Lecture 2: The Chebotarev Density Theorem

1. Artin L-series. Yesterday, we looked at the following context:

K/k a finite Galois extension of algebraic number fields.

$\mathrm{Gal}(K/k) = G$. Let $\rho : G \to Gl(V)$ be a complex linear representation. For each prime ideal $\mathfrak{p}$ of k, we looked at the set of prime ideals $\mathfrak{P}$ of K that lie above $\mathfrak{p}$. We noted that G acts transitively on the $\mathfrak{P}$'s above $\mathfrak{p}$.

We defined the decomposition group $D_{\mathfrak{P}} = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\}$ and the inertia group

$$I_{\mathfrak{P}} = \{\sigma \in G : \sigma(x) \equiv x \pmod{\mathfrak{P}} \ \forall x \in \mathcal{O}_K\}$$

We noted that $D_{\mathfrak{P}}/I_{\mathfrak{P}} \underset{\text{can.}}{\simeq} \mathrm{Gal}((\mathcal{O}_K/\mathfrak{P})/(\mathcal{O}_k/\mathfrak{p}))$

and there is a $\sigma_{\mathfrak{P}} \in D_{\mathfrak{P}}$ (unique mod $I_{\mathfrak{P}}$) such that

$$\sigma_{\mathfrak{P}}(x) \equiv x^{N\mathfrak{p}} \pmod{\mathfrak{P}} \quad \forall x \in \mathcal{O}_K.$$

As we range over the $\sigma_{\mathfrak{P}} : \mathfrak{P} \mid \mathfrak{p}$, we get a conjugacy class of G. This conjugacy class is defined to be the Artin symbol $\sigma_{\mathfrak{p}}$ (well defined for all unramified $\mathfrak{p}$).

Examples: ① $K = \mathbb{Q}(\sqrt{D})$, $k = \mathbb{Q}$ $\quad \mathrm{Gal}(K/k) \simeq \{\pm 1\}$

$$\sigma_p = \left(\frac{D}{p}\right) \quad \text{for } p \nmid D.$$

② $K = \mathbb{Q}(\zeta_q)$ $\quad k = \mathbb{Q}$. $\quad \mathrm{Gal}(K/k) = (\mathbb{Z}/q\mathbb{Z})^*$

$$\mathrm{Fix}\ (a,q) = 1 \longleftrightarrow \tau_a(\zeta_q) = \zeta_q^a$$

What is the artin symbol? $\sigma_p = \tau_a$ if $p \equiv a \pmod{q}$.

The Chebotarev density theorem says that the assignment $\mathfrak{p} \mapsto \sigma_{\mathfrak{p}}$ fills up all the conjugacy classes with the expected probability.

and

$$\#\{\mathfrak{p} : N\mathfrak{p} \le x : \sigma_{\mathfrak{p}} = C\} \sim \frac{|C|}{|G|}\pi(x)$$

Thus, the Chebotarev density theorem is a generalization of the Dirichlet's theorem about primes in arithmetic progressions.

Let us note one special situation. In any group, the identity element forms a special class by itself. What does it mean that $\sigma_{\mathfrak{P}} = 1$?

It means that $\sigma_{\mathfrak{P}} = 1 \quad \forall\, \mathfrak{P} \mid \mathfrak{p}$. In other words, the set $\{\sigma(\mathfrak{P}) : \sigma \in G\}$ is a distinct collection of prime ideals. In other words,

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1 \cdots \mathfrak{P}_g \qquad g = |G|.$$

That is, $\mathfrak{p}$ splits completely in K. Conversely, if $\mathfrak{p}$ splits completely in K, then $\sigma_{\mathfrak{P}} = 1$.

So, the Chebotarev density theorem tells us how often $\mathfrak{p}$ splits completely in K. It is $1/[K:k]$ of the time.

