GALOIS REPRESENTATIONS AND L-FUNCTIONS
TCC 13.1.16 – 1.12.16

<u>Big picture</u>   [Fermat, Langlands, BSD, ...]

$\boxed{\text{L-functions}} \rightsquigarrow \boxed{\text{Galois representations}} \rightsquigarrow \boxed{\text{Varieties}}$ } this course

$\uparrow$

$\boxed{\text{Modular and automorphic forms}}$

Plan:

Riemann $\zeta(s)$	$\rightsquigarrow$	$\mathbb{1}$	$\rightsquigarrow$	$\bullet$
Dedekind ζ-functions $\zeta_K(s)$	$\rightsquigarrow$	permutation reps of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$	$\rightsquigarrow$	$\therefore \circlearrowleft \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$
Artin L-fncs	$\rightsquigarrow$	pieces of $\zeta_K(s)$, all finite image reps	$\rightsquigarrow$	dim 0
L-fncs of varieties / $\mathbb{Q}$	$\rightsquigarrow$	General Galois reps	$\rightsquigarrow$	dim > 0

} need number fields, Frobenius, inertia.

} need local fields, ell. curves.

§1 <u>Riemann ζ & L-functions</u>

← the only analysis in this course.

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}$$

$$= \left(1 + \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{8^s} + \dots\right)\left(1 + \frac{1}{3^s} + \frac{1}{9^s} + \dots\right)\cdots$$

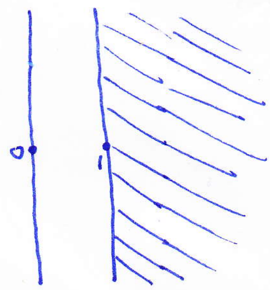
$$= \prod_p \frac{1}{1-p^{-s}}$$

Encodes distribution of primes, e.g.

$$\sum \frac{1}{n} = \infty \quad \Rightarrow \exists \infty \text{ primes.}$$

Viewed as fnc. of $\mathbb{C}$-variable $s = \sigma + it$

$$\left|\frac{1}{n^s}\right| = \frac{1}{n^\sigma} \quad \Rightarrow \quad \text{converges for } \operatorname{Re} s > 1.$$



Thm (Riemann)

$\zeta(s)$ has meromorphic cont. to $\mathbb{C}$, only poles at $s=0$ (simple, residue -1) and $s=1$ (simple, residue $=1$),

and the completed ζ-function

$$\hat{\zeta}(s) = \frac{1}{\pi^{s/2}}\,\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

or ξ or Λ

satisfies functional equation

$$\hat{\zeta}(s) = \hat{\zeta}(1-s)$$

Proof [Meromorphic cont. for $\sigma = \mathrm{Re}\, s > 0$ can be done directly

$$\zeta(s) - \frac{1}{s-1} = \sum_n \left[\frac{1}{n^s} - \int_n^{n+1} x^{-s}\,dx\right] = \sum_n \int_n^{n+1} \underbrace{\left(\frac{1}{n^s} - \frac{1}{x^s}\right)}_{|\cdot| \le |s|\, n^{-1-\sigma}} dx$$

converges to analytic fnc.]

Poisson summation formula: $f(n): \mathbb{R} \to \mathbb{C}$ $\left(C^2,\ |f + f''| = O\left(\frac{1}{|n|^r + 1}\right)\ \text{some } r > 1\right)$

$$(\mathcal{F}f)(m) = \int_{-\infty}^{\infty} e^{2\pi i n m} f(n)\,dn \qquad \text{Fourier transform}$$

Then $$\sum_{n\in\mathbb{Z}} f(n) = \sum_{m\in\mathbb{Z}} (\mathcal{F}f)(m).$$

Apply: $f(n) = e^{-\pi x n^2}$,

$$\Theta(x) := \sum_{n\in\mathbb{Z}} \overbrace{e^{-\pi x n^2}}^{f(n)} \overset{\text{Poisson}}{=} \sum_{m\in\mathbb{Z}} \overbrace{\frac{1}{\sqrt{x}} e^{-\frac{\pi}{x} m^2}}^{(\mathcal{F}f)(m)} = \frac{1}{\sqrt{x}}\,\Theta\left(\frac{1}{x}\right) \qquad (*)$$

← Θ-function (Jacobi)

