An instance of the Cebotarev density theorem - Postgraduate Seminar 2012

Daniel Fretwell

THANK EUGENIA AND PEOPLE FOR COMING.

One of the first theorems people ever see proved is Euclid's result...that there are infinitely many primes. This result can be rephrased as the fact that "there are infinitely many primes in any arithmetic progression of common difference 1". Many mathematicians tried to study primes in other arithmetic progressions but Dirichlet was the one to prove the general theorem. His result says:

Theorem 1. *(Dirichlet) Given any integer $n \geq 1$ and any integer a coprime to n there are infinitely many primes congruent to a mod n.*

In undergrad courses on elementary number theory you prove simple cases of this result (such as for $n = 4$ or $n = 8$) using the same rough ideas as Euclid's original proof.

Dirichlet's original proof used the theory of what are now known as *Dirichlet characters* (of $(\mathbb{Z}/n\mathbb{Z})^\times$) and their corresponding L-series. It is quite a difficult proof but beautiful...it opened many doors in modern analytic number theory.

After the work of Dirichlet, number theorists found more. In assigning a natural density to subsets of primes they were able to find that actually the primes are uniformly distributed between the classes mod n mentioned above. Roughly speaking a prime is just as likely to be congruent to 4 mod 9 as being congruent to 7 mod 9.

In this talk we discuss a more general theorem of algebraic number theory, specifically a corollary of class field theory, called the Cebotarev density theorem. At the end we will see how it specialises easily to prove Dirichlet's result.

PLAN

- 1. A few basics of algebraic number theory
- 2. Frobenius elements
- 3. Cebotarev density theorem
- 4. Application to Dirichlet's theorem

1 A few basics of algebraic number theory

Recall that a number field is a field K containing $\mathbb{Q}$ such that $[K : \mathbb{Q}]$ is finite.

Example 2. The fields $\mathbb{Q}$, $\mathbb{Q}(\sqrt{-5})$ and $\mathbb{Q}(\zeta_n)$ (where ζ_n is a primitive nth root of unity) are all number fields.

Each number field contains a special ring, its ring of integers $\mathfrak{O}_K$. This ring consists of those elements of K that satisfy a monic polynomial over $\mathbb{Z}$. This ring minics the inclusion $\mathbb{Z} \subset \mathbb{Q}$.

Example 3. The number field $K = \mathbb{Q}$ has $\mathfrak{O}_K = \mathbb{Z}$. The number field $K = \mathbb{Q}(\sqrt{-5})$ has $\mathfrak{O}_K = \mathbb{Z}[\sqrt{-5}]$. The number field $\mathbb{Q}(\zeta_n)$ has $\mathfrak{O}_K = \mathbb{Z}[\zeta_n]$.

Unfortunately $\mathfrak{O}_K$ is not always a UFD (e.g. in $\mathbb{Z}[\sqrt{-5}]$ we have $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$). However, Dedekind restored unique factorisation by looking at the *ideals* rather than the elements. He found that in $\mathfrak{O}_K$ every ideal $\mathfrak{a}$ has a unique factorisation into prime ideals:

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_1}$$

and that this factorisation is unique upto reordering of the prime ideals (this is essentially what caused the non-unique factorisation above). What is going on here is that instead of trying to factorise an element we are trying to factorise the *multiplies* of the element as an object in its own right.

We can define the *norm* of an ideal $\mathfrak{a}$ to be $N(\mathfrak{a}) = |\mathfrak{O}_K/\mathfrak{a}|$. This is always finite and is multiplicative.

Example 4. In $K = \mathbb{Q}$ we have $N(a\mathbb{Z}) = |\mathbb{Z}/a\mathbb{Z}| = |a|$ for any integer a.

What happens when we have an extension L/K of number fields?

Well we have a kind of covering. Each prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$ can be "lifted" to an ideal $\mathfrak{p}\mathfrak{O}_L$ of $\mathfrak{O}_L$. This new ideal may or may not be prime but since $\mathfrak{O}_L$ has unique factorisation of ideals we are definately guaranteed a factorisation:

$$\mathfrak{p}\mathfrak{O}_L = \mathfrak{q}_1^{e_1} \dots \mathfrak{q}_g^{e_g}.$$

It is actually quite rare to see any $e_i > 1$. When this happens we say that $\mathfrak{p}$ ramifies in L. This fits the notion of ramification in our covering analogy.

