# Math 649 (L-Function Seminar) Notes

Krystin Manguba-Glover
University of Hawaii

Fall 2016

# October 3 (Allan)

## Dedekind Zeta Function

Let $K$ be a number field (i.e. a finite extension over $\mathbb{Q}$)
Let $\mathcal{O}_K$ be the ring of algebraic integers in $K$
When $K=\mathbb{Q}(\sqrt{m})$, $\mathcal{O}_K=\begin{cases}\mathbb{Z}[\sqrt{m}] & , m\equiv 2 \text{ or } 3 \pmod 4\\ \mathbb{Z}[\frac{1+\sqrt{m}}{2}] & , m\equiv 1 \pmod 4\end{cases}$

Example: $m=-1$, $\mathcal{O}_K=\mathbb{Z}[\sqrt{-1}]=\mathbb{Z}[i]$
$m=-5$, $\mathcal{O}_K=\mathbb{Z}[\sqrt{-5}]$, $6=2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5})$

$\mathcal{O}_K$ is always a Dedekind domain $\Rightarrow$ every ideal is factored uniquely into a product of prime ideals

Let $\sigma_1,\sigma_2,\dots,\sigma_n$ be embeddings of $K$ in $\mathbb{C}$, where $n=[K:\mathbb{Q}]$
For $\alpha\in K$, define $N_{\mathbb{Q}}^{K}(\alpha)=\sigma_1(\alpha)\sigma_2(\alpha)\cdots\sigma_n(\alpha)$

Facts:
1) $N_{\mathbb{Q}}^{K}(\alpha)$ is rational. If $\alpha\in\mathcal{O}_K$, then $N_{\mathbb{Q}}^{K}(\alpha)$ is an integer
2) $N_{\mathbb{Q}}^{K}$ is multiplicative
3) If $\alpha\in\mathcal{O}_K$, $N_{\mathbb{Q}}^{K}(\alpha)=\pm 1$ iff $\alpha$ is a unit
4) If $N_{\mathbb{Q}}^{K}(\alpha)$ is a prime number (so $\alpha\in\mathcal{O}_K$), then $\alpha$ is irreducible

For any $n$-tuple of elements $\alpha_1,\alpha_2,\dots,\alpha_n\in K$, define the discriminant of $\alpha_1,\alpha_2,\dots,\alpha_n$ to be
$\text{disc}(\alpha_1,\alpha_2,\dots,\alpha_n)=|\sigma_i(\alpha_j)|^2$

1. $\mathcal{O}_K$ is a free abelian group of finite rank $n\Rightarrow$ $\mathcal{O}_K$ has a basis over $\mathbb{Z}$ and we call this basis an integral basis

$\text{disc}(K)=\text{disc}(\text{an integral basis of } \mathcal{O}_K)$

Let $I$ be an ideal of $\mathcal{O}_K$. Define the norm of $I$ by $N(I)=|\mathcal{O}_K/I|$ ($N(I)$ is finite)

Claim: $N(I)$ is well-defined
Proof: Let $\alpha\in I$, $\alpha\neq 0$ and let $0\neq m=N_{\mathbb{Q}}^{K}(\alpha)$. wts $m\in I$.
$m=\alpha\cdot\beta\Rightarrow\beta=\frac{m}{\alpha}\in K$. $\beta$ is an algebraic integer $\Rightarrow\beta\in\mathcal{O}_K\Rightarrow m\in I\Rightarrow(m)\subseteq I$

Look at $|\mathcal{O}_K/I|\leq|\mathcal{O}_K/(m)|$
$|\mathcal{O}_K/(m)|$ is finite (since $\mathcal{O}_K$ is a free abelian group of finite rank and $G/mG\cong\bigoplus_n\mathbb{Z}/m(\bigoplus_n\mathbb{Z})\cong\bigoplus_n\mathbb{Z}/m\mathbb{Z}$)
so $N(I)$ is well-defined ☒

Facts:
1) $N(IJ)=N(I)N(J)$
2) $N((\alpha))=|N_{\mathbb{Q}}^{K}(\alpha)|$

A fractional ideal $\mathfrak{a}$ of $K$ is a set of the form $\alpha\cdot I$ for some $\alpha\in K$ and some ideal $I$ of $\mathcal{O}_K$

Define the product of two fractional ideals by: $(\alpha I)(\beta J)=\alpha\beta IJ$ so the product of two fractional ideals is a fractional ideal

Define $\mathfrak{a}^{-1} := \{\alpha \in K : \alpha\mathfrak{a} \subseteq \mathcal{O}_K\}$ ← also a fractional ideal
↳ $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$
So the fractional ideals form a group

Define the ideal class group $Cl(K)$ as $Cl(K) := G/H$ where $G$ is the group of fractional ideals and $H$ is a subgroup consisting of all the principal fractional ideals
↑ looks like $\alpha\mathcal{O}_K$

For a fractional ideal $\mathfrak{a}$, let $[\mathfrak{a}]$ be the ideal class containing $\mathfrak{a}$. Let $h_K = |G/H| = \#$ ideal classes. $h_K$ is the ideal class number

Theorem: For all $K$, $h_K < \infty$ ($h_K = 1$ iff $\mathcal{O}_K$ is a PID)

Key Theorem: For all nonzero fractional ideals $\mathfrak{a}$ of $\mathcal{O}_K$, $\exists \alpha \in \mathfrak{a}, \alpha \neq 0$ s.t. $|N_{\mathbb{Q}}^{K}(\alpha)| \leq M_K N(\mathfrak{a})$ where
$M_K = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|\text{disc}(K)|}$ (note if $\mathfrak{a} = \beta I$ then $N(\mathfrak{a}) = N(\beta)N(I)$)

$r_2$ is the number of pairs of complex embeddings of $K$

Let $\sigma_1, \dots, \sigma_{r_1}$ = real embeddings and $\tau_1, \overline{\tau_1}, \dots, \tau_{r_2}, \overline{\tau_{r_2}}$ = complex embeddings ($r_1 + 2r_2 = n$) and define
$K \to \mathbb{R}^n$
$\alpha \mapsto (\sigma_1(\alpha), \sigma_2(\alpha), \dots, \sigma_{r_1}(\alpha), \text{Re}(\tau_1(\alpha)), \text{Im}(\tau_1(\alpha)), \dots, \text{Re}(\tau_{r_2}(\alpha)), \text{Im}(\tau_{r_2}(\alpha)))$
The map is an additive homomorphism with a trivial kernel thus it is an embedding
$\Rightarrow \mathcal{O}_K$ maps onto an $n$-dimensional lattice $\Lambda_{\mathcal{O}_K}$
$\text{vol}(\Lambda_{\mathcal{O}_K}) = \frac{1}{2^{r_2}} \sqrt{|\text{disc}(K)|}$

For a sublattice $M$ of a lattice $\Lambda$, $\text{vol}(M) = \text{vol}(\Lambda)|\Lambda/M|$

image $\Lambda_I$ of $I$ gives $\text{vol}(\Lambda_I) = \text{vol}(\Lambda_{\mathcal{O}_K})|\mathcal{O}_K/I| = \text{vol}(\Lambda_{\mathcal{O}_K})N(I)$

Define a special norm on $\mathbb{R}^n$ depending on $r_1$ and $r_2$ in the following: $x = (x_1, x_2, \dots, x_n) \in \mathbb{R}^n$, set
$N(x) = x_1 x_2 \cdots x_{r_1}(x_{r_1+1}^2 + x_{r_1+2}^2) \cdots (x_{n-1}^2 + x_n^2)$
If $\alpha \in \mathcal{O}_K$, $\alpha \mapsto x \in \Lambda_{\mathcal{O}_K}$, then $N(x) = N_{\mathbb{Q}}^{K}(\alpha)$

Theorem: Every $n$-dimensional lattice $\Lambda$ in $\mathbb{R}^n$ contains a nonzero point $x$ with
$|N(x)| \leq \frac{n!}{n^n} \left(\frac{8}{\pi}\right)^{r_2} \text{vol}(\Lambda)$ (apply $\Lambda = \Lambda_I$)

Lemma 1: Let $\mathfrak{a}$ be a fractional ideal of $K$. Then $\exists I \trianglelefteq \mathcal{O}_K$ s.t.
i) $[\mathfrak{a}] = [I]$
ii) $N(I) \leq M_K$
Proof: Consider $\mathfrak{a}^{-1}$ of $\mathfrak{a}$. $\exists \beta \in K^\times$ s.t. $J = \beta\mathfrak{a}^{-1}$ is an ideal in $\mathcal{O}_K$
$\exists \alpha \in J, \alpha \neq 0$ s.t. $|N_{\mathbb{Q}}^{K}(\alpha)| \leq M_K N(J)$
Also $(\alpha) \subseteq J \Rightarrow (\alpha) \subseteq JI$ for some $I \trianglelefteq \mathcal{O}_K$
$[I] = [J^{-1}] = [\mathfrak{a}] \cdot N(I)N(J) = N((\alpha)) = |N_{\mathbb{Q}}^{K}(\alpha)| \leq M_K N(J)$