2. A more concrete look at the Chebotarev density theorem:

Let us recall Dedekind's theorem. Suppose that K is an algebraic number field with $K = \mathbb{Q}(\theta)$, and $f(x) \in \mathbb{Z}[x]$ is the minimal poly of K.

~~Assume for the moment that $K/\mathbb{Q}$ is a Galois extension.~~
For any prime $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$, we have

$$f(x) \equiv f_1(x)^{e_1} \cdots f_g(x)^{e_g} \pmod{p} \qquad f_i(x) \text{ irred.}$$

Then $p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ $\qquad \mathfrak{P}_i = (p, f_i(\theta))$.
also $N\mathfrak{P}_i = p^{\deg f_i}$

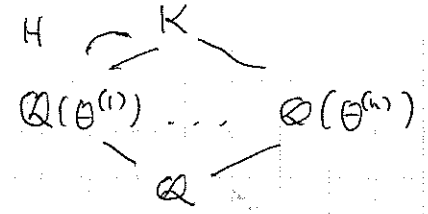
What does it mean that $f(x)$ has a root (mod p) ?
It means that there is a prime ideal $\mathfrak{P}$ above p with $N\mathfrak{P} = p$, i.e. a prime ideal of degree 1.

If $K/\mathbb{Q}$ is Galois, then if $\mathfrak{P} \mid p$, and $\mathfrak{P}$ has degree d, then $\sigma(\mathfrak{P})$ also has degree d $\forall \sigma \in Gal(K/\mathbb{Q})$. In other words, in the Galois setting, $\deg f_i$ is the same in the factorization. In particular, if $f(x)$ has one root (mod p), it has all roots mod p, and it splits completely as a product of linear factors.

Applied to our context, it means that (in the Galois setting) $f(x)$ factors completely (mod p) $\Leftrightarrow$ $f(x)$ has a root (mod p) $\Leftrightarrow$ p splits completely in K (for p unramified in K). Thus, if $f(x)$ is a "Galois" polynomial then the probability that $f(x)$ (mod p) has a root is $1/[K:\mathbb{Q}]$.

What if $f(x)$ is <u>not</u> a "Galois" polynomial?

Let us look at the normal closure of $\mathbb{Q}(\theta)$.



$$X = \bigcup_{g \in G} g H g^{-1}$$

The probability that $f(x)$ (mod p) has a root is $|X|/|G|$.

Exercise: if $f(x)$ is irreducible and <u>not</u> linear /$\mathbb{Q}$ then the prob. $f(x)$ mod p has a root is < 1. In other words, if $f(x)$ is irreducible ~~(mod p)~~ /$\mathbb{Q}$ then there are inf. many primes p for which $f(x)$ (mod p) has <u>no root</u>.

This gives us an ~~idea~~ algorithm to determine the irreducibility of a given polynomial /$\mathbb{Q}$. We look at it (mod p) and if for ~~some~~ every prime $p \nmid D(f)$, we have $f(x)$ (mod p) has ~~no root~~ a root, then f is reducible. We may want an effectively computable bound to ensure ~~that only a~~ the finite amount of time needed to run the algorithm.

Lecture 2 (page 4)

The Prime ideal theorem.

$$\#\{\mathfrak{p} : N\mathfrak{p} \le x\} \sim \pi(x).$$

Concrete formulation: let $f(x) \in \mathbb{Z}[x]$ be irreducible. For each prime p, let

$$\nu_f(p) = \#\text{ roots of } f(x) \pmod p.$$

Then $$\sum_{p \le x} \nu_f(p) \sim x/\log x.$$

3. Applications to Artin's primitive root Conjecture.

2 is a primitive root $\pmod p$ $\iff$ $2^{(p-1)/q} \not\equiv 1 \pmod p$ $\forall\, q \mid p-1$.

$\iff$ p does not split completely in $\mathbb{Q}(\zeta_q, \sqrt{q}/2)$.

The probability is $= \prod_q \left(1 - \frac{1}{q(q-1)}\right)$.

