18.786: Number Theory II

(lecture notes)

Taught by Bjorn Poonen

Spring 2015, MIT

Last updated: May 14, 2015

Disclaimer

These are my notes from Prof. Poonen's course on number theory, given at MIT in spring 2015. I have made them public in the hope that they might be useful to others, but these are not official notes in any way. In particular, mistakes are my fault; if you find any, please report them to:

Eva Belmont
`ekbelmont at gmail.com`

Contents

LECTURE 1: FEBRUARY 3

Topics:

- Tate's thesis (what led to the Langlands program)
- Galois cohomology
- Introduction to Galois representation theory (also tied in to the Langlands program)

Reference (for Tate): Deitmar Introduction to harmonic analysis. Also, Bjorn will be posting official notes!

Before Tate, there was Riemann – the prototype for Tate's thesis is the analytic continuation and functional equation for the Riemann zeta function. For $\operatorname{Re} s > 1$, recall

$$\zeta(s) = \prod (1-p^{-s})^{-1} = \sum_{n\geq 1} n^{-s}.$$

Theorem 1.1 (Riemann, 1860). *(Analytic continuation) The function $\zeta(s)$ extends to a meromorphic function on $\mathbb{C}$, which is holomorphic except for a simple pole at 1.*

(Functional equation) The completed zeta function[1] $\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$*, where Γ is the gamma function, satisfies $\xi(s) = \xi(1-s)$.*

Hecke (1918, 1920) generalized this to $\zeta_K(s)$ and other L-functions. Margaret Matchett (1946) started reinterpreting this in adelic terms, and John Tate (1950) finished this in his Ph.D. thesis. (It's not just a reinterpretation: it gives more information than Hecke's proofs.)

Analytic prerequisites. Recall that the Gamma function is

$$\Gamma(s) = \int_0^\infty e^{-t} t^{-s} \frac{dt}{t}.$$

Note that e^{-t} is a function $\mathbb{R} \to \mathbb{C}^\times$ and t^{-s} (as a function of t) takes $\mathbb{R}^\times_{>0} \to \mathbb{C}^\times$ and $\frac{dt}{t}$ is a Haar measure on $\mathbb{R}^\times_{>0}$ (it's translation-invariant on the multiplicative group). (If you do this sort of thing over a finite field you get Gauss sums!)

This is convergent for $\operatorname{Re} s > 0$.

Proposition 1.2.

(1) $\Gamma(s+1) = s\Gamma(s)$ *(use integration by parts)*
(2) $\Gamma(s)$ *extends to a meromorphic function on $\mathbb{C}$ with simple poles at $0, -1, -2, \dots,$ and no zeros*
(3) $\Gamma(n) = (n-1)!$ *for $n \in \mathbb{Z}_{\geq 1}$*
(4) $\Gamma\frac{1}{2} = \sqrt{\pi}$ *(by a change of variables this is equivalent to $\int_{-\infty}^{\infty} e^{-x^2} dx = \sqrt{\pi}$)*

Now I'll review the Fourier transform.

[1] think of ξ as ζ with extra factors corresponding to the infinite places

Definition 1.3. $f : \mathbb{R} \to \mathbb{C}$ *tends to zero rapidly* if for every $n \geq 1$, $x^n f(x) \to 0$ as $|x| \to \infty$ (i.e. $|f(x)| = O\left(\frac{1}{|x|^n}\right)$).

Definition 1.4. Call $f : \mathbb{R} \to \mathbb{C}$ a *Schwartz function* if for every $r \geq 0$, $f^{(r)}$ tends to zero rapidly. Write $\mathscr{S} = \mathscr{S}(\mathbb{R})$ for the set of Schwartz functions.

Examples: e^{-x^2}, zero, bump functions (any C^∞ function with compact support).

Definition 1.5. Given $f \in \mathscr{S}$, define the Fourier transform

$$\widehat{f} = \int_{\mathbb{R}} f(x) e^{-2\pi i x y} dx.$$

Because f is a Schwartz function, this converges, and it turns out that $\widehat{f}$ is also a Schwartz function.

Example 1.6. If $f(x) = e^{-\pi x^2}$, then $f \in \mathscr{S}$ and $\widehat{f} = f$.

You can also define Fourier transforms on L^2. Eventually we'll have to generalize all of this from $\mathbb{R}$ to compact abelian groups.

