MATH 6370, LECTURE 5
MARCH 27

GORDAN SAVIN

Let ℓ be a prime, and a an integer prime to ℓ. Let S be the set of primes $p \equiv a \pmod{\ell}$. We shall apply results from the previous two lectures to prove that S has Dirichlet density $1/(\ell-1)$. Recall that the Dirichlet density is the limit

$$\delta(S) := \lim_{s\to 1^+} \frac{\sum_{p\in S} \frac{1}{p^s}}{\sum_{p\in X} \frac{1}{p^s}},$$

if it exists, where X is the set of all primes. Consider a as an element of the abelian group $G = (\mathbb{Z}/\ell\mathbb{Z})^\times$. Let $\delta_a : G \to \mathbb{C}$ be the characteristic function of a, that is,

$$\delta_a(b) = \begin{cases} 1 \text{ if } a = b \\ 0 \text{ otherwise.} \end{cases}$$

We can view δ_a as a periodic function on $\mathbb{Z}$, by defining $\delta_a(n) = 0$ for all n divisible by 0. In this way the above formula can be rewritten as

$$\delta(S) = \lim_{s\to 1^+} \frac{\sum_{p\in X} \frac{\delta_a(p)}{p^s}}{\sum_{p\in X} \frac{1}{p^s}}$$

We shall now apply the Fourier transform to express δ_a as a linear combination of characters of G. Recall that

$$\delta_a = \sum_{\chi\in\hat{G}} \hat{\delta}_a(\chi)\cdot\chi$$

where

$$\hat{\delta}_a(\chi) = \frac{1}{|G|}\sum_{x\in G} \delta_a(x)\bar{\chi}(x) = \frac{1}{\ell-1}\bar{\chi}(a).$$

Thus

$$\delta_a = \frac{1}{\ell-1}\sum_{\chi\in\hat{G}} \bar{\chi}(a)\cdot\chi$$

and we can write

$$\sum_{p\in X} \frac{\delta_a(p)}{p^s} = \frac{1}{\ell-1}\sum_{\chi\in\hat{G}} \bar{\chi}(a)\sum_{p\in X}\frac{\chi(p)}{p^s}.$$

If $\chi \neq 1$ then we proved that

$$\lim_{s\to 1^+} \frac{\sum_{p\in X} \frac{\chi(p)}{p^s}}{\sum_{p\in X} \frac{1}{p^s}} = 0,$$

hence $\delta(S) = 1/(\ell-1)$.

We now discuss relationship with splitting of primes in cyclotomic extensions. Working generally, let F be a Galois extension of $\mathbb{Q}$ of degree n. Let A be the ring of integers. Let p be an unramified prime. Then we have a factorization $Ap = P_1 \cdot \ldots \cdot P_g$, where these primes are mutually different. Let P one of these primes. Then A/P is a degree f extension of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ where $n = fg$. Recall that the decomposition group $D_P \subset G$ consists of all $\sigma \in G$ such that $\sigma(P) = P$. In particular D_P acts naturally on A/P. In fact we have proved that the natural action gives an isomorphism

$$D_P \cong \mathrm{Gal}(A/P).$$

The Galois group $\mathrm{Gal}(A/P)$ is a cyclic group of order f, generated by the Frobenius element, raising to the p-th power. In view of the isomorphism there exists a unique element $\mathrm{Fr}_P \in D_P$ such that

$$\mathrm{Fr}_P(x) \equiv x^p \pmod{P}$$

for all $x \in A$. Since G acts transitively on the primes $P_1, \ldots, P_g$,

$$\mathrm{Fr}_p = \{\mathrm{Fr}_{P_1}, \ldots, \mathrm{Fr}_{P_g}\}$$

is a conjugacy class in G, the Frobenius class of p. If G is abelian, every conjugacy class is a singleton, hence we have a proper (Frobenius) element Fr_p in G.

Let's work this out for the case $F = \mathbb{Q}(\omega)$ where ω is ℓ-th root of 1. Then $G \cong (\mathbb{Z}/\ell\mathbb{Z})^\times$ where $a \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ gives $\sigma_a \in G$ defined by $\sigma_a(\omega) = \omega^a$. All primes $p \neq \ell$ are unramified, and it is clear that $\mathrm{Fr}_p = \sigma_p$. Thus, if we fix σ, which is the same as fixing a, then the set S of primes $p \neq \ell$ such that $\mathrm{Fr}_p = \sigma$ is the same as the set of primes $p \equiv a \pmod{\ell}$. In particular, S has Dirichlet density $1/(\ell - 1)$. This is a special case of the Čebotarev density theorem:

Theorem 0.1. *Let F be a Galois extension of $\mathbb{Q}$ with (finite) Galos group G. Fix a conjugacy class $\mathcal{C} \subset G$. Let S be the set of unramified primes such that the Frobenius class is $\mathcal{C}$. Then*

$$\delta(S) = \frac{|\mathcal{C}|}{|G|}.$$

Recall that we have proved the above theorem for the class $\{1\}$, that is, the density of primes that split completely is $1/|G|$.

Exercise. Let F be a degree 6 Galois extension of $\mathbb{Q}$ with the Galois group S_3, the group of permutations of three letters. Prove Čebotarev density theorem for F, using that the density of primes that split completely in F is $1/6$ and in the intermediate quadratic extension K is $1/2$.