Lemma 2: There exists only finitely many integral ideals of bounded norms
$N(I) = N(P_1)^{e_1} N(P_2)^{e_2} N(P_r)^{e_r} \leq m$

# October 17 (Dan)

## Dirichlet Characters and Number Fields

Theorem (Quadratic Reciprocity): Let $p,q$ be odd primes, then $p$ is a square mod $q$ if and only if $q$ is a square mod $p$ unless $p\equiv q\equiv 3 \pmod 4$ in which the opposite is true. (Further 2 is a square mod $p$ if and only if $p\equiv \pm 1 \pmod 8$ and $-1$ is a square if and only if $p\equiv 1 \pmod 4$)

## Euler's Formulation

Definition: Let $p$ be an odd prime. A quadratic residue mod $p$ is just a square mod $p$

Definition: The Legendre symbol $\left(\frac{a}{p}\right)$ for $a\in\mathbb{Z}$ is given by $\left(\frac{a}{p}\right)=\begin{cases}0 \text{ if } p\mid a\\ 1 \text{ if } a \text{ is a quadratic residue mod } p\\ -1 \text{ if } a \text{ is not a quadratic residue mod } p\end{cases}$

so Quadratic Reciprocity says: $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$ unless $p\equiv q\equiv 3 \pmod 4$, then $\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right)$

Euler's version: if $p\equiv \pm q \pmod{4|a|}$, then $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)$

Note: $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Some people express Quadratic Reciprocity as $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$

we want to extend this to get "$\left(\frac{a}{n}\right)\left(\frac{n}{a}\right)=(-1)^{\left(\frac{a-1}{2}\right)\left(\frac{n-1}{2}\right)}$" ← not quite right. Robby doesnt like it

Definition: The Kronecker symbol $\left(\frac{a}{n}\right)$ for $a,n\in\mathbb{Z}$: let $n=up_1^{e_1}\cdots p_k^{e_k}$, $u=\pm 1$, $p_i$ prime and let

$\left(\frac{a}{n}\right)=\left(\frac{a}{u}\right)\prod_{i=1}^{k}\left(\frac{a}{p_i}\right)^{e_i}$ $n\neq 0$ where $\left(\frac{a}{1}\right)=1$, $\left(\frac{a}{-1}\right)=\begin{cases}1, a\geq 0\\ -1, a<0\end{cases}$, $\left(\frac{a}{0}\right)=\begin{cases}1, a=\pm 1\\ 0, \text{otherwise}\end{cases}$

If $p$ is odd, $\left(\frac{a}{p}\right)$ = Legendres symbol. $\left(\frac{a}{2}\right)=\begin{cases}0, 2\mid a\\ 1, a\equiv \pm 1 \pmod 8\\ -1, a\equiv \pm 3 \pmod 8\end{cases}$

Then $\left(\frac{ab}{n}\right)=\left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$, $n\neq -1$, $\left(\frac{a}{mn}\right)=\left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$ $a\neq -1$

Euler's Quadratic Reciprocity => if $p\equiv q \pmod{4|a|}$, then $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)$ => if $m\equiv n \pmod{4|a|}$, then

$\left(\frac{a}{m}\right)=\left(\frac{a}{n}\right)\Rightarrow\left(\frac{a}{-}\right)$ is a Dirichlet character mod $4|a|$

# Quadratic Fields

Let $d \in \mathbb{Z}$ be squarefree, $d \neq 0, 1$, and let $K_d = \mathbb{Q}(\sqrt{d})$, then $\mathcal{O}_{K_d} = \mathcal{O}_d = \begin{cases} \mathbb{Z}[\sqrt{d}] & , d \equiv 2,3 \pmod 4 \\ \mathbb{Z}[(1+\sqrt{d})/2] & , d \equiv 1 \pmod 4 \end{cases}$

so $\Delta(K_d) = \begin{cases} 4d & , d \equiv 2,3 \pmod 4 \\ d & , d \equiv 1 \pmod 4 \end{cases}$

Example: $d=-1$: $\mathbb{Q}(i)$, $\mathcal{O}_{-1} = \mathbb{Z}[i]$, $\Delta(K_{-1}) = -4$ (Gaussian integers)

$d=-3$, $\mathbb{Q}(\sqrt{-3})$, $\mathcal{O}_{-3} \supsetneq \mathbb{Z}[\sqrt{-3}]$, $\omega = \frac{-1+\sqrt{-3}}{2}$, $1+\omega = \frac{1+\sqrt{-3}}{2}$, $\omega^3 = 1 \Rightarrow K_{-3} = \mathbb{Q}(\omega)$ and $\mathcal{O}_{-3} = \mathbb{Z}[\omega]$ (Eisenstein integers)

$\mathbb{Z}[(1+\sqrt{-3})/2]$

Definition: A fundamental discriminant is an integer that is the discriminant of a quadratic field i.e. $\Delta$ is fundamental if $\Delta \equiv 1 \pmod 4$ and squarefree or $\Delta = 4d$, $d \equiv 2,3 \pmod 4$ and $d$ squarefree

Let $\Delta$ be a fundamental discriminant and let $\chi_\Delta := \left(\frac{\Delta}{-}\right) = \chi_d = \left(\frac{d}{-}\right)$ (since either $\Delta = d$ or $\Delta = 4d$

$\Rightarrow \left(\frac{\Delta}{-}\right) = \left(\frac{4}{-}\right)\left(\frac{d}{-}\right) = \left(\frac{2}{-}\right)^2\left(\frac{d}{-}\right) = \left(\frac{d}{-}\right)$

Theorem: $\chi_\Delta$ is a Dirichlet character of conductor $|\Delta|$ and $\left(\frac{\Delta}{-}\right)$ is odd $\left(\text{i.e. } \frac{\Delta}{-1} = -1\right)$ if and only if $\Delta < 0$

Let $p$ be prime in $\mathbb{Z}$. Question: How does it factor in $\mathcal{O}_K$? By the unique factorization into prime ideals, look at $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}$, $\mathfrak{p}_i$ prime ideals in $\mathcal{O}_K$

For quadratic fields: $p\mathcal{O}_d = \mathfrak{p}_1\mathfrak{p}_2$ ($p$ is "split") $\mathfrak{p}_1 \neq \mathfrak{p}_2$
or $p\mathcal{O}_d = \mathfrak{p}$ ($p$ is "inert")
or $p\mathcal{O}_d = \mathfrak{p}^2$ ($p$ is "ramified")

set up a dictionary

Example: $d=-1$, $\mathbb{Z}[i]$, $(5) = (1+2i)(1-2i)$ split $\longleftrightarrow 1$
$(3) = (3)$ inert $\longleftrightarrow -1$
$2\mathcal{O}_{-1} = (1+i)^2\mathcal{O}_{-1}$ ramified $\longleftrightarrow 0$

(Generally if $p \equiv 1 \pmod 4$ it splits. If $p \equiv 3 \pmod 4$ its inert. $p=2$ ramified)

Then the way $p\mathcal{O}_{-1}$ factors is given by $\left(\frac{d}{p}\right) = \left(\frac{-1}{p}\right) = \left(\frac{-4}{p}\right) = \chi_{-1}$ since $\left(\frac{-1}{p}\right) = \begin{cases} 1 & , p \equiv 1 \pmod 4 \\ -1 & , p \equiv 3 \pmod 4 \\ 0 & , p = 2 \end{cases}$

Theorem: $d$ squarefree and $\Delta = \Delta(K_d)$ then $p$ is ramified, split, or inert according to $\chi_\Delta(p) = 0, 1$, or $-1$

$N(p\mathcal{O}_d) = p^2$, $p\mathcal{O}_d = \mathfrak{p}_1\mathfrak{p}_2 \Rightarrow N(\mathfrak{p}_i) = p$
$= \mathfrak{p} \Rightarrow N(\mathfrak{p}) = p^2$
$= \mathfrak{p}^2 \Rightarrow N(\mathfrak{p}) = p$
} Since $n$ is multiplicative

So $\zeta_{K_d}(s) = \prod_{0 \neq \mathfrak{p} \subset \mathcal{O}_d \text{ prime}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = \prod_{\left(\frac{\Delta}{p}\right)=0} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{\left(\frac{\Delta}{p}\right)=-1} \left(1 - \frac{1}{p^{2s}}\right) \prod_{\left(\frac{\Delta}{p}\right)=1} \left(1 - \frac{1}{p^s}\right)^{-2} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \prod_p \left(1 - \frac{1}{\chi_\Delta(p)p^s}\right)^{-1}$
$= \zeta(s)L(s, \chi_\Delta)$

# October 24 (Sarah)

## Elliptic Curves and their Hasse-Weil L-Functions

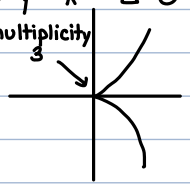
Definition: Let $K$ be a field. An elliptic curve over $K$ is a smooth (non-singular) projective plane curve given by an affine model:

