Math 80550 Algebraic Number Theory
Lecture 37

Notes by Erin Bela

April 30, 2014

1 April 23, 2014 - Function Fields and Hecke Theory

Hecke Theory is a fancy way of saying L-functions and their functional equations. Let $K = \mathbb{F}_q$ where $q = p^r$, C a smooth projective curve over K, and $C(\bar{K}) = \{\text{all points on } C \text{ with coefficients in } \bar{K}\}$. We defined,

$$\mathrm{Div}(C) = \bigoplus_{P \in C(\bar{K})} [P] \cdot \mathbb{Z}$$

Let $\mathrm{Div}(C/K)$ be the abelian subgroup of $\mathrm{Div}(C)$ defined by

$$\left\{ \sum n_P \cdot [P] \,|\, P \in C(\bar{K}) \text{ such that } n_P \text{ are all equal if } P \text{ varies in } G_{\bar{K}/K}\text{-orbit} \right\}$$

Example Let $C = \mathbb{P}^1$, $p \equiv 3 \mod 4$, $\sqrt{-1} \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$. Then $[\sqrt{-1} : 1] \in \mathrm{Div}(\mathbb{P}^1)$. We have,

$$\underset{[P]}{[\sqrt{-1} : 1]} \underset{+}{+} \underset{[\bar{P}]}{[-\sqrt{-1} : 1]} \in \mathrm{Div}(\mathbb{P}^1/\mathbb{F}_p).$$

Also, have

$$[1 : 1] + 2\left([\sqrt{1} : 1] + [-\sqrt{1} : 1]\right) \in \mathrm{Div}(\mathbb{P}^1/\mathbb{F}_p).$$

Idea: We have a correspondence

$$\begin{aligned} \mathrm{Div}(C/K) &\leftrightarrow \text{ fractional ideals in } K(C) \\ \sum n_P \cdot [P] &\mapsto \prod \mathfrak{m}_P^{n_P} \end{aligned}$$

Get,

$$\prod_{P/Gal.\,conjugacy} \left(\prod_{Q \in P-\text{ Galois orbit}} m_Q \right)^{n_P}.$$

We define:

$$\begin{gathered} \deg : \mathrm{Div}(C/K) \to \mathbb{Z} \\ \mathrm{Div}^0(C/K) = \ker(\deg). \end{gathered}$$

Remark: If $f \in K(C)$, then $div(f) \in \mathrm{Div}(C/K)$. (Why? If $\sigma \in Gal(\bar{K}/K)$, then $\sigma(f) = f$ because $f \in K(C)$. Then

$$\underset{\sum n_{\sigma(P)}[P]=\sum n_P[\sigma(P)]}{\underset{||}{\sigma(div(f))}} = div(\sigma(f)) = \underset{\sum n_P[P]}{\underset{||}{div(f)}}.$$

Definition We define:

$$Pic(C/K) = Div(C/K)/div(K(C))^x$$
$$\underset{\text{class group}}{Cl(C)} \to \mathrm{Pic}^0(C/K) = \mathrm{Div}^0(C/K)/div(K(C))^x$$

Proposition 1.1 *If $D \in \mathrm{Div}(C)$, define $||D|| = q^{\deg D}$.*

1. *There exists $D \in \mathrm{Div}(C/K)$ with $\deg(D) = 1$,*
2. *$\#\{D \in \mathrm{Div}(C/K), ||D|| \le n\} < \infty$,*
3. *$\mathrm{Pic}^0(C/K)$ is finite. $h_C = \#\,\mathrm{Pic}(C/K)$ (class number).*

Proof (1) Non-trivial. If $C(K)$ has a point P, $D = [P] \in \mathrm{Div}(C/K)$. Otherwise, if $C(K) = \emptyset$, then D of degree 1 would have to have positive and negative coefficients. Proof omitted.

(2) $\#\{D \in \mathrm{Div}(C/K), ||D|| \le n\} < \infty \iff \#\left\{D \ge 0 \in \mathrm{Div}(C/K) \text{ s.t. } \deg D < \log_q(n)\right\}$ is bounded for $P \in C(\bar{K})$. $P \in C(\mathbb{F}_{q^r})$ but not in any smaller field. Define

$$a_P := r = \#\left\{\sigma(P) \,|\, \sigma \in G_{\bar{K}/K}\right\}.$$

Then

$$\deg D = \sum_{\substack{P \text{ up to} \\ \text{Galois action}}} n_P \cdot a_P \qquad (D \in \mathrm{Div}(C/K))$$

$C(\mathbb{F}_{q^r})$ is finite. e.g. $C \subset \mathbb{P}^{\mathbb{N}}$, $C(\mathbb{F}_{q^r}) \subset \mathbb{P}^N_{\mathbb{F}_{q^r}}$ where $\mathbb{P}^N_{\mathbb{F}_{q^r}}$ has size $q^{r(N+1)-1}$.