Theorem 1.7 (Fourier inversion formula)**.** *If $f \in \mathscr{S}$ then*

$$f(x) = \int_{\mathbb{R}} \widehat{f} e^{2\pi i x y} dy.$$

In particular, $\widehat{\widehat{f}}(x) = f(-x)$.

Theorem 1.8 (Poisson summation formula)**.** *If $f \in \mathscr{S}$, then*

$$\sum_{n \in \mathbb{Z}} f(n) = \sum_{n \in \mathbb{Z}} \widehat{f}(n).$$

Definition 1.9. For real $t > 0$, define

$$\theta(t) = \sum_{n \in \mathbb{Z}} e^{-\pi n^2 t}.$$

This actually makes sense for any t in the right half plane. You can also define $\underline{\theta}(it) = \theta(t)$, defined in the upper half plane; it is a modular form.

In general, theta functions are associated to lattices. In this case, the lattice is just $\mathbb{Z} \subset \mathbb{R}$.

Theorem 1.10 (Functional equation of θ)**.** *For every real $t > 0$,*

$$\theta(t) = t^{-\frac{1}{2}} \theta\left(\frac{1}{t}\right).$$

PROOF. If $f \in \mathscr{S}$ and $c \neq 0$, then the Fourier transform of $f\left(\frac{x}{c}\right)$ is $c\widehat{f}(cy)$. Apply this to $f(x) = e^{-\pi x^2}$ and $c = t^{-\frac{1}{2}}$ to get that the Fourier transform of $f_t(x) = e^{-\pi t x^2}$ is $\widehat{f_t}(y) = t^{-\frac{1}{2}} e^{-\pi\left(\frac{1}{t}\right)y^2}$. Now apply the Poisson summation formula to $f_t(x)$ to get

$$e^{-\pi n^2 t} = \sum_{n\in\mathbb{Z}} t^{-\frac{1}{2}} e^{-\pi n^2\cdot\frac{1}{t}}.$$

□

Note that $\theta(t) = 1 + 2\sum_{n\geq 1} e^{-\pi n^2 t}$, so

$$\sum_{n\geq 1} e^{-\pi n^2 t} = \frac{\theta(t)-1}{2}.$$

PROOF OF THEOREM 1.1. Recall $\xi(s) = \sum_n \pi^{-s/2}\Gamma(\frac{s}{2})n^{-s}$; start by looking at an individual summand:

$$\pi^{-\frac{s}{2}}\Gamma\left(\tfrac{s}{2}\right)n^{-s} = \pi^{-\frac{s}{2}}n^{-s}\int_0^\infty e^{-x}x^{s/2}\frac{dx}{x}$$

Make a change of variables $x = \pi n^2 t$ and recall that $\frac{dx}{x}$ is translation-invariant:

$$= \int_0^\infty e^{-\pi n^2 t}t^{s/2}\frac{dt}{t}$$

Now sum over n. As long as you can justify interchanging the sum and integral,

$$\xi(s) = \int_0^\infty \frac{\theta(t)-1}{2}t^{s/2}\frac{dt}{t}$$

Why can you interchange the sum and integral? For $s \in \mathbb{R}_{>1}$, this is OK because everything is nonnegative and the sum on the left converges. In fact, $\sum\int\ldots$ converges absolutely for any complex s: changing the imaginary part does not affect the absolute value $|t^{s/2}|$.

If $s < 0$, you can't expect this to make any sense: if t is close to zero, then the $t^{s/2}$ part won't converge, and the θ part doesn't help enough. Now I want to replace this expression with something that *does* make sense for all s.

Plan: we have

$$\xi(s) = \underbrace{\int_1^\infty \frac{\theta(t)-1}{2}t^{s/2}\frac{dt}{t}}_{I(s)} + \int_0^1 \frac{\theta(t)-1}{2}t^{s/2}\frac{dt}{t}$$

where $I(s)$ converges for all $s \in \mathbb{C}$: this is because $\frac{\theta(t)-1}{2} = \sum_{n\geq 1} e^{-\pi n^2 t}$, and as $t \to \infty$, the first term ($n = 1$) dominates. The second part is problematic for some s. We will fix it by using the functional equation for θ.