$E: y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$, $a_i \in K$ ← long weirstrass form

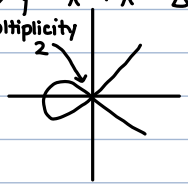
If $\text{char}(K) \neq 2,3$, a change of variable gives $E: y^2 = x^3+Ax+B$ (short weirstrass form), $A,B \in K$ $\Delta(E) = -16(4a^3+27B^2) \neq 0$ (want)

Examples:

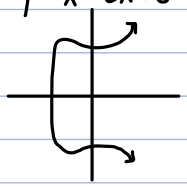
1) $y^2 = x^3$ $\Delta = 0$ — multiplicity 3 — cusp at (0,0)



2) $y^2 = x^3+x^2$ $\Delta = 0$ — multiplicity 2 — node at (0,0)



3) $y^2 = x^3-3x+3$ $\Delta = 2160$ — smooth, non-singular



$f(x) = x^3 - Ax + B$ (singular), $\theta_1,\theta_2,\theta_3$ are roots

$\Delta(f) = [(\theta_1-\theta_2)(\theta_2-\theta_3)(\theta_1-\theta_3)]^2 = -(4A^3+27B^2)$

$\Delta f$ non-zero as long as $\theta_1,\theta_2,\theta_3$ are distinct

Definition: A projective plane over $K$ is $\mathbb{P}^2(K) := \mathbb{A}^3(K)\setminus\{(0,0,0)\}/\sim$ where $[x_0:y_0:z_0] \sim [\lambda x_0:\lambda y_0:\lambda z_0]$ $x_0,y_0,z_0,\lambda \in K$, $\lambda \neq 0$

Projective planes have the property that each class of parallel lines intersect. i.e. all vertical lines intersect at $\infty$, a point at $\infty$

$K = \mathbb{Q}$. Given an elliptic curve $E\setminus\mathbb{Q}$, we are particularly interested in $E(\mathbb{Q})$, rational solutions of $E$

Homogenize: $E: y^2 = x^3+Ax+B$, $A,B \in \mathbb{Q}$, $\Delta(E) \neq 0$

$\lambda f(x) = f(\lambda x)$ $\quad x = \frac{x_0}{z_0}$ $\quad y = \frac{y_0}{z_0}$ $\quad \frac{y_0^2}{z_0^2} = \frac{x_0^3}{z_0^3} + A\frac{x_0}{z_0} + B \Rightarrow y_0^2 z_0 = x_0^3 + Ax_0z_0^2 + Bz_0^3$

let $z_0 = 1 \Rightarrow$ back to short weirstrass form

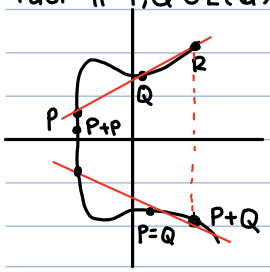
If $[x_0:y_0:1] \sim [\lambda x_0:\lambda y_0:\lambda] \Rightarrow (x,y) = (x_0,y_0)$

$\mathbb{A}^3(\mathbb{Q})$ $\quad$ $\mathbb{P}^2(\mathbb{Q})$

let $z_0 = 0$ then $x_0 = 0 \Rightarrow$ If $[0:1:0]$ is a solution $\Rightarrow (x,y) = (\ )$ (undefined) since $x = x_0/z_0$, call it $\mathcal{O}$, point at $\infty$

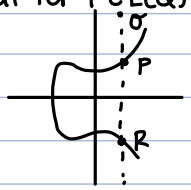
so for any $E\setminus(\mathbb{Q})$, $\mathcal{O} \in E(\mathbb{Q})$

Fact: If $P,Q \in E(\mathbb{Q})$, $R \in E(\mathbb{Q})$

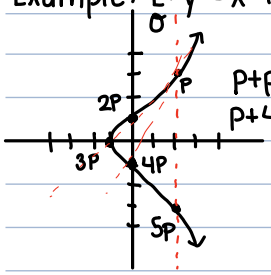


Using this fact, we define additional points $P, Q \in E(\mathbb{Q})$
↳ If $P \neq Q$, secant line hits at point $R$. Reflect this about the x-axis and that is $P+Q$
↳ If $P=Q$, use the tangent line and do the same thing

Note that for $P \in E(\mathbb{Q})$, $P+\mathcal{O}=\mathcal{O}+P=P$
Sketch:




Example: $E: y^2=x^3+1$ $E(\mathbb{Q})=\{(-1,0),(0,1),(0,-1),(2,3),(2,-3),\mathcal{O}\}$




P+P hits at 4P
P+4P hits at P

$P=(2,3)$
$P+P=2P=(0,1)$
$P+2P=3P=(-1,0)$
$P+3P=4P=(0,-1)$

$P+4P=5P=(2,-3)$
$P+5P=6P=\mathcal{O}$

Question: Is $E(\mathbb{Q})$ a group? Yes! with $\mathcal{O}$ as the identity. $\langle P \rangle = E(\mathbb{Q}) \approx \mathbb{Z}/6\mathbb{Z}$

Mordell-Weil Theorem: $E(\mathbb{Q})$ is a finitely generated abelian group. In fact $E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^{R_E}$ where
$E(\mathbb{Q})_{tors} = \{P \in E(\mathbb{Q}) : |P| < \infty\} = \{P \in E(\mathbb{Q}) : nP=\mathcal{O} \text{ for some } n \in \mathbb{N}\}$

Theorem (Mazur): $E(\mathbb{Q})_{tors} \cong \begin{cases} \mathbb{Z}/n\mathbb{Z} & , 1 \leq n \leq 10 \text{ or } n=12 \\ \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & , m=2,4,6,8 \end{cases}$

↳ There are only 15 possible torsion subgroups
↳ $E(\mathbb{Q})_{tors}$ is finite

$|E(\mathbb{Q})| < \infty$ is entirely dependent on the rank. $\text{rank}(E)=0 \Rightarrow |E(\mathbb{Q})|$ is finite. $\text{rank}(E) \neq 0$, $|E(\mathbb{Q})| = \infty$

Computing the rank of E is difficult

Examples:
$E_1: y^2=x^3+1$, $E_1(\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z} \Rightarrow \text{rank}(E_1)=0$
$E_2: y^2=x^3+6$, $E_2(\mathbb{Q})=\{\mathcal{O}\} \cong \mathbb{Z}/1\mathbb{Z} \Rightarrow \text{rank}(E_2)=0$
$E_3: y^2=x^3-2$, $E_3(\mathbb{Q})=\langle (3,5) \rangle \cong \mathbb{Z}$
(Fun Fact: $E(\mathbb{Q})_{tors}=\{\mathcal{O}\} \Rightarrow$ every affine rational point on $E_3$ has infinite order!)
$E_4: y^2=x^3+7105x^2+1327104x$, $E_4(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}^3 \Rightarrow \text{rank}(E_4)=3$

Noam Elkies:
(2006) $E: y^2+xy+y=x^3-x^2+ax+b$, $\text{rank}(E) \geq 28$ ← someone discovered its equal to 28 recently
a has 56 digits, b has 83 digits
(2009) largest known rank $(E_*)=19$

Conjecture: There is no bound on the largest rank for an elliptic curve ← probably wrong

# November 7 (Sarah)

Last time:

Mordel-Weil Theorem: $E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^{R_E}$ ← rank of E, "not so easy" ("easy", finite)

$\#E(\mathbb{Q}) < \infty \iff R_E = 0$

$\#E(\mathbb{Q}) = \infty \iff R_E \geq 1$

Motivation for "How do we find/estimate $R_E$?"

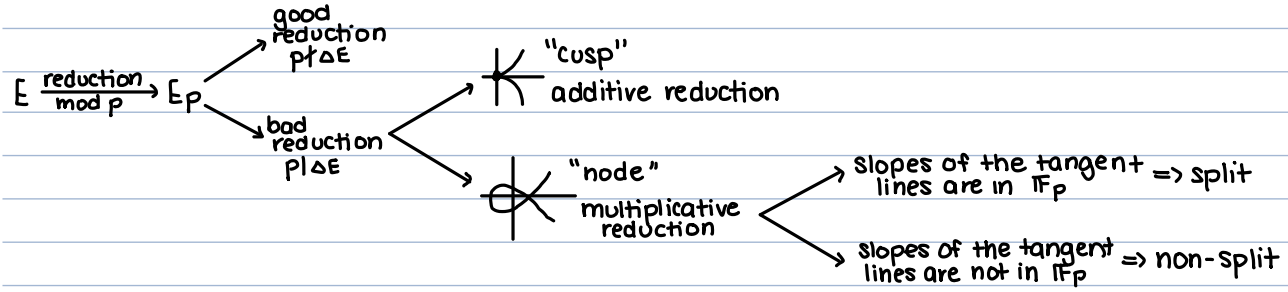
Analytic Approach

$E\backslash\mathbb{Q}$, $E: y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$ (see table 31 Silverman A.E.C.) $\Delta_E = -16(4a^3 + 27b^2) \neq 0$ (smooth)