ROOM FOR EXAMPLES OF SPLITTING/RAMIFICATION.

ANY QUESTIONS?

2 Frobenius elements

From now on we assume that L/K is a *Galois extension.*

The nice thing here is that the Galois group $\mathrm{Gal}(L/K)$ acts *transitively* on the primes $\mathfrak{q}_i$ dividing $\mathfrak{p}\mathfrak{O}_L$ via $\mathfrak{q}_i \longmapsto \sigma(\mathfrak{q}_i) = \{\sigma(x) \,|\, x \in \mathfrak{q}_i\}$. This, along with unique factorisation tells us that the e_i's are all equal!

So factorisation of $\mathfrak{p}\mathfrak{O}_L$ in a Galois extension is nicer:

$$\mathfrak{p}\mathfrak{O}_L = (\mathfrak{q}_1 ... \mathfrak{q}_g)^e$$

for some $e \geq 1$. In fact $eg|[L : K]$ so that there are only finitely many possibilities for e and g.

Now that we have a group action we can construct the stabilizer subgroup for each $\mathfrak{q}_i$. We call these groups the *decomposition groups*:

$$D_{\mathfrak{q}_i/\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(L/K) \,|\, \sigma(\mathfrak{q}_i) = q_i\}.$$

These groups contain lots of information about the splitting of primes.

COMPLICATED BIT

The fact that every element of $D_{\mathfrak{q}_i/\mathfrak{p}}$ stabilizes $\mathfrak{q}_i$ tells us that we have a well-defined automorphism of fields for each $\sigma \in D_{\mathfrak{q}_i/\mathfrak{p}}$:

$$\bar{\sigma} : \mathfrak{O}_L/\mathfrak{q}_i \longrightarrow \mathfrak{O}_L/\mathfrak{q}_i,$$

defined by:

$$\bar{\sigma}(x + \mathfrak{q}_i) = \sigma(x) + \mathfrak{q}_i.$$

Further we can view $\mathfrak{O}_K/\mathfrak{p}$ as a subfield of $\mathfrak{O}_L/\mathfrak{q}_i$ and each of these automorphisms fix this subfield.

So putting all of this together, we get an homomorphism:

$$D_{\mathfrak{q}_i/\mathfrak{p}} \longrightarrow \mathrm{Gal}((\mathfrak{O}_L/\mathfrak{q}_i)/(\mathfrak{O}_K/\mathfrak{p}))$$
$$\sigma \longmapsto \bar{\sigma}$$

Non-trivial fact: This is a surjection. Actually if $\mathfrak{p}$ is unramified in L then it is an isomorphism!

But the Galois group on the right is isomorphic to a Galois group of finite fields $\mathrm{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q)$ (since both of $\mathfrak{O}_L/\mathfrak{q}_i$ and $\mathfrak{O}_K/\mathfrak{p}$ can be shown to be finite fields). Such Galois groups are cyclic, generated by the Frobenius automorphism $x \mapsto x^q$.

So what we have here is that whenever $\mathfrak{p}$ is unramified in L there must be some unique generator of $D_{\mathfrak{q}_i/\mathfrak{p}}$ that induces the Frobenius automorphism in $\mathrm{Gal}((\mathfrak{O}_L/\mathfrak{q}_i)/(\mathfrak{O}_K/\mathfrak{p}))$. This element is called the *Frobenius element* of $\mathfrak{q}_i$, denoted $\left(\frac{L/K}{\mathfrak{q}_i}\right)$ and by definition satisfies:

$$\left(\frac{L/K}{\mathfrak{q}_i}\right)(x) \equiv x^{N(\mathfrak{p})} \bmod \mathfrak{q}_i$$

for all $x \in \mathfrak{O}_L$.

END OF COMPLICATED BIT

All you have to know from this bit is that we are assigning a nice element of the Galois group to every such $\mathfrak{q}_i$ in the factorisation of $\mathfrak{p}\mathfrak{O}_L$ and such an element satisfies the above congruence. We will see an example soon.