First do the substitution $t \mapsto \frac{1}{t}$, which sends $\frac{dt}{t} \mapsto -\frac{dt}{t}$:

$$\int_0^1 \frac{\theta(t)-1}{2}t^{s/2}\frac{dt}{t} = \int_1^\infty \left(\frac{\theta\left(\frac{1}{t}\right)-1}{2}\right)t^{-\frac{s}{2}}\frac{dt}{t}$$

Now use the functional equation $\theta(t) = t^{-\frac{1}{2}}\theta\left(\frac{1}{t}\right)$

$$= \int_1^\infty \left(\frac{t^{\frac{1}{2}}\theta(t) - 1}{2}\right) t^{-\frac{s}{2}} \frac{dt}{t}$$

$$= \int_1^\infty \frac{\theta(t)-1}{2} \cdot t^{\frac{1-s}{2}} \frac{dt}{t} + \int_1^\infty t^{\frac{1-s}{2}} \frac{dt}{t} - \int_1^\infty t^{-\frac{s}{2}} \frac{dt}{t}$$

$$= I(1-s) - \frac{1}{1-s} - \frac{1}{s}$$

Putting all of this together, we have

$$\xi(s) = I(s) + I(1-s) - \frac{1}{1-s} - \frac{1}{s};$$

this is true for $\operatorname{Re} s > 1$, but you can take the RHS as the meromorphic continuation of $\xi(s)$ for all s.

The conclusion is that

$$\zeta(s) = \frac{\xi(s)}{\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)}$$

is meromorphic. ξ has poles at 0 and 1, and you don't get any new poles from zeros of the denominator. The denominator has simple poles at $0, -2, -4, \dots$, which cancels out the pole in the numerator at 0. So ζ is meromorphic, and holomorphic except for a simple pole at $s = 1$. □

The above used the Poisson summation formula for $\mathbb{Z} \subset \mathbb{R}$. The idea is to replace this with a Poisson summation formula for $K \subset \mathbb{A}_K$. This will require a certain amount of analysis review.

Measure theory review. Let X be a set, and $\mathscr{M}$ be a collection of subsets of X.

Definition 1.11. $\mathscr{M}$ is a σ-algebra if $\mathscr{M}$ is closed under complementation and countable unions (including finite unions).

Example 1.12. If X is a topological space, the set $B = B(X)$ of Borel subsets is the smallest σ-algebra containing all the open subsets.

Fix a σ-algebra $\mathscr{M}$ on a set X; this will be the collection of *measurable sets.*

Definition 1.13. $f : X \to \mathbb{C}$ is *measurable* if inverse images of measurable sets are measurable.

For example, if $S \in B(\mathbb{C})$, then $f^{-1}S \in \mathscr{M}$. If f is real-valued, it is enough to check $f^{-1}S \in \mathscr{M}$ for S of the form (a, ∞).

Definition 1.14. A *measure* on $(X, \mathscr{M})$ is a function $\mu : \mathscr{M} \to [0, \infty]$ such that $\mu(\bigcup A_i) = \sum \mu(A_i)$ for any countable (or finite) collection of disjoint sets $A_i \in \mathscr{M}$. If $\mathscr{M} = B$, μ is called a *Borel measure.*

Definition 1.15. $N \subset X$ is a *null set* if $N \subset$ a measure-zero set (even if it's not measurable).

Call $f : X \to \mathbb{C}$ a *null function* if $\{x \in X \,:\, f(x) \neq 0\}$ is a null set.

It is easy and convenient to enlarge $\mathscr{M}$ so that all null sets are in $\mathscr{M}$.

Now let's integrate. Fix $(X, \mathscr{M}, \mu)$. Given $S \in \mathscr{M}$ with $\mu(S) < \infty$, let 1_S be the function that is 1 on S and 0 outside S. Define $\int 1_S := \mu(S)$.

Definition 1.16. A *step function* is a finite $\mathbb{C}$-linear combination of functions of the form 1_S. If f is a step function, define $\int f$ so that it's linear in f.

Define the L^1-norm $\|f\|_1 := \int |f| \in \mathbb{R}_{\geq 0}$. This leads to a notion of distance, and Cauchy sequences, in the space of functions.

Say $f : X \to \mathbb{C}$ is *integrable* if, outside a measure 0 set, it equals the pointwise limit of an L^1-Cauchy sequence (f_i) of step functions. Then define $\int f = \int_X f d\mu := \lim_{i\to\infty} \int f_i \in \mathbb{C}$.