↓ reduction mod p, p prime

$E_p: y^2 \equiv x^3 + \bar{a}x + \bar{b}$ $\bar{a}, \bar{b} \in \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ $\Delta_{E,p} \neq 0$

$E\backslash\mathbb{F}_p$




There are only finitely many p such that $p \mid \Delta E$

Fix p. Define $N_p^m := \#E(\mathbb{F}_{p^m})$, $m \geq 1$, p prime $\{N_{p^m}\}_{m=1}^{\infty}$

look at $Z(E_p, u) = \exp \sum_{m=1}^{\infty} N_p^m \frac{u^m}{m} = \sum_{n=0}^{\infty} \frac{1}{n!} \left( \sum_{m=1}^{\infty} N_p^m \frac{u^m}{m} \right)^n = \frac{1 - a_p u + p u^2}{(1-u)(1-pu)}$ (Riemann-Roch Theorem)

This $a_p$ depends on p

$$a_p = \begin{cases} 0 & \text{additive reduction} \\ 1 & \text{split multiplicative reduction} \\ -1 & \text{non-split multiplicative reduction} \end{cases} \Big\} p \mid \Delta E$$

$a_p = p + 1 - N_p(E)$ ($\#E(\mathbb{F}_p)$) good reduction ← $p \nmid \Delta E$

The global-zeta function $\zeta(E,s) = \prod_p \zeta(E_p, s) = \prod_p \frac{1}{(1-p^{-s})(1-p^{1-s})} \cdot \prod_{p \nmid \Delta E} (1 - a_p p^{-s} + p^{1-2s})$

$$= \zeta(s)\zeta(s-1) \prod_{p \nmid \Delta E} (1 - a_p p^{-s} + p^{1-2s}) := L(s,E)^{-1}$$

Definition: The Hasse-Weil L-function of $E\backslash\mathbb{Q}$ is $L(s,E) := \prod_p (1 - a_p p^{-s} + 1_\Delta(p) p^{1-2s})^{-1}$, where $1_\Delta(p) = \begin{cases} 0, & p \mid \Delta E \\ 1, & p \nmid \Delta E \end{cases}$

Fact: Theres overwhelming evidence that $\zeta(E,p)$ can be analytically continued to all of $\mathbb{C}$

$L(s,E)$ converges for $Re(s) > 3/2$

Question: Can $L(s,E)$ be analytically continued to all of $\mathbb{C}$? (conjecture: maybe)

$L(S,E)$ has an analytic continuation to the entire complex plane as an analytic function $L^*(S,E)$ that satisfies the functional equation: $L^*(S,E)=\omega(E)\cdot L^*(2-S,E)$

$\omega(E)$: root #, $\omega(E)=\pm 1$

$L^*(S,E)=(N_E)^{S/2}(2\pi)^{-S}\Gamma(S)L(S,E)$

$N_E$: conductor of $E$ (roughly the product of primes with bad reduction)

Assuming the conjecture (Robby says it's proven), it now makes sense to talk about $L(S,E)$ at $S=1$

Birch, Swinnerton-Dyer (BSD) conjecture: The rank of $E$ over $\mathbb{Q}$ is equal to the order of the zeros of $L(S,E)$ at $S=1$. ($\text{ord}_{S=1}L(S,E)=R_E$)

Fun Facts

1) Millenium problem: $1 million
2) $a_p$ measures the error in your estimate of the rank. $a_p \le 2\sqrt{p}$ ← Hasse Bound
3) $L^*(S,E)=\omega(E)L^*(2-S,E)$
   consider $\omega(E)=-1$ at $S=1$, $L^*(1,E)=-L^*(1,E) \Rightarrow L^*(1,E)=0$ so $L(S,E)$ has a zero at $S=1$, by BSD, $R_E \ge 1$, $|E(\mathbb{Q})|=\infty$
4) Reflects around $\text{Re}(S)=1$, compared to $\text{Re}(S)=\frac{1}{2}$ (Riemann zeta function)

New Question: How do we find $\text{ord}_{S=1}L(S,E)$?

Recall: Analytic class number equation:

$F$, a field, $R_F := \text{ord}_{S=0}\zeta_F(S)$

$$\lim_{S\to 0}\frac{\zeta_F(S)}{S^{R_F}} = \frac{-h_F \text{Reg}_F}{W_F}$$

$h_F = \#Cl(F)$ $\quad W_F = \#\mu(F)$ roots of units $\quad \text{Reg}_F = \text{covol}(\mathbb{Z}^{R_F})$

The BSD makes this analogous for an elliptic curve

BSD Conjecture

ii) $$\lim_{S\to 1}\frac{L(S,E)}{(S-1)^{R_E}} = \frac{\Omega_E \#Ш_E \cdot \text{Reg}_E}{(\#E(\mathbb{Q})_{tors})^2}\cdot\prod_p c_p$$

$$\Omega_E := \int_{E(\mathbb{R})}\frac{dx}{|2y|}$$

$\text{reg}_E$: elliptic regulator of $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$

$\hat{h}: E(\mathbb{Q}) \to \mathbb{R}$

Since $E$ is a projective curve, $E(\mathbb{Q}_p)=E(\mathbb{Z}_p)$

Tamagawa numbers, $E_0(\mathbb{Q}_p) := \{p \in E(\mathbb{Q}_p)$: $p$ reduces to a non-singular point in $E(\#p)\}$

$c_p := \#(E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p))$. $c_p$ is 1 if $p \nmid \Delta_E$

$Ш_E$ is called the "shafarevich tate group"

$$0 \to \underbrace{E(\mathbb{Q})\otimes\mathbb{Q}/\mathbb{Z}}_{(\mathbb{Q}/\mathbb{Z})^{R_E}} \to \text{sel}(E) \to Ш_E \to 0$$

↳ "selmer group of $E$". Consider $E$ over $\mathbb{Q}_p$ over $\mathbb{R}$ and over $\mathbb{C}$

Let $K$ be a number field $Ш_{E/K} := \ker[H^1(K,E) \to \prod_p H^1(K_p,E)]$ where $H^1(K,E) := H^1(\text{Gal}(\bar{K},K), E(\bar{K}))$ induced by $\text{Gal}(\bar{K}_p/K_p) \hookrightarrow \text{Gal}(\bar{K},K)$.

Shafarevich-Tate Conjecture: $Ш_E$ is finite

2009: Verified true for all $E\backslash\mathbb{Q}$ with $R_E \le 1$ and conductor $< 5000$

# November 14 (Erik)

## Modular Forms and L-functions

Let $H$ = the upper half plane $= \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ with metric $dxdy/y^2$

Define the modular group to be $SL_2(\mathbb{R})$. we define an action of $SL_2(\mathbb{R})$ on $H$:

$$\gamma(z) = \frac{az+b}{cz+d} \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

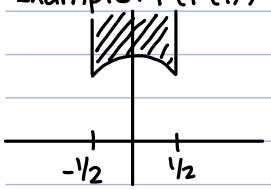
This action is isometric, transitive, and "almost" faithful

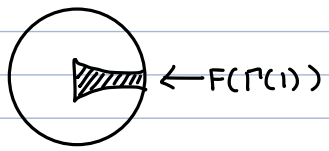
$\gamma, -\gamma$ act identically

$PSL_2(\mathbb{R})$

Definition: The fundamental domain for $\Gamma(1) = SL_2(\mathbb{Z})$ is the set of $z \in H$ such that $z_1 \not\sim_{\Gamma(1)} z_2$ for $z_1, z_2 \in F(\Gamma(1))$ and given any $z \in H$ $\exists \gamma \in \Gamma(1)$ such that $\gamma(z) \in F(\Gamma(1))$

Example: $F(\Gamma(1)) = \{z \in H : |\mathrm{Re}(z)| < 1/2,\ |z| > 1\}$. There is a map $C : H \longrightarrow D$, $z \longmapsto z-1/z+1$




Extend: $\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \right\}$, $\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N \right\}$

$$\Gamma(1) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$$

cusp of $\Gamma$ are the points ($\Gamma$ orbits) of $\mathbb{Q} \cup \{\infty\}$

Let $H^* = H \cup \{\text{cusps}\}$

Definition: $f$ is a modular form of weight $k$, for $\Gamma$, if $f$ is holomorphic on $H^*$ and has the property that

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \text{ for } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$$

Definition: Given a Dirichlet character mod $N$, $M_k(N, \chi)$ is the space of functions holomorphic on $H^*$ with the property $f\left(\frac{az+b}{cz+d}\right) = \overline{\chi(d)}\,(cz+d)^k f(z)$

Denote $M_k(\Gamma)$, the space of modular forms for $\Gamma$ weight $k$.