Back to $\hat{\zeta}$:

$$\Gamma(s) = \int_0^\infty x^s e^{-x} \frac{dx}{x} \qquad \text{Mellin transform of } e^{-x} \quad ; \quad \Gamma(s+1) = s\,\Gamma(s)$$

$$\hat{\zeta}(2s) = \frac{1}{\pi^s}\Gamma(s)\underbrace{\zeta(2s)}_{\sum \frac{1}{n^{2s}}} = \int_0^\infty \sum_{n=1}^\infty \underbrace{\frac{x^s}{\pi^s n^{2s}}}_{\left(\frac{x}{\pi n^2}\right)^s} e^{-x}\frac{dx}{x} \overset{x \to \pi n^2 x}{=}$$

$$= \text{Mellin transform of } \underbrace{\sum_{n=1}^\infty e^{-\pi n^2 x}}_{\frac{\Theta(x)-1}{2}}.$$

Break $\int_0^\infty = \int_0^1 + \int_1^\infty$, replace $x \to \frac{1}{x}$ in 1st one using $(*)$ $\Rightarrow$

$$\hat{\zeta}(s) = \frac{1}{s-1} - \frac{1}{s} + \int_1^\infty \left(\frac{\Theta(x)-1}{2}\right)\left(x^{s/2} + x^{\frac{1-s}{2}}\right)\frac{dx}{x}$$

← symmetric under $s \mapsto 1-s$, converges everywhere

Def An <u>L-function</u> is a Dirichlet series

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \quad , a_n \in \mathbb{C} \ , \ a_n = O(n^r) \text{ some } r$$

($\Rightarrow$ converges on $\operatorname{Re} s > r+1$)

It has an <u>Euler product</u> and <u>has degree d</u> if

$$L(s) = \prod_p \frac{1}{F_p(p^{-s})} \qquad F_p(t) \in \mathbb{C}[t] \ \text{degree} \leq d, \ = d$$

for almost all p.

All L-fncs we will see are conjectured to (will satisfy this, and)

(A) Have <u>mer. cont</u> to $\mathbb{C}$ with fin. many poles (usually none)

(B) <u>Fun. eq.</u> : $\exists$ <u>weight</u> k, <u>sign</u> w, <u>conductor</u> N,

<u>Γ-factor</u> $\gamma(s) = \Gamma\left(\frac{s+\lambda_1}{2}\right) \cdots \Gamma\left(\frac{s+\lambda_d}{2}\right)$ s.t.

$$\hat{L}(s) = \left(\frac{N}{\pi^d}\right)^{s/2} \gamma(s) \, L(s)$$

satisfies

$$\hat{L}(s) = w \cdot \hat{\bar{L}}(k-s) \qquad [\bar{L}(s) = \sum \bar{a}_n n^{-s}]$$

(c) <u>Riemann Hypothesis</u> All non-trivial zeroes lie on $\operatorname{Re} s = \frac{k}{2}$ $\leftarrow$ Not known, ever

Rmks • If $L(s)$ satisfies (A)+(B) [say, no poles], as before

$$\hat{L}(s) = \int_1^{\infty} \left(x^{s/2} + w x^{\frac{k-s}{2}}\right) \Theta(\sqrt{N} \cdot x) \frac{dx}{x} \quad ; \quad \Theta(x) = \sum_{n=1}^{\infty} a_n \, \phi_{n,\gamma}(x)$$

depends only on $\gamma(s)$, decays exp. with n, e.g. $e^{-\pi n^2 x}$ for $\gamma = \Gamma(\frac{s}{2})$.

In fact, B $\Leftrightarrow$

$$\Theta\left(\frac{1}{Nx}\right) = w \cdot \Theta(x) \qquad (\ast\ast)$$

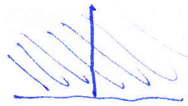
Gives a way to compute L-fncs numerically (with $\sim\sqrt{N}$ terms)

"measure of arithmetic complexity"

- There are functions called "modular forms"

$$f : \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\} \longrightarrow \mathbb{C}$$

[technically newforms of wt k, level N, w-eigenform for the Atkin-Lehner involution]



such that

$$\Theta(x) = f(ix)$$

satisfies $(**)$ by defn.

$\Rightarrow$ their L-functions satisfy $(A) + (B)$.