Notation: if f, g are functions on X and I write $f \leq g$, I mean implicitly that f, g are functions $X \to [0, \infty]$, and $f(x) \leq g(x)$ for all $x \in X$).

For $f \geq 0$, the alternative definition

$$\int f = \sup \left\{ \int g \,:\, g \text{ is a step function with } 0 \leq g \leq f \right\}$$

agrees with the previous one and gives ∞ if f is not integrable.

Lecture 2: February 5

Last time we said that if we have a set X, a set of measurable subsets $\mathscr{M}$, and a measure μ, you can talk about the integral $\int f d\mu$ of an integrable function f. For measurable functions $f : X \to \mathbb{C}$, f is integrable iff $|f|$ is integrable. Now we have two theorems for interchanging limits and integrals:

Theorem 2.1 (Monotone convergence theorem)**.** *Suppose (f_n) is a sequence of measurable functions $X \to [0, \infty]$ such that $0 \leq f_1 \leq f_2 \leq \dots$ and we can define $f = \lim f_n$ (note we are allowing the pointwise limits to be ∞). Then $\int f_n \to \int f$.*

Theorem 2.2 (Dominated convergence theorem)**.** *Let f_1, f_2 and f be measurable functions $X \to \mathbb{C}$ such that $f_n \to f$ pointwise. If there is an integrable function $g : X \to \mathbb{C}$ such that $|f_n| \leq |g|$ for all n, then all the f_n and f are integrable, and $\int f_n \to \int f$.*

Variant 2.3. Instead of $f_1, f_2, \dots$, you can consider a family of functions $f(x, t)$ depending on the parameter t, and ask about $\lim_{t\to 0} f(x, t)$ instead of $\lim_{n\to\infty} f_n$. The same thing holds for this setting.

Definition 2.4 (L^p spaces)**.** For $p \in \mathbb{R}_{>1}$, define

$$\mathcal{L}^p(X) := \{\text{measurable functions } f : X \to \mathbb{C} \text{ s.t. } |f|^p \text{ is integrable}\}.$$

(Note that this depends on $\mathscr{M}$ and μ as well, but including this makes the notation unwieldy.)

Define the L^p-norm of $f \in \mathcal{L}^p(X)$ by

$$\|f\|_p := \left(\int |f|^p\right)^{\frac{1}{p}}.$$

$\| \ \|_p$ is almost a norm on $\mathcal{L}^p(X)$, except that there could be nonzero functions f with $\|f\|_p = 0$, namely the null functions. To fix this, define

$$L^p(X) := \mathcal{L}^p(X)/\{\text{null functions}\}.$$

This is a Banach space with the $\| \ \|_p$ norm.

$L^2(X)$ is also a Hilbert space under the Hermitian inner product $\langle f, g\rangle := \int f\overline{g} \in \mathbb{C}$.

Definition 2.5. A Hausdorff topological space is called *locally compact* if every $x \in X$ has a compact neighborhood (i.e. a compact set that contains an open neighborhood).

From now on, X is a locally compact Hausdorff topological space. On such a space, measures correspond to integrals.

Definition 2.6. An *outer Radon measure* on X is a Borel measure $\mu : B \to [0, \infty]$ that is:

- *locally finite*: every $x \in X$ has an open neighborhood U such that $\mu(U) < \infty$,
- *outer regular*: every Borel set $S \in B$ can be "approximated from above", i.e. $\mu(S) = \inf_{\text{open } U \supset S} \mu(U)$, and
- *inner regular on open sets*: every open $U \subset X$ satisfies $\mu(U) = \sup_{\text{compact } K \subset U} \mu(K)$.

Definition 2.7. A function $f : X \to \mathbb{C}$ has *compact support* if the closure of $\{x \in X : f(x) \neq 0\}$ is compact. Write $C(X)$ for the set of continuous functions $X \to \mathbb{C}$, and $C_c(X)$ for the set of continuous functions of compact support.

Definition 2.8. A *Radon integral* on X is a $\mathbb{C}$-linear map $I : C_c(X) \to \mathbb{C}$ such that $I(f) \geq 0$.