$S_k(\Gamma)$ is the space of modular forms for $\Gamma$ of weight $k$, which vanish at the cusps

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \Rightarrow f(z) = f(z+1),\ f(z) = \sum_{n=0}^{\infty} a_n q^n = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$$

Notes about these spaces:

↳ They form a vector space over $\mathbb{C}$

↳ $M(\Gamma(1))$ is a graded ring. $f \in M_k(\Gamma(1)), g \in M_\ell(\Gamma(1)) \Rightarrow fg \in M_{k+\ell}(\Gamma(1))$

↳ $f$ is an automorphic function if meromorphic

$$f\left(\frac{az+b}{cz+d}\right) = f(z) \text{ for } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$$

↳ $f, g \in M_k(\Gamma(1))$ then $f/g$ is an automorphism

Examples: Eisensteins series:

let $k=2m>4$ and $(m,n\in\mathbb{Z})$. Define $E_k(z)=\frac{1}{2}\sum_{(m,n)=(0,0)}(mz+n)^{-k}$

(it can be shown that $E_k(z)$ is a weight $k$ modular form for $\Gamma(1)$)

$E_k(z)=\zeta(k)+\frac{(2\pi)^k(-1)^{k/2}}{(k-1)!}\sum\sigma_{k-1}(n)q^n$ where $\sigma_k(n)=\sum_{d|n}d^k$

$G_k(z)=\zeta(k)^{-1}E_k(z)$

Define $\Delta(z)$: $G_4(z)=1+240\sum\sigma_3(n)q^n$, $G_6(z)=1-504\sum\sigma_5(n)q^n$

Take $\frac{G_4(z)^3-G_6(z)^2}{1728}=\Delta(z)=q-24q^2+252q^3$

This is a cusp form of weight 12 for $\Gamma(1)$. $S_k(\Gamma(1))$ has dimension 1

Mellin transform: $f:(0,\infty)\to\mathbb{C}$, $M(s,f)=\int_{\mathbb{R}>0}f(y)y^s\frac{dy}{y}$

Example: $M(s,e^{-t})=\int_{\mathbb{R}>0}e^{-t}t^s\frac{dt}{t}=\Gamma(s)$

L-function of mod form: given $f(z)=\sum_{n=0}^{\infty}a_nq^n$. Define $L(s,f)=\sum_{n=1}^{\infty}a_nn^{-s}$

Trivial estimate: $a_n<Cn^{k/2}$

Proposition: L-function has meromorphic continuation to all s and satisfies a functional equation if $\Lambda(s,f)=(-1)^{k/2}\Lambda(k-s,f)$. The $\Lambda(s,f)$ extends to a function on s

$\Lambda(s,f)=(2\pi)^{-s}\Gamma(s)L(s,f)$

First conjectured Euler product was by Ramanujan

$L(s,\Delta)=\sum\tau(n)n^{-s}=\prod_p(1-\tau(p)p^{-s}+p^{1-2s})^{-1}$, $\sum\tau(n)q^n=q\prod(1-q^n)^{24}$

This is in general not true, $\Delta$ is a Hecke eigenform (Modularity Theorem)

Generalization: $L(s,f,\chi)=\sum\chi(n)a_nn^{-s}$

Converse theorem: Given an L-function satisfying some functional equations, when can we say $L(s,f)$ comes from a modular form?

In the case of $\Gamma(1)$, things arent so bad

Given $f(z)=\sum a_nq^n$, $L(s,f)=\sum a_nn^{-s}$, $\Lambda(s,f)=(2\pi)^{-s}\Gamma(s)L(s,f)=(-1)^{k/2}\Lambda(k-s,f)$ and sometimes on Euler product

Theorem: Given a sequence $|a_n|=\mathcal{O}(n^k)$ for some $k$ sufficiently large, $L(s,f)=\sum a_nn^{-s}$ $\Lambda(s,f)$ has a continuation then $f(z)=\sum a_nq^n$ is a modular form, $S_k(\Gamma(1))$

Theorem: For $k$ an even integer, $f$ holomorphic on $H$ with Fourier expansion $\sum a_ne^{2\pi inz}$, $f(z)\in M_k(\Gamma(1))$ if and only if $\Lambda(s,f)=(2\pi)^{-s}\Gamma(s)L(s,f)=(-1)^{k/2}\Lambda(k-s,f)$, $\Lambda(s,f)+\frac{a_0}{s}+\frac{(-1)^{k/2}a_0}{k-s}$ and $a_0=0\Rightarrow f$ is a cusp form

# November 21 (Erik)

Recall: we introduced modular forms for $\Gamma(1)$ and also for congruence subgroups

$f(z)=f(z+1) \Rightarrow f(z)=\sum a_n q^n$, $q=e^{2\pi i z}$

$L(s,f)=\sum a_n n^{-s}$

$\Lambda(s,f)=(2\pi)^{-s}\Gamma(s)L(s,f)$

Also we mentioned the Mellin Transform: $M(f):=\int_{\mathbb{R}>0} f(t)t^s\frac{dt}{t}$

Question: what is the connection?

$\Lambda(s,f)=M(f(it))$

(In Diamond/Sherman theres a nice example)

$M^{-1}(L(s,f))=f$

Given conditions on the L-function, can we say it comes from a modular form?

Converse Theorem: (for $\Gamma(1)$) $f\in M_k(\Gamma(1))$ if and only if $\Lambda(s,f)=(2\pi)^{-s}\Gamma(s)L(s,f)$ has an analytic continuation, is bounded in vertical strips and $\Lambda_k(s,f)=(-1)^{k/2}\Lambda_k(k-s,f)$

Example: Recall the Eisenstein series $E_k(z)=\zeta(k)+\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^k$, $L(s,E_z(k))=\sum\sigma_{k-1}(n)n^{-s}$

Can we show that this has the desired properties?

conditions to satisfy:

$\Lambda(s,E_k(s))=(2\pi)^{-s}\Gamma(s)L(s,E_k(z))$

$\zeta(s),\Lambda(s)=\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)\rightarrow\Lambda(s)+\frac{1}{s}-\frac{1}{s-1}$

$Z_k(s)=\Lambda(s)\Lambda(s-(k+1))$

$\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s-(k+1)}{2}\right)$ $\qquad$ $\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s}{2}+\frac{1}{2}\right)=\Gamma(s)$

$Z_k(s)$ has the required properties to apply the converse theorem (exercise for the reader)

$\Gamma(1)=\langle S,T\rangle$ has minimal generators, $\Gamma(N)$ has more generators

Question: Can we say something similar to the Hecke converse theorem

Weil Converse theorem: If $N\in\mathbb{Z}_{>0}$, $\chi$ is a Dirichlet character mod N, $a_n$ and $b_n$ are sequences of complex numbers, and $|a_n|,|b_n|=O(n^k)$ for k sufficiently large

$(D,N)=1$, $\chi$ a Dirichlet character mod D

$L_1(s,\chi)=\sum\chi(n)a_nn^{-s}$ $\qquad$ $L_2(s,\overline{\chi})=\sum\overline{\chi(n)}b_nn^{-s}$

$\Lambda_1(s,\chi)=(2\pi)^{-s}\Gamma(s)L_1(s,\chi)$ $\qquad$ $\Lambda_2(s,\overline{\chi})=(2\pi)^{-s}\Gamma(s)L_2(s,\overline{\chi})$ $\qquad$ too long to write

(imposing extra conditions)

$\Lambda_1(s,\chi)$, $\Lambda_2(s,\overline{\chi})$ have analytic continuation, bounded in strips, and satisfy a functional equation

Then $f(z)=\sum a_nq^n$ is a mod form in $M_k(N,\chi)$

$g(z)=\sum b_nq^n\ldots$

We hope that an L-function has an Euler product

$\Delta(z)$ a weight 12 cusp form, $L(s,\Delta(z))=\sum_{n=1}^{\infty}\tau(n)n^{-s}=\prod_p(1-\tau(p)p^{-s}+p^{11-2s})^{-1}$

Question: which modular forms have an Euler product?
Answer: when $f \in M_k(\Gamma)$ is a Hecke eigenform in $M_k(\Gamma)$

Digress: we can think of $SL_2(\mathbb{Z})\backslash\mathcal{H}$ as the space of 2-dimensional lattices
define a lattice over $\mathbb{C}$, $(\omega_1, \omega_2)$ to form the lattice $\Lambda(\omega_1, \omega_2) = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ so $B = \{(\omega_1, \omega_2) \in (\mathbb{C}^\times)^2 : \mathrm{Im}(\omega_1/\omega_2) > 0\}$

$B \longrightarrow L$ (space of lattices)

$(\omega_1, \omega_2) \longmapsto \Lambda(\omega_1, \omega_2)$

Proposition: $\Lambda(\omega_1, \omega_2) = \Lambda(\omega_1', \omega_2')$ if and only if $\exists \gamma \in \Gamma(1)$ such that $\gamma(\omega_1, \omega_2) = (\omega_1', \omega_2')$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} a\omega_1 + b\omega_2 \\ c\omega_1 + d\omega_2 \end{pmatrix}$$