- 2 categories of L-fncs $L(s) = \sum \frac{a_n}{n^s}$:

(i) With a direct formula for the a_n,

[e.g. $\zeta(s)$ $\quad a_n = 1$

$L(\chi, s)$ $\quad$ Dirichlet, $a_n = \chi(n)$

$\zeta_K(s)$ $\quad$ Dedekind, $a_n = \#$ ideals of norm n in $\mathcal{O}_K$]

$\Rightarrow$ Generally know how to prove A + B.

(ii) Only defined by an Euler product

[e.g. $L(\rho, s)$ Artin,

$L(E, s)$ ell. curves

Other varieties, ...]

$\Rightarrow$ Never know how to prove A+B, except when can reduce to (i). !

§2 Dedekind ζ-functions

K number field, $[K : \mathbb{Q}] = d$

$\mathcal{O} = \mathcal{O}_K$ ring of integers,

$K \cong \mathbb{Q}^d$ a v.space

$\mathcal{O} \cong \mathbb{Z}^d$ as ab. group.

$I \subseteq \mathcal{O}_K$ ideal, $\neq 0$

$NI = (\mathcal{O}_K : I)$ norm, $< \infty$.

$N(IJ) = NI \cdot NJ$

I unique product of prime ideals

$$I = \prod_{i=1}^{r} \mathfrak{p}_i^{n_i}$$

$\mathcal{O}/\mathfrak{p}_i$ finite domain $\Rightarrow$ field $\mathbb{F}_{p^r}$

$\Rightarrow \mathfrak{p}_i \subseteq (p_i)$ some primes $p_i \in \mathbb{Z}$.

In particular, take $I = (p)$

$$(p) = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$$

$\mathfrak{p}_i$ = primes above p

e_i = ramification indices

($=1$ for a.a. p, namely $p \nmid \Delta_K$) called unramified primes in $K/\mathbb{Q}$

$f_i = [\mathcal{O}/\mathfrak{p}_i : \mathbb{F}_p]$ residue degrees

$$N(\mathfrak{p}) = [\mathcal{O} : p\mathcal{O}] = p^d \quad \Rightarrow \quad d = \sum_{i=1}^{r} e_i f_i \qquad \forall p$$

($\mathcal{O} \cong \mathbb{Z}^d$, $p\mathcal{O} \cong p\mathbb{Z}^d$)

$$\left[d = \sum_{i=1}^{r} f_i \text{ for unramified ones} \right].$$

N.B. If $K/\mathbb{Q}$ Galois, $e_1 = \dots = e_d$, $f_1 = \dots = f_d$ ($\mathrm{Gal}(K/\mathbb{Q})$ permutes $\mathfrak{p}_i$ transitively)

In practice:

Thm (Kummer–Dedekind) $K = \mathbb{Q}[x]/g(x)$, $g \in \mathbb{Z}[x]$, monic. Then $\Delta_K \mid \Delta_g$, and for all $p \nmid \Delta_g$, $p = \prod_{i=1}^{r} \mathfrak{p}_i$, we have

$$g(x) \equiv g_1 \cdots g_r \bmod p, \qquad \deg g_i = f_i.$$

Def The Dedekind ζ-function of K

$$\zeta_K(s) = \sum_{n \geq 1} \frac{a_n}{n^s} \qquad a_n = \#\{\text{ideals of norm } n \text{ in } \mathcal{O}_K\}$$

$$= \sum_{\substack{I \subseteq \mathcal{O}_K \\ I \neq 0}} \frac{1}{NI^s}$$

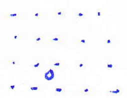
$$= \prod_{\mathfrak{p} \text{ prime}} \frac{1}{1 - N\mathfrak{p}^{-s}} \overset{\text{Exc}}{=} \prod_{\substack{p \\ \text{prime of } \mathbb{Z}}} \frac{1}{F_p(p^{-s})}$$

$F_p \in \mathbb{Z}[x]$ degree d for $p \nmid \Delta_K$, $< d$ for $p \mid \Delta_K$.

degree d L-function.

Ex $K = \mathbb{Q}(i)$

$\mathcal{O} = \mathbb{Z}[i]$ Gaussian integers, Euclidean $\Rightarrow$ PID. $\Rightarrow$ every ideal $I = (m+ni)$, $NI = m^2 + n^2$.



$\mathcal{O}^\times = \{\pm 1, \pm i\}$ units.