Given an outer Radon measure μ, you can get a Radon integral

$$I_\mu : C_c(X) \to \mathbb{C} \text{ by } f \mapsto \int_X f d\mu.$$

It turns out that the converse holds too.

Theorem 2.9 (Riesz representation theorem)**.** *Let X be a locally compact Hausdorff space. Then there is a bijection*

$$\{\textit{outer Radon measures on } X\} \longleftrightarrow \{\textit{Radon integrals on } X\}$$

where the forwards map sends $\mu \mapsto I_\mu$.

You can use this to construct Radon measures, if it is easier to construct the integral.

Example 2.10. Let $X = \mathbb{R}^n$. Consider the Radon integral $C_c(\mathbb{R}^n) \to \mathbb{C}$ sending $f \mapsto \int_{\mathbb{R}^n} f$ (where $\int$ means the Riemann integral). By the theorem, there is a corresponding Radon measure; this is *Lebesgue measure.*

Definition 2.11. A *topological group* is a topological space G equipped with a group structure such that the multiplication map $G \times G \to G$ and the inverse map $G \to G$ are continuous.

Equivalently, it's just a group in the category of topological spaces.

Definition 2.12. A Borel measure μ is *left-invariant* if $\mu(gS) = \mu(S)$ for all $g \in G$ and $S \in B$.

For example, Lebesgue measure is left (and right) invariant.

You can guess what right invariant means. . . These don't have to be the same – the group doesn't have to be abelian.

From now on, G is a locally compact Hausdorff topological group. For example: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$, $\mathbb{Q}_p$, $\mathbb{A}$ (adele ring of any global field) are topological groups under addition. The unit group $A^\times$ of any of these rings A are topological groups under multiplication. These are abelian, but $GL_n(A)$ isn't. Or, consider any group with the discrete topology.

Definition 2.13. A *left Haar measure* on G is a nonzero left-invariant outer Radon measure on G.

Theorem 2.14. *There exists a left Haar measure μ on G, and every other Haar measure on G is $c\mu$ for a scalar $c \in \mathbb{R}_{>0}$.*

By the Riesz representation theorem, you also get a Haar integral.

Warning 2.15. A left Haar measure μ need not be right-invariant.

If $g \in G$, then define $\mu_g(S) := \mu(Sg)$; this is still a left Haar measure. By the theorem, you can write $\mu_g = \Delta(g)\mu$ for some constant $\Delta(g)$, called the *modular function.* In fact, $\Delta : G \to \mathbb{R}^\times_{>0}$ is a homomorphism. If G is abelian, then left-invariant measures are right-invariant, and $\Delta \equiv 1$. If G is compact, then $\Delta \equiv 1$ as well (its image in $\mathbb{R}^\times_{>0}$ has to be a compact subgroup, and there's only one of those). In this case, say G is *unimodular.*

A group that is not unimodular is subgroup of $GL_2(\mathbb{R})$ consisting of matrices $\begin{pmatrix} 1 & * \\ & * \end{pmatrix}$.

Definition 2.16. An *LCA group* is a locally compact abelian Hausdorff topological group. LCA groups, along with continuous homomorphisms, form a category.

$0 \to A \to B \to C \to 0$ is a short exact sequence of LCA groups if:

- it is a short exact sequence, A, B, and C are LCA groups, and the homomorphisms are continuous;
- the induced homomorphism $B/A \to C$ identifies the quotient topology on B/A with the topology on C, and the topology on A has the subspace topology inherited from B.

In this case, A is identified with a *closed* subgroup since otherwise B/A would not be Hausdorff. Given Haar measures on any two of A, B, C, there exists a unique Haar measure on the third such that the three Haar measures da, db, and dc satisfy

$$\int_B f(b)db = \int_C \underbrace{\int_A f(\underbrace{c}_{\in B}\, a)da}_{\substack{\text{depends only} \\ \text{on } cA \in B/A \cong C}} dc$$

for every $f \in C_c(B)$.

Let G be an LCA group.

Let $\mathbb{T} = \{x \in \mathbb{C} : |z| = 1\}$ denote the group under multiplication; this is $\cong \mathbb{R}/\mathbb{Z}$ as a topological group. This is sometimes called $U(1)$ or even S^1.