Now, $\deg D = \sum n_P \cdot a_P < m = \log_q(n)$ implies $a_P \le n$ for all P appearing in D. Thus $P \in C(\mathbb{F}_q^{a_P})$ is finite. So all P appearing in $D_{\ge 0} \in \mathrm{Div}(C/K)$ must be among finitely many possibilities $C(\mathbb{F}_q) \cup C(\mathbb{F}_{q^2}) \cup \cdots \cup C(\mathbb{F}_{q^m})$. So,

$$D \subset \left\{\sum n_P[P] \,|\, P \in \bigcup_{i=1}^{m} \subset C(\mathbb{F}_{q^i})\right\} \qquad (n_P \ge 0)$$
$$\deg D = \sum n_P a_P \le m$$
$$\implies n_P \le m$$

and there are finitely many such D.

(3) $\mathrm{Pic}^0(C/K)$ has size $h_C < \infty$. Pick $u \in \mathrm{Div}(C/K)$ with $\deg(u) = 1$. Pick $D \in \mathrm{Pic}^0(C/K)$, $n \gg 2g-2$. Recall from Riemann Roch,

$$\deg(D + nu) = n \gg 2g - 2$$
$$\dim_{\bar{K}} \mathscr{L}(D + nu) = n - g + 1$$

Can pick $f \in \mathscr{L}(D + nu)$, $f \in K(C)^x$ such that $div(f) \ge -(D + nu)$. $A = div(f) + D + nu \ge 0$, $\deg(A) = n$, so there are finitely many choices for A. Then $D = A - div(f) - nu$ and the image of D in $\mathrm{Pic}^0(C/K)$ is $A - n \cdot u$ (finitely many choices for A and $n \cdot u$ is fixed). So $\mathrm{Pic}^0(C/K)$ is finite.

We have a correspondence

$$\mathrm{Div}(C/K) \leftrightarrow \text{ideals}$$
$$\mathrm{Pic}^0(C/K) \leftrightarrow \text{class group}$$

Definition

$$\zeta_C(s) := \sum_{\substack{D\in \mathrm{Div}(C/K)\\ D\geq 0}} \frac{1}{||D||^s} = \sum_{\substack{D\in \mathrm{Div}(C/K)\\ D\geq 0}} q^{-(\deg D)\cdot s}$$

Remark: S a finite set of points of $C(\bar{K})$, $\mathcal{O}_S$ is a Dedekind domain.

$$\zeta_{\mathcal{O}_S}(s) = \zeta_C(s) = \prod_{P\in S}\left(1 - \frac{1}{q^{a_P\cdot s}}\right)$$

Theorem 1.2 *(1) Functional equation:*

$$\zeta_C(s) = \frac{P(q^{-s})}{(1-q^{-s})(1-q^{1-s})}$$

where $P(z)\in\mathbb{Z}[z]$ of degree $2g$. $P(z)$ satisfied $P(z) = q^g z^{2g} P(\frac{1}{qz})$.

(2) (Analytic Class Number Formula) $P(0) = 1$, $P(1) = h_C$, where h_C is the class number of the curve. From this and (1) *we immediately get*

$$\lim_{s\to 0} s\,\zeta_C(s) = \frac{h_C}{(q-1)\log(q)}.$$

(3) (Riemann Hypothesis) All roots of $P(z)$ have $|\alpha| = \sqrt{q}$ (hard except for elliptic curves).

In general, if X is a smooth projective variety of $\dim d$

$$\zeta_X(s) = \frac{P_1(q^{-s})P_3(q^{-s})\cdots P_{2d-1}(q^{-s})}{P_0(q^{-s})P_2(q^{-s})\cdots P_{2d}(q^{-s})}.$$

$P_i(z)$ has roots of $|\alpha| = \sqrt{q}^i$. (HARD)

Say $E/\mathbb{F}_q$ is an elliptic curve. Then $a = \#E(\mathbb{F}_q) - q - 1$.

$$\zeta_E(s) = \frac{1 - a_q^{-s} + q^{1-2s}}{(1-q^{-s})(1-q^{1-s})}$$

We'll show $|a| < 2\sqrt{q}$. $P(z) = 1 - az + qz^2$, $a^2 - 2q < 0$ so P has complex roots. So same $|\alpha| = |\beta| = \sqrt{q}$.