1-\chi(p)p^{-s}} \\
log(L(s,\chi)) &= \sum_p -log(1-\chi(p)p^{-s}) \\
&= \sum_p \sum_n \frac{\chi(p)^n}{np^{ns}} \\
&= \sum_p \frac{\chi(p)}{p^s} + \sum_p \sum_{n\geq q} \frac{\chi(p)^n}{np^{ns}} \\
&= \sum_p \frac{\chi(p)}{p^s} + \beta(s,\chi)
\end{aligned}$$

The important thing is that $\beta(s,\chi)$ converges for $Re(s) > \frac{1}{2}$. Now we proceed with the proof of Dirichlet's theorem.

Theorem 5.2. *For $(a,m) = 1$, there are infinitely many primes $p \equiv a \pmod{m}$.*

Proof. Consider the following sum over the characters χ of $(\mathbb{Z}/m\mathbb{Z})^\times$:

$$\begin{aligned}
\sum_\chi \chi(a)^{-1} log(L(s,\chi)) &= \sum_\chi \chi(a)^{-1} \left(\sum_p \frac{\chi(p)}{p^s} + \beta(s,\chi) \right) && (1) \\
&= \sum_p \frac{1}{p^s} \sum_\chi \chi(pa^{-1}) + \sum_\chi \chi(a)^{-1}\beta(s,\chi) && (2) \\
&= \phi(m) \sum_{p\equiv a \pmod{m}} p^{-s} + \beta'(s,\chi) && (3)
\end{aligned}$$

In the above, $\beta'(s,\chi)$ converges at $s = 1$. To deduce the theorem we need to know that $L(1,\chi) \neq 0$ whenever χ is nontrivial. Assuming this fact for the meantime, then since $L(s,\chi_0)$ diverges for χ_0 the trivial character, we see that the LHS of (1) must diverge at $s = 1$, which says that there must be infinitely many primes $p \equiv a \pmod{m}$, and we are done. □

There are various ways of proving $L(1,\chi) \neq 0$ for $\chi \neq \chi_0$, and this fact certainly constitutes the main analytic meat of the proof. There are ways of doing this using certain techniques from analysis, as well as one using the analytic class number formula.