Corollary: $L \cong SL_2(\mathbb{Z})\backslash B$

$B \longrightarrow \mathcal{H}$

$(\omega_1, \omega_2) \longmapsto z = \omega_1/\omega_2$

$B/\mathbb{C}^\times \cong \mathcal{H}$

$SL_2(\mathbb{Z})\backslash B/\mathbb{C}^\times \cong SL_2(\mathbb{Z})\backslash\mathcal{H}$

Define operator on $L$ $\quad T(n)\Lambda = \sum_{\substack{\Lambda' \subseteq \Lambda \\ [\Lambda : \Lambda'] = n}} \Lambda'$

$S(n)\Lambda : \Lambda \longmapsto n\Lambda$

Proposition:
1) $S(n)S(m) = S(n,m)$
2) $S(n)T(m) = T(m)S(n)$
3) $T(m)T(n) = T(mn) \quad (m,n) = 1$
4) $T(p^n)T(p) = T(p^{n+1}) + pT(p^{n-1})S(p)$

If $f$ is a Hecke eigenform normalized, $L(s,f) = \prod_p (1 - T(p)p^{-s} + p^{k-1-2s})^{-1} \quad T(p) = a_p$

# November 28 (Jamal)

## Hecke Characters and their L-Functions

Recall: Given $m \in \mathbb{Z}_{>0}$, a Dirichlet character mod m is a function $\chi: (\mathbb{Z}/m\mathbb{Z})^\times \to S^1$. The corresponding Dirichlet L-function is $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p (1-\chi(p)p^{-s})^{-1}$

Application: Primes in arithmetic progressions
Given $a,d \in \mathbb{Z}$, $(a,d)=1$?, there exists infinitely many primes p such that $p \equiv a \pmod d$

## Work Over Number Fields

Let K = number field, $\mathcal{O}_K$ = ring of integers
Problem: $\mathcal{O}_K \neq$ UFD in general but it is a Dedekind domain $\Rightarrow$ unique factorization of ideals

Analogous: Study "distribution of primes along a field ideal class" $\rightsquigarrow$ Define characters on ideals

Motivation: work over $\mathbb{Z}$

Let $\chi \bmod m$ be a Dirichlet character
Goal: Extend to a character $\tilde{\chi}$ on ideals of $\mathbb{Z}$ relatively prime to $m\mathbb{Z}$

Naive approach: Define $\tilde{\chi}((a)) = \chi(a)$ whenever $(a,m)=1$
Problem: $(a)=(-a)$ but $\chi(a) \neq \chi(-a)$ in general so $\tilde{\chi}$ is not well-defined

Note: a and -a differ by $-1 \in \mathbb{Z}^\times$

Now, $\chi(-1) = (-1)^p$, $p \in \{0,1\}$, (p = exponent of $\chi$)
Define $\tilde{\chi}((a)) = \chi(a)\left(\frac{a}{|a|}\right)^p$ for $0 \neq a \in \mathbb{Z}$, $(a,m)=1$

Let K = number field such that $\mathcal{O}_K$ is a PID. Let $0 \neq M \triangleleft \mathcal{O}_K$
Let $J^M = \{$fractional ideals of K coprime to $M\}$
we want to define $\chi: J^M \to S^1$ and decompose into two parts:
i) finite component $\chi_f: (\mathcal{O}_K/M)^\times \to S^1$
ii) infinite component $\chi_\infty: \mathcal{O}_K^\times \to S^1 \Rightarrow \chi(\langle a \rangle) := \chi_f(a)\chi_\infty(a) \quad \forall a \in K^\times, (a,M)=1$

Such a character $\chi: J^M \to S^1$ is called a Grössen charakter mod M or Hecke character

Determining $\chi$ mod M $\leftrightsquigarrow$ determing $\chi_f$ and $\chi_\infty$

The infinite component: A more convenient space than $\mathcal{O}_K^\times$ is (Minkowski space)
$(K \otimes_{\mathbb{Q}} \mathbb{R})^\times \cong (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$ where $r_1 + 2r_2 = n = [K:\mathbb{Q}]$
$\mathbb{R}^\times \cong \{\pm 1\} \times \mathbb{R}_{>0}$
$\mathbb{C}^1 \cong S^1 \times \mathbb{R}_{>0}$

characters on:

$\{\pm 1\}: x \mapsto x^p$, $p \in \{0,1\}$

$\mathbb{R}_{>0}: x \mapsto x^{iq}$, $q \in \mathbb{R}$

$S^1: x \mapsto x^p$, $p \in \mathbb{Z}$

So for $x \in (K \otimes \mathbb{R})^\times$, $x = (x_1, \dots, x_{r_1}, x_{r_1+1}, \dots, x_{r_1+r_2})$

$$x \mapsto \prod_{j=1}^{r_1+r_2} \left(\frac{x_j}{|x_j|}\right)^{p_j} |x_j|^{iq_j} \text{ where } q_j \in \mathbb{R},\ p_j \in \begin{cases} \{0,1\} & : 1 \le j \le r_1 \\ \mathbb{Z} & : r_1+1 \le j \le r_1+r_2 \end{cases}$$

$$x \mapsto N\left(\frac{x}{|x|}\right)^p |x|^{iq},\ p \in \mathbb{Z}^{r_1},\ q \in \mathbb{R}^{r_2}$$

$p - iq$ is the exponent of $\chi$

we say that $\chi$ is of type $(p,q)$

Example: $K = \mathbb{Q}(i) \rightsquigarrow \mathcal{O}_K = \mathbb{Z}[i]$ $[r_1, r_2] = [0,1]$

take $M = 1 \Rightarrow \chi_f = 1$, $\chi = \chi_\infty$

$(\mathbb{Q}(i) \otimes \mathbb{R})^\times \cong \mathbb{C}^\times$

Define $\mathbb{Q}(i)^\times \hookrightarrow \mathbb{C}^\times$

$\chi: J \longrightarrow S^1$

Take $\langle a \rangle \in J^M$ where $a \in \mathbb{Q}(i)^\times$ then $a \mapsto |a|^{iq}\left(\frac{a}{|a|}\right)^p$, $q \in \mathbb{R}$, $p \in \mathbb{Z}$

Ensure that $\chi$ is well-defined

$\mathcal{O}_K^\times = \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

check $\chi(\pm i, a) = |\pm ia|^{iq}\left(\frac{\pm ia}{|\pm ia|}\right)^p = |a|^{iq}\left(\frac{\pm ia}{|a|}\right)^p = \chi((a))(\pm i)^p$

Thus $(\pm i)^p = 1 \Rightarrow p = 4n$, $n \in \mathbb{Z}$. Therefore Hecke characters on J look like $\chi(\langle a \rangle) = |a|^{iq}\left(\frac{a}{|a|}\right)^{4n}$

## The Finite Component

Let $K^{(M)} = \{a \in K^\times : (a, M) = 1\}$ $K^M = \{a \in K^\times : a \equiv 1 \pmod M\}$ $\mathcal{O}_K^M = \{a \in \mathcal{O}_K^\times : a \equiv 1 \pmod M\}$

Then $\chi_f(a) = 1$ $\forall a \in \mathcal{O}_K^M \Rightarrow \chi(\langle a \rangle) = \chi_\infty(a)$ $\forall a \in \mathcal{O}_K^M$

But $a \in \mathcal{O}_K^\times$ is a unit so $\chi(\langle a \rangle) = \chi_\infty(a) = 1$. so $\chi_\infty$ is a character on $(K \otimes \mathbb{R})^\times / \mathcal{O}_K^M$

$\Rightarrow$ Define $\chi_f: (\mathcal{O}_K/M)^\times \longrightarrow S^1$ by $\chi_f(a) = \frac{\chi(\langle a \rangle)}{\chi_\infty(a)}$

Proposition: Let $\chi \bmod M$ be a Hecke character. Let $M' \mid M$, the following are equivalent:

i) $\chi$ = restriction of Hecke character $\chi': J^{M'} \longrightarrow S' \bmod M'$

ii) $\chi_f$ factors through $(\mathcal{O}_K/M')^\times$

$\chi \pmod M$ is primitive if it is not the restriction of a $\chi' \bmod M'$ $\forall M' \mid M$

The conductor of $\chi$ is the smallest $f \mid M$ such that $\chi$ = restriction of a character $\pmod f$

# Arbitrary Number Fields

A modulus for $K$ is a function $M: \{\text{primes of } K\} \to \mathbb{Z}$ such that

i) $M(\mathfrak{p}) \geq 0$ $\forall$ prime $\mathfrak{p}$, $M(\mathfrak{p}) = 0$ for almost all $\mathfrak{p}$ (i.e. all but finitely many $\mathfrak{p}$)

ii) $\mathfrak{p}$ real $\Rightarrow M(\mathfrak{p}) \in \{0,1\}$

iii) $\mathfrak{p}$ complex $\Rightarrow M(\mathfrak{p}) = 0$

write $M = \prod_{\mathfrak{p}} \mathfrak{p}^{M(\mathfrak{p})}$

Decompose $M = M_0 M_\infty$ where $M_0$ = product of positive powers of prime ideals, $M_\infty$ = product of real primes