$[K : \mathbb{Q}] = 2 \Rightarrow$ every prime p of $\mathbb{Q}$ either

ramifies $(p) = \mathfrak{p}_1^2$

splits $(p) = \mathfrak{p}_1 \mathfrak{p}_2 = (\alpha + \beta i)(\alpha - \beta i)$

is inert (p) prime ideal, res. field $\mathcal{O}/(p) \cong \mathbb{F}_{p^2}$

Kummer–Dedekind for $g(x) = x^2 + 1 \Rightarrow$ all $p \neq 2$ unramified

(in fact $(2) = (1+i)^2$ ramifies ; $2 = (1+i)^2 \cdot \underbrace{(-i)}_{\text{unit}}$)

$p \equiv 3 \mod 4 \Rightarrow x^2+1$ irr. mod $p \Rightarrow p$ inert

$p \equiv 1 \mod 4 \Rightarrow -1 \in \underbrace{\mathbb{F}_p^{\times 2}}_{\text{cyclic gp, 4 | order}} \Rightarrow p$ splits. $\Rightarrow p = (a+bi)(a-bi) = a^2+b^2$.

e.g. $5 = 2^2+1^2$, $13 = 3^2+2^2$, ...

primes of $\mathbb{Z}[i]$ $\quad (1+i) \quad (3) \quad \begin{matrix}(2+i)\\(2-i)\end{matrix} \quad (7) \quad (11) \quad \begin{matrix}(3+2i)\\(3-2i)\end{matrix} \quad \cdots$

primes of $\mathbb{Z}$ $\quad 2 \quad 3 \quad 5 \quad 7 \quad 11 \quad 13 \quad \cdots$

2 ramified, 3 inert, 5 splits.

L

As for Riemann ζ,

$$\zeta_K(s) = \sum_{\substack{I \subseteq \mathbb{Z}[i]\\ I \neq 0}} \frac{1}{NI^s} = \sum_{\substack{0 \neq \alpha \in \mathbb{Z}[i]\\ \text{mod } \mathbb{Z}[i]^\times}} \frac{1}{(\alpha\bar\alpha)^s} = \frac{1}{4} \sum_{(m,n) \in \mathbb{Z}^2 \setminus \{0\}} \frac{1}{(m^2+n^2)^s}$$

and same computation $\Rightarrow \frac{2^s}{\pi^s}\Gamma(s)\zeta_K(s) =$ Mellin transform of $\frac{\Theta(x)-1}{4}$,

$$\Theta(x) = \sum_{m,n \in \mathbb{Z}} e^{-\pi(m^2+n^2)x} \Rightarrow$$

$$= \sum_m e^{-\pi m^2 x} \sum_n e^{-\pi n^2 x} = \frac{1}{\sqrt{x}}\frac{1}{\sqrt{x}}\Theta\left(\frac{1}{x}\right)$$

$\Rightarrow$ fun. eq. for $\zeta_K(s)$.

In general:

K number field, $[K:\mathbb{Q}] = d = r_1 + 2r_2$

$r_1 = \#$ real embeddings $K \hookrightarrow \mathbb{R}$
$r_2 = \#$ pairs of cpx emb. $K \hookrightarrow \mathbb{C}$
[$K = \mathbb{Q}[x]/g \rightarrow r_1 = \#$ real roots of g, $r_2 = \#$ pairs of cpx roots.]

$\mathcal{O} \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ $(\cong \mathbb{R}^d)$ lattice.

Poisson summation: $V = \mathbb{R}^d$, $f: V \to \mathbb{C}$ (decaying)

V^* dual v.space, $\mathcal{F}f: \underset{\text{dual}}{V^*} \to \mathbb{C}$ $\quad \mathcal{F}f(\underline{m}) = \int_V e^{-2\pi i \langle \underline{m}, \underline{n}\rangle} f(\underline{n})\, d\underline{n}$

$\Gamma \subseteq V$ rk d lattice $\Rightarrow$

$$\sum_{n \in \Gamma} f(n) = \frac{1}{\mathrm{vol}(V/\Gamma)} \sum_{m \in \Gamma^*} \mathcal{F}f(m).$$

Compare $\sum_{I \neq 0} \frac{1}{NI^s}$ to $\sum_{\substack{\alpha \in \mathcal{O}\\ \alpha \neq 0}} \frac{1}{N\alpha^s}$ $\quad \leftarrow$ involves $h = $ [ideals/principal ideals]
$\leftarrow$ units, roots of unity.

Poisson summation $\Rightarrow$