An application of the principle of inclusion–exclusion requires explicit error terms.

4. Effective versions of the Chebotarev density theorem

Three versions:

① unconditional — Lagarias Odlyzko

② assuming GRH for Dedekind zeta functions — Lagarias Odlyzko

③ assuming GRH + Artin's hol. conjecture — Murty-Murty Saradha

$\exists$ an absolute constants c_1, c_2 (effectively determinable) so that

$$\left|\#\{\mathfrak{p} : N\mathfrak{p} \le x : \sigma_{\mathfrak{p}}(\mathcal{L}/\mathbb{Q}) = C\} - \frac{|C|}{|G|} \operatorname{li} x\right| \le \frac{|C|}{|G|} \operatorname{li} x^{\beta} + O\left(|C| x \exp\left(-c_1 \sqrt{\frac{\log x}{[K:\mathbb{Q}]}}\right)\right)$$

provided

$$\log x > c_2 [K:\mathbb{Q}] (\log |d_K|)^2.$$

Here β is the possible simple zero in the region $\left[1 - \frac{1}{\log |d_K|}, 1\right]$ of $\zeta_K(s)$.

Lecture 2 (page 5)

$$\log M(K/k) = \sum_{\substack{p \text{ ram} \\ \text{in } K}} \log p + \frac{\log |d_k|}{[k:\mathbb{Q}]} + \log [K:\mathbb{Q}]$$

(2) Assuming GRH. (Lagarias-Odlyzko, Serre)

$$\left| \pi_C(x) - \frac{|C|}{|G|} \operatorname{li} x \right| \leq c_3 \frac{|C|}{|G|} x^{1/2} (\log |d_K| + [K:\mathbb{Q}] \log x)$$

$$\leq c_4 |C| x^{1/2} (\log M(K/k) + \log x)$$

(3) Assuming GRH & AC.

$$\left| \pi_C(x) - \frac{|C|}{|G|} \operatorname{li} x \right| \leq c_4 |C|^{1/2} (\log M(K/k) + \log x)$$

5. The relationship of Artin's conjecture & GRH

$$\zeta_K(s) = L(s, \chi_{reg}, K/k)$$

$$\chi_{reg} = \sum_{\chi} \chi(1)\chi \quad \Rightarrow \quad \zeta_K(s) = \prod_{\chi} L(s, \chi, K/k)^{\chi(1)}$$

$$L(s, 1, K/k) = \zeta_k(s).$$

Dedekind's Conjecture. For any number field K/k (not nec Galois)

$$\zeta_K(s) / \zeta_k(s) \quad \text{is entire.}$$

Dedekind's Conjecture is known if K/k is Galois.
In general Artin conj $\Rightarrow$ Dedekind conj.

To study zeros & possible poles of Artin L-series:
Let us introduce the Heilbronn-Stark character: fix $s_0 \in \mathbb{C}$.

Θ_G with $G = Gal(K/k)$, put

$$\Theta_G(g) = \sum_{\chi} n(\chi, s_0) \chi(g) \qquad n(\chi, s_0) \in \mathbb{Z} \text{ (Brauer)}$$

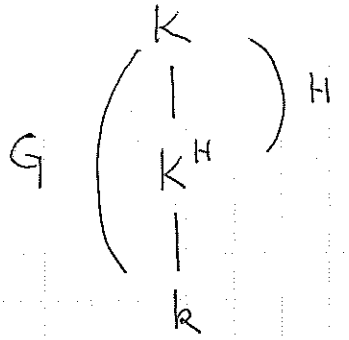
$$n(\chi, s_0) \geq 0 \text{ (Artin conj)}$$

Recall: Frobenius reciprocity.