Definition: Given a modulus $M$, the ray class group mod $M$ is given by $C_M := J^M / P^M$ where

$J^M = \{\text{fractional ideals of } K \text{ coprime to } M\}$

$P^M = \{\text{principal fractional ideals } (a) \text{ of } K \text{ such that } a \equiv 1 \pmod{M_0} \text{ and } a \text{ totally positive } \forall \mathfrak{p} | M_\infty\}$

# December 5 (Jamal)

## Hecke L-Functions

Last time: Formally defined a modulus $\mathfrak{M} = \prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})} = \mathfrak{M}_0 \cdot \mathfrak{M}_\infty$

$\rightsquigarrow$ Ray class group mod $\mathfrak{M}$: $C_{\mathfrak{M}} = J^{\mathfrak{M}}/P^{\mathfrak{M}}$, where $J^{\mathfrak{M}} = \{$fractional ideals of $K$ coprime to $\mathfrak{M}\}$
$P^{\mathfrak{M}} = \{$principal fractional ideals $\langle a\rangle$ of $K$ such that $a \equiv 1 \pmod{\mathfrak{M}}$, $\tau(a) > 0 \ \forall \tau \mid \mathfrak{M}_\infty$

$\rightsquigarrow$ Define Hecke characters over arbitrary number fields

Definition: A (generalized) Dirichlet character mod $\mathfrak{M}$ is a character $\chi: C_{\mathfrak{M}} \to S^1$, i.e. a character $\chi: J^{\mathfrak{M}} \to S^1$ such that $\chi(P^{\mathfrak{M}}) = 1$

Proposition: These characters mod $\mathfrak{M}$ are precisely the Hecke characters mod $\mathfrak{M}$ of type $(p,0)$ i.e.

$$\chi_f(\langle a\rangle) = \chi_f(a)\cdot\chi_\infty(a) = \chi_f(a)\cdot N\left(\frac{a}{|a|}\right)^p, \quad p \in \mathbb{Z}^{r_1+r_2}$$

$$\text{Type}(p,q) \rightsquigarrow \chi_\infty(a) = |a|^{iq}\left(\frac{a}{|a|}\right)^p, \quad q \in \mathbb{R}^{r_1+r_2}$$

Given a Hecke character mod $\mathfrak{M}$, define the Hecke L-function attached to $\chi$ by:
For $0 \neq A \triangleleft \mathcal{O}_K$, $\chi(A) = 0$ if $(A, \mathfrak{M}) \neq 1$
Then $L(s,\chi) = \sum_{0 \neq A \triangleleft \mathcal{O}_K} \chi(A) N(A)^{-s}$, where $N(A) = \left|\mathcal{O}_K/A\right|$.

we have an Euler product $L(s,\chi) = \prod_{\substack{0 \neq \mathfrak{p} \triangleleft \mathcal{O}_K \\ \mathfrak{p} \text{ prime}}} (1 - \chi(\mathfrak{p})N(\mathfrak{p})^{-s})^{-1}$

Proposition: $L(s,\chi)$ converges absolutely and uniformly for $\text{Re}(s) \geq 1+\delta \ \forall \delta > 0$

Example: Hasse-Weil L-functions as Hecke L-functions
Must define an algebraic Hecke character first

Last time: $\chi: J^{\mathfrak{M}} \to S^1$, $\chi(\langle a\rangle) = \chi_f(a)\chi_\infty(a)$ where $\chi_\infty(a) = |a|^{iq}\left(\frac{a}{|a|}\right)^p$

More generally, define $\chi_\infty(a) = |a|^s\left(\frac{a}{|a|}\right)^p$, where $s \in \mathbb{C}$

(note: $|a| = (a\cdot\bar{a})^{1/2}$)

Let $K = \mathbb{Q}(i)$, $\mathcal{O}_K = \mathbb{Z}[i]$, $G = \text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \Rightarrow \chi(\langle a\rangle) = \chi_\infty(a) = |a|^s\left(\frac{a}{|a|}\right)^p = (a\bar{a})^{s/2}a^p(a\bar{a})^{-p/2} = a^{s+p/2}\bar{a}^{s-p/2}$

Let $\theta = \left(\frac{s+p}{2}\right)\text{id} + \left(\frac{s-p}{2}\right)j \in \mathbb{C}[G]$

we say that $\chi$ is algebraic if $\theta \in \mathbb{Z}[G]$. For such a $\theta$, we have that for $a \in \mathcal{O}_K$, $a \equiv 1 \pmod{\mathfrak{M}}$, $\chi(\langle a\rangle) = a^\theta$

Recall: Given an elliptic curve $E: y^2 = x^3 - Ax - B$
$\rightsquigarrow L(E,s) = \prod_{p \nmid \Delta}(1 - a_p p^{-s} + p^{1-2s})^{-1}$ where $a_p = p+1-N_p$, $N_p = \#E(\mathbb{F}_p)$

Example: $E: y^2 = x^3 - x$, $\mathrm{End}(E) = \mathbb{Z}[i]$, $\Delta(E) = 2^6$, so consider $p \neq 2$

Theorem: $p \equiv 3 \pmod 4 \Rightarrow N_p = p+1$. $p \equiv 1 \pmod 4 \Rightarrow p = \pi \cdot \overline{\pi}$, $\pi \in \mathbb{Z}[i]$, $\pi \equiv 1 \pmod{(2+2i)} \Rightarrow N_p = p+1-\pi-\overline{\pi}$

Goal: construct algebraic Hecke character $\chi$ on $\mathbb{Z}[i]$ of modulus $(8)$ such that $L(E,s) = L(s,\chi)$
If $p \mid (2)$ then $\chi(p) := 0$
If $N(p) = p$ prime, then $p \equiv 1 \pmod 4$ and $p = \pi \equiv 1 \pmod{(2+2i)} \Rightarrow \chi(p) = 1$
If $N(p) = p^2$, then $p \equiv 3 \pmod 4$ and $P = (p) \Rightarrow \chi(P) = -p$

Proposition: $\chi$ (defined above) is an algebraic Hecke character for modulus $(8)$ and $L(E,s) = L(s,\chi)$
Proof: Assume $p \neq 2$. If $p \equiv 3 \pmod 4$, then $N_p = p+1 \Rightarrow a_p = 0$.
Let $P = (p) \Rightarrow N(P) = p^2$ and $\chi(P) = -p$. $1 - a_p p^{-s} + p^{1-2s} = 1 + p^{1-2s} = 1 - (-p)(p^2)^{-s} = 1 - \chi(p) N(P)^{-s}$
If $p \equiv 1 \pmod 4$, then write $p\mathbb{Z}[i] = p\bar{p}$, $p = (\pi)$, $\pi \equiv 1 \pmod{(2+2i)}$, $N(P) = p$ and $a_p = \pi + \overline{\pi}$
Then $1 - a_p p^{-s} + p^{1-2s} = 1 - \pi p^{-s} - \overline{\pi} p^{-s} + \pi\overline{\pi} p^{-2s} = (1 - \pi p^{-s})(1 - \overline{\pi} p^{-s}) = (1 - \chi(P) N(P)^{-s})(1 - \chi(\bar{P}) N(\bar{P})^{-s})$
$\Rightarrow L(E,s) = L(s,\chi)$ ☒

## Analytic Continuation and the Functional Equation

Let $\chi$ be (without loss of generality assume unitary) a Hecke character mod $M$ of type $(p,q)$
i.e. $\chi_\infty(a) = N\left(|a|^{iq}\left(\frac{a}{|a|}\right)^p\right)$ Define $L_\infty(\chi,s) = N(\pi^{-s/2}) \int_{\mathbb{R}>0} N(e^{-y} y^{s/2}) \frac{dy}{y}$ (*)

Define the completed Hecke L-series: $\Lambda(\chi,s) = (|\Delta(K)|\, N(M))^{s/2} L_\infty(\chi,s) L(\chi,s)$

Theorem: If $M \neq 1$, then $\Lambda(\chi,s)$ has analytic continuation to all of $\mathbb{C}$. Moreover, $\Lambda(s,\chi) = W(\chi)\Lambda(1-s,\bar{\chi})$ where $|W(\chi)| = 1$

# December 12 (Rob)

Dirichlet Characters: $\chi: (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$

Kronecker Symbol: $\left(\frac{m}{n}\right)$

p odd prime: $\left(\frac{m}{p}\right) = \begin{cases} 1, & m \neq 0, \text{a square mod } p \\ -1, & m \neq 0, \text{non-square mod } p \\ 0, & p \mid m \end{cases}$

$K_d = \mathbb{Q}(\sqrt{d})$ quadratic field

$d \in \mathbb{Z}$ squarefree $\quad \mathcal{O}_d \subseteq K_d, \quad \Delta_{K_d} = \begin{cases} d, & d \equiv 1 \pmod 4 \\ 4d, & d \equiv 2,3 \pmod 4 \end{cases}$ $\quad \chi_d(a) := \left(\frac{\Delta_{K_d}}{a}\right)$ Dirichlet character of conductor $\Delta_{K_d}$