Definition 2.17. A *character* of G is a continuous homomorphism $\chi : G \to \mathbb{C}^\times$. A *unitary character* of G is a continuous homomorphism $\chi : G \to \mathbb{T}$. (Some people use "character" to mean our unitary characters, and call our characters "quasi-characters".)

Since our groups are abelian, all of the characters are 1-dimensional.

Definition 2.18. The *Pontryagin dual* of G is

$$\widehat{G} := \mathrm{Hom}_{conts}(G, \mathbb{T}) = \{\text{unitary characters of } G\}.$$

This is an abelian group under pointwise multiplication of functions. You can make this into a topological group by using the compact-open topology (the topology generated by sets $\{\chi \in \widehat{G} : \chi(K) \subset U\}$ for every compact $K \subset G$ and open $U \subset \mathbb{T}$).

It turns out that $\widehat{G}$ is another LCA group. Any continuous homomorphism $G \to H$ induces a continuous homomorphism $\widehat{H} \to \widehat{G}$ sending $H \xrightarrow{\chi} \mathbb{T}$ to $G \to H \xrightarrow{\chi} \mathbb{T}$. $\widehat{(-)}$ is a contravariant functor the set of LCA groups to itself. If $0 \to A \to B \to C \to 0$ is exact, then so is $0 \to \widehat{C} \to \widehat{B} \to \widehat{A} \to 0$.

Theorem 2.19 (Pontryagin duality theorem)**.** *The canonical homomorphism $G \to \widehat{\widehat{G}}$ sending $g \mapsto (\chi \mapsto \chi(g))$ is an isomorphism of LCA groups.*

If H is the Pontryagin dual of G, then there exists a continuous bilinear pairing $G \times H \to \mathbb{T}$ sending $(g, \chi) \mapsto \chi(g)$. Pontryagin duality says that the roles of G and H are interchangeable.

G	$\widehat{G}$	
$\mathbb{R}$	$\mathbb{R}$	
$\mathbb{Q}_p$	$\mathbb{Q}_p$	
$\mathbb{A}$	$\mathbb{A}$	
$\mathbb{Z}$	$\mathbb{T}$	(just have to say where 1 goes)
$\mathbb{Z}_p$	$\mathbb{Q}_p/\mathbb{Z}_p$	$(\widehat{\varinjlim} = \varprojlim)$
finite	finite	
discrete	compact	
discrete torsion	profinite	(discrete torsion group is an injective limit of finite groups)

Example 2.20. The self-duality of $\mathbb{R}$ is given by the pairing $\mathbb{R} \times \mathbb{R} \to \mathbb{T}$ sending $(x, y) \mapsto e^{2\pi ixy}$. In other words, we are claiming that the homomorphism $\mathbb{R} \to \widehat{\mathbb{R}}$ sending $y \mapsto \chi_y(x) = e^{2\pi ixy}$ is an isomorphism of LCA groups. We'll prove this later for all local fields.

Fourier transform. Recall: if $f \in \mathscr{S}(R)$ then we defined

$$\widehat{f}(y) := \int_{\mathbb{R}} f(x)e^{-2\pi ixy}dx.$$

Definition 2.21. If $f \in \mathcal{L}^1(G)$, define the Fourier transform $\widehat{f} : \widehat{G} \to \mathbb{C}$

$$\widehat{f}(\chi) := \int_G f(g)\overline{\chi(g)}dg.$$

Even if f is not continuous, the Fourier transform is not continuous.

Lecture 3: February 12

There is a pairing $G \times \widehat{G} \to \mathbb{T}$, and if $H \leq G$, you can use the pairing to define an orthogonal $H^\perp = \{\chi \in \widehat{G} \,:\, \chi(h) = 1 \ \forall h \in H\}$.

Definition 3.1. For $f \in \mathcal{L}^1(G)$, we defined a Fourier transform $\widehat{f} : \widehat{G} \to \mathbb{C}$ by

$$\widehat{f}(\chi) = \int_G f(g)\overline{\chi(g)}dg.$$

Theorem 3.2 (Fourier inversion formula)**.** *If G is an LCA group and dg is a Haar measure, then there exists a unique Haar measure $d\chi$ ("dual measure", "Plancherel measure") on $\widehat{G}$ such that if $\in \mathcal{L}^1(G)$ is such that $\widehat{f} \in \mathcal{L}^1(\widehat{G})$ then*

$$f(g) = \int_{\widehat{G}} \widehat{f}(\chi)\chi(g)d\chi$$

for almost all (i.e. "outside a null set") $g \in G$. If f is continuous then it holds for all $g \in G$.