Actually, given two prime ideals $\mathfrak{q}_i, \mathfrak{q}_j$ in the factorisation of $\mathfrak{p}$ we can relate their Frobenius elements by conjugation:

$$\left(\frac{L/K}{\mathfrak{q}_j}\right) = \sigma \left(\frac{L/K}{\mathfrak{q}_i}\right) \sigma^{-1}$$

where $\sigma \in \mathrm{Gal}(L/K)$ is such that $\sigma(\mathfrak{q}_i) = \mathfrak{q}_j$ (this σ exists by transitivity of the action!).

Note: If $\mathrm{Gal}(L/K)$ is abelian (i.e. L/K is an abelian extension) then all of the Frobenius elements are equal! In this case the Frobenius element is really something "belonging to $\mathfrak{p}$" and so we may denote it as $\left(\frac{L/K}{\mathfrak{p}}\right)$.

ANY QUESTIONS?

3 Cebotarev density theorem

We are now going to see that the Frobenius elements have a nice distribution inside of the Galois group. Cebotarev found that we learn quite a lot about unramified prime ideals by studying their Frobenius elements. We only state the theorem in abelian Galois extensions of number fields, but there is a more general version of the theorem for any Galois extension of number fields.

Theorem 5. *(Cebotarev) Let L/K be an abelian Galois extension of number fields and pick any $\sigma \in Gal(L/K)$. Then $\sigma = \left(\frac{L/K}{\mathfrak{p}}\right)$ for infinitely many prime ideals $\mathfrak{p}$ of $\mathfrak{O}_K$ that are unramified in L. (Further the Dirichlet density of this set of prime ideals is $\frac{1}{[L:K]}$)*

So this theorem is basically telling us that the Frobenius elements, whenever they are well-defined, are distributed uniformly over the whole of the Galois group. The proof of the Cebotarev density theorem is itself quite complicated and relies on heavy machinery from class field theory. It is quite a handy result to have as we will now see.

ANY QUESTIONS?

4 Application to Dirichlet's theorem

In order to see how Dirichlet's theorem follows from the Cebotarev density theorem we are going to take $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_n)$ for some primitive nth root of unity ζ_n.

Well known facts:

- $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$
- $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a Galois extension thus $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ (which is abelian). The isomorphism is via:
$$(\sigma_a : \zeta_n \mapsto \zeta_n^a) \longmapsto \bar{a}.$$
- The primes of $\mathfrak{O}_K = \mathbb{Z}$ that ramify in $\mathbb{Q}(\zeta_n)$ are exactly the ones dividing n.

Let's fix an $a \in \mathbb{Z}$ such that a is coprime to n. Then we have a corresponding $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

The Cebotarev density theorem now tells us that $\sigma_a = \left(\frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{p\mathbb{Z}}\right)$ for infinitely many primes $p \in \mathbb{Z}$ (ignoring ones that divide n since they ramify).

But what exactly are the Frobenius elements here?

We know that for such primes p they satisfy:
$$\left(\frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{p\mathbb{Z}}\right)(x) \equiv x^{N(p\mathbb{Z})} \equiv x^{|\mathbb{Z}/p\mathbb{Z}|} \equiv x^p \bmod \mathfrak{q},$$
for all $x \in \mathfrak{O}_L = \mathbb{Z}[\zeta_n]$, where $\mathfrak{q}$ is just some prime ideal in $\mathfrak{O}_L$ that appears in the factorisation of $p\mathfrak{O}_L$.

We can see that when $x = \zeta_n$ the Frobenius element satisfies:
$$\left(\frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{p\mathbb{Z}}\right)(\zeta_n) \equiv \zeta_n^p \bmod \mathfrak{q}.$$

Now the LHS is the action of an element of the Galois group on ζ_n, so must be some other primitive nth root of unity. However it turns out that the primitive nth roots of unity are distinct mod $\mathfrak{q}$ (the polynomial $x^n - 1$ is separable mod p) so that really the congruence is an equality. Hence the Frobenius element of p really is σ_p.

So now we know that $\sigma_a = \sigma_p$ for infinitely many primes. Since σ_a matters only upto congruence mod n we find that this is the same as saying that there are infinitely many primes $p \equiv a \bmod n$. This concludes the proof.

Actually we get a little extra knowledge from the Cebotarev density theorem. It tells us that the primes are distributed evenly over all classes of $(\mathbb{Z}/n\mathbb{Z})^\times$.