If $d=-1$, $\Delta = -4$ $\quad \chi_{-1}(a) = \left(\frac{-4}{a}\right) = \left(\frac{-1}{a}\right)$ $\quad \mathcal{O}_{-1} = \mathbb{Z}[i]$

$p \in \mathbb{Z}$, $p = ?$ in $\mathbb{Z}[i]$, $= \begin{cases} \pi_1\pi_2, & p \equiv 1 \pmod 4 \\ p, & p \equiv 3 \pmod 4 \\ \pi^2, & p = 2 \end{cases}$ $\quad \pi_1, \pi_2$ not associative

and $\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod 4 \\ -1, & p \equiv 3 \pmod 4 \\ 0, & p \equiv 2 \end{cases}$

Theorem: let $p \in \mathbb{Z}$, $\left(\frac{\Delta_{K_d}}{p}\right) = \chi_d(p) = \begin{cases} 1, & p = \pi_1\pi_2 \to \text{split} \\ -1, & p \text{ irreducible} \to \text{inert} \\ 0, & p = \pi^2 \to \text{ramified} \end{cases}$

Kronecker-Weber Theorem: If $K/\mathbb{Q}$ is Galois with $\mathrm{Gal}(K/\mathbb{Q})$ (finite) abelian, then $\exists\, N \in \mathbb{Z}_{\geq 1}$ such that $K \subseteq \mathbb{Q}(\mu_N)$, $\mu_N = \{\zeta \in \mathbb{C} : \zeta^N = 1\}$

$\mathbb{Q}(\zeta_N)$ $\quad e^{2\pi i/N}$

Definition: The least such N is called the conductor of K, $\mathfrak{f}_K$

Example: $\mathfrak{f}_{\mathbb{Q}(i)} = 4$, $\mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$ $\quad i = \zeta_4$

Example: $\mathfrak{f}_{\mathbb{Q}(\sqrt{5})}$ $\quad \zeta_5 = \cos\left(\frac{2\pi}{5}\right) + i\sin\left(\frac{2\pi}{5}\right)$ $\quad \frac{\zeta_5 + \zeta_5}{2} = \frac{\zeta_5 + \zeta_5^{-1}}{2} = \cos\left(\frac{2\pi}{5}\right) = \frac{1}{4}(-1+\sqrt{5})$

In fact, $\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\zeta_5 + \zeta_5^{-1})$ and $\mathfrak{f}_{\mathbb{Q}(\sqrt{5})} = 5$

Now: $\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

$(\zeta_N \mapsto \zeta_N^a) \longleftarrow\!\shortmid\, a$

So any Dirichlet character $\chi \bmod N$ can be thought of as $\chi^{\mathrm{Gal}}: \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/N)^\times \xrightarrow{\chi} \mathbb{C}$

$\ker(\chi^{\mathrm{Gal}}) \triangleq \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$

By Galois correspondence

$\mathbb{Q}(\mu_N)$

$\ker(\chi^{\mathrm{Gal}})$ |

$K_\chi = \mathbb{Q}(\mu_N)^{\ker(\chi^{\mathrm{Gal}})}$

| $\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})/\ker(\chi^{\mathrm{Gal}})$ (abelian)

$\mathbb{Q}$

so to every $\chi$, get $K_\chi/\mathbb{Q}$ abelian extension. Conversely, every abelian extension $K/\mathbb{Q}$ has attached to it

$\mathbb{Q}(\mu_{f_K})$
| $H_K \leq Gal(\mathbb{Q}(\mu_{f_K})/\mathbb{Q})$
$K$
| cyclic
$\mathbb{Q}$

and then a Dirichlet character $\chi_K$ such that $\ker(\chi_K^{Gal}) = H_K$

Get a bijection

| $K_\chi$ | $\{K/\mathbb{Q}$ finite cyclic$\}$ | $K$ |
|---|---|---|
| $\updownarrow$ | $\updownarrow$ | $\downarrow$ |
| $\chi$ | $\{\chi$ primitive Dirichlet$\}$ | $\chi_K$ |

Theorem: $K_d = \mathbb{Q}(\sqrt{d})$ (cyclic) and $\chi_d = \left(\frac{\Delta_{K_d}}{\cdot}\right)$, then $f_{K_d} = f_{\chi_d}$, $\chi_{K_d} = \chi_d$, $K_{\chi_d} = K_d$

$\chi^{Gal}: G_\mathbb{Q} \twoheadrightarrow Gal(\mathbb{Q}(\mu_N)/\mathbb{Q}) \xrightarrow{\chi^{Gal}} \mathbb{C}^\times$

$G_\mathbb{Q} = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$

$\overline{\mathbb{Q}}$
| $H$
$\mathbb{Q}(\mu_N)$
| $G_\mathbb{Q}/H$
$\mathbb{Q}$

so any $\chi: (\mathbb{Z}/N)^\times \to \mathbb{C}^\times$ gives $\chi^{Gal}: G_\mathbb{Q} \to \mathbb{C}^\times$

$\ker(\chi^{Gal}) \longleftrightarrow K_\chi$
|
$\mathbb{Q}$

$p \in \mathbb{Z}$, $p = \cdots$ in $\mathcal{O}_{K_\chi}$ if $n = [K_\chi : \mathbb{Q}]$

Say $p$ splits completely if $p = \pi_1 \pi_2 \cdots \pi_n$, $\pi_i$ irreducible and $\pi_i$ not associative to $\pi_j$ (for $i \neq j$)

Theorem: $p$ splits completely in $K_\chi$ if and only if $\chi(p) = 1$ if and only if $p \in \ker\chi \leq (\mathbb{Z}/f_{K_\chi})^\times$

Replace $\mathbb{Q}$ with $F/\mathbb{Q}$ finite

Class field theory

Key part: $rec_N: (\mathbb{Z}/N)^\times \xrightarrow{\sim} Gal(\mathbb{Q}(\mu_N)/\mathbb{Q})$

Artin reciprocity map

Get every abelian extension of F from one or more of $G_\mathbb{Q}$, equivalent Dirichlet characters

## Non-abelian Extensions

$\chi: G_\mathbb{Q} \to \mathbb{C}^\times = GL_1(\mathbb{C})$

A finite dimensional linear representation of $G_\mathbb{Q}$ is a homomorphism $\rho: G_\mathbb{Q} \to GL_d(\mathbb{C})$

Definition: An Artin representation of $\mathbb{Q}$ is $\rho: G_\mathbb{Q} \to GL_d(\mathbb{C})$

For characters $\chi$, the L-functions depended on $\chi(p)$, $L(s,\chi) = \prod_p (1 - \chi(p)p^{-s})^{-1}$

Key part: $\mathrm{rec}_N : (\mathbb{Z}/N)^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$

$p \longmapsto \mathrm{Frob}_p := \mathrm{rec}_N(p)$

"inertia at p" $\downarrow$

In fact, given p prime, have $\mathrm{Frob}_p \in G_{\mathbb{Q}}$ (up to conjugacy and some group $I_p \leq G_{\mathbb{Q}}$)

$\chi(p) = \chi^{\mathrm{Gal}}(\mathrm{Frob}_p)$

So $L(s,\chi) = \prod_p \left(1 - \chi^{\mathrm{Gal}}(\mathrm{Frob}_p) p^{-s}\right)^{-1}$

Given $\rho : G_{\mathbb{Q}} \longrightarrow GL_d(\mathbb{C})$, say $\rho$ is unramified at p if $\rho(I_p) = 1$ if $\rho$ is unramified at p, let

$Z_p(X, \rho) = \det(I - \rho(\mathrm{Frob}_p) X)$

Artin L-function of $\rho$ is $L(s,\rho) = \prod_{p \text{ unramified}} Z_p(p^{-s}, \rho)^{-1} \prod_{p \text{ ramified}} \ldots$

Example: If $K/\mathbb{Q}$ degree 8 and Galois with group $D_4$ and $\rho : D_4 \longrightarrow GL_2(\mathbb{C})$ say

$\rho(\mathrm{Frob}_p) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ rotation by $\frac{\pi}{2}$ $\qquad Z_p(X,\rho) = \left| \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 0 & -X \\ X & 0 \end{pmatrix} \right| = \begin{vmatrix} 1 & X \\ -X & 1 \end{vmatrix} = 1 + X^2 \rightsquigarrow (1 + p^{-2s})^{-1}$

For 2D representations, $\rho : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{C})$ get $L(s,\rho) = \prod_p (\text{polynomial of degree 2 in } p^{-s})^{-1}$

Conjecture (Langlands): Approx: $\forall \rho$ 2 dimensional, $\exists$ a modular form f of weight 1 such that $L(s,\rho) = L(s,f)$ in particular, $\forall p$ uniform for $\rho$ $\mathrm{tr}(\rho(\mathrm{Frob}_p)) = a_p(f)$