$$(\operatorname{Ind}_H^G \psi, \chi)_G = (\psi, \chi|_H).$$

Lecture 2 (page 6)

$$\theta_H(g) = \sum_{\psi} n(\psi, s_0)\,\psi(1)$$



$$\zeta_K(s) = L(s, \chi_{reg}, K/k) = \prod_{\chi} L(s, \chi, K/k)^{\chi(1)}$$

$$\text{ord}_{s_0} n(s, \chi_{reg}) = \sum_{\chi} \chi(1)\, n(s_0, \chi)$$

Lemma (Heilbronn) $\quad \theta_G|_H = \theta_H$

Proof.

$$\theta_G|_H = \sum_{\chi} n(\chi, s_0)\,\chi|_H$$

$$= \sum_{\chi} n(\chi, s_0) \left(\sum_{\psi} (\chi|_H, \psi)\,\psi \right)$$

$$= \sum_{\psi} \psi \left(\sum_{\chi} n(\chi, s_0)\,(\chi|_H, \psi) \right)$$

$$= \sum_{\psi} \psi \cdot \left(\sum_{\chi} n(\chi, s_0)\,(\chi, \text{Ind}_H^G \psi) \right) \quad \text{(Frobenius recip.)}$$

But $\quad L(s, \text{Ind}_H^G \psi, K/k) = \prod_{\chi} L(s, \chi, K/k)^{(\chi, \text{Ind}_H^G \psi)}$

$$= L(s, \psi, K/K^H)$$

Thus $\quad \theta_G|_H = \sum_{\psi} n(\psi, s_0)\,\psi = \theta_H.$

Theorem. $\quad \sum_{\chi} n(\chi, s_0)^2 \le n(\chi_{reg}, s_0)^2$

Proof.

$$(\theta_G, \theta_G) = \sum_{\chi} n(\chi, s_0)^2 = \frac{1}{|G|} \sum_{g \in G} |\theta_G(g)|^2$$

$$= \frac{1}{|G|} \sum_{g \in G} |\theta_{\langle g \rangle}(g)|^2 \qquad \text{(by Heilbronn's lemma)}$$

$$= \frac{1}{|G|} \sum_{g \in G} \left| \sum_{\psi} n(\psi, s_0)\,\psi(g) \right|^2 \le \frac{1}{|G|} \cdot \sum_{g \in G} \underbrace{\left(\sum_{\psi} |n(\psi, s_0)| \right)^2}_{n(\chi_{reg}, s_0)^2}$$

$$\le n(\chi_{reg}, s_0)^2.$$

Corollary 1. GRH $\Rightarrow$ Artin L-series are analytic for $\mathrm{Re}(s) > 1/2$.

Thus, all the poles (if any) lie on $\mathrm{Re}(s) = 1/2$.

Corollary 2. If $\zeta_K(s)$ is analytic and non-zero at $s = s_0$, then all artin L-series are analytic at $s = s_0$.

In particular, $\zeta_K(1+it) \neq 0$ (Hadamard de la Vallée Poussin)

$\Rightarrow$ $L(1+it, \chi, K/k) \neq 0$ $\Rightarrow$ Chebotarev.

If $\zeta_K(s)$ has a simple zero at $s = s_0$, then any artin L-series is analytic ~~there and non-vanishing.~~

Proof. $n(\chi_{reg}, s_0) = 1$. Thus

$$\sum_{\chi} n(\chi, s_0)^2 \leq n(\chi_{reg}, s_0)^2 = 1.$$

$\Rightarrow$ at most one χ exists so that $n(\chi, s_0) \neq \pm 1$

Look at $$\zeta_K(s) = \prod_{\chi} L(s, \chi, K/k)^{\chi(1)}$$

at $s = s_0$. LHS has a simple zero. RHS has only one factor that contributes. This cannot be a pole. $\Rightarrow \chi(1) = 1$.

$\Rightarrow \chi$ is abelian.

(Foote - Murty) If K/k is Galois (finite) of odd degree and $n(\chi_{reg}, s_0) \leq 3$ then all artin L-series are analytic at $s = s_0$.