Another way of saying this is

$$\widehat{\widehat{f}}(x) = f(-x).$$

Theorem 3.3 (Plancherel theorem)**.** *Let dg and $d\chi$ be dual measures on G and $\widehat{G}$, respectively. If $f \in \mathcal{L}^1(G) \cap \mathcal{L}^2(G)$ then $\|f\|_2 = \|\widehat{f}\|_2$. (Implicit in this is the claim that $\widehat{f} \in \mathcal{L}^2(\widehat{G})$.)*

Corollary 3.4. *The map $L^1(G) \cap L^2(G) \to L^2(\widehat{G})$ sending $f \mapsto \widehat{f}$ extends to a map $L^2(G) \to L^2(\widehat{G})$ and this extended Fourier transform is an isomorphism of Hilbert spaces.*

Proof of Corollary 3.4. According to the Plancherel theorem, $f \mapsto \widehat{f}$ maps L^2-Cauchy sequences to L^2-Cauchy sequences. So the Fourier transform extends to the completion of $L^1(G) \cap L^2(G)$ w.r.t. $\| \;\; \|_2$. I claim that $L^1(G) \cap L^2(G)$ is dense; in fact, even the subspace $C_c(G) \subset L^1(G) \cap L^2(G)$ of continuous functions with compact support is dense. The Plancherel theorem implies that the map $L^2(G) \to L^2(\widehat{G})$ sending $f \mapsto \widehat{f}$ preserves $\| \;\; \|_2$. The extended Fourier transform on $\widehat{G}$ (with negation) gives the inverse. □

A lot of this theory generalizes to locally compact *nonabelian* groups, but instead of looking at just characters, you have to look at higher-dimensional representations.

Local fields.

Definition 3.5. A *local field* is a field satisfying one of the following definitions:

(1) F is $\mathbb{R}$ or $\mathbb{C}$, or the fraction field of a complete DVR with finite residue field (some people don't agree with the latter condition);
(2) F is a finite separable extension of $\mathbb{R}$, $\mathbb{Q}_p$, or $\mathbb{F}_p((t))$ for some prime p;
(3) F is the completion of a global field;
(4) F is a nondiscrete locally compact topological field.

Note that F isn't just a field; it's a field that comes with a topology. For proof that these are equivalent, see the book in the references list. (4) is there for motivation – it's the least ad hoc definition; but most of the time, we want to use one of the other ones.

From now on, F will denote a local field.

Recall that $\mathbb{R}$ and $\mathbb{C}$ are archimedean, and the fraction field of a complete DVR is nonarchimedean. In this case, write

- $\mathcal{O}$ is the valuation ring
- $\mathfrak{p}$ is the maximal ideal of $\mathcal{O}$
- k is the residue field $\mathcal{O}/\mathfrak{p}$
- ϖ is the uniformizer
- p is the characteristic of k
- q is the cardinality of k

Let μ be a Haar measure on F. Let $a \in F$ (nonzero), so $F \overset{a}{\to} F$ is an isomorphism of LCA groups. So $S \mapsto \mu(aS)$ is another Haar measure μ_a, and there is some number $|a| \in \mathbb{R}_{>0}$ such that $\mu = |a|\mu$. Note that $|a|$ is independent of μ. In particular,

- if $F = \mathbb{R}$ then $|a|$ is the ordinary absolute value;
- if $F = \mathbb{C}$ then $|a|$ is the square of the ordinary absolute value (so it's not an absolute value at all since the triangle inequality fails);
- if F is nonarchimedean and $a \in \mathcal{O}$, then $|a| = \#(\mathcal{O}/a\mathcal{O})^{-1}$.

The "absolute value" defines the topology on F.

Say that $S \subset F^n$ is a bounded subset if it is bounded w.r.t. the sup norm:

$$\|(x_1, \dots, x_n)\| := \sup_i |x_i|.$$

Theorem 3.6 (Heine-Borel theorem for local fields)**.** *Let $S \subset F^n$ for any $n \geq 0$. Then S has compact closure iff S is bounded.*

Additive characters. You know there are nontrivial additive characters, because otherwise that violates Pontryagin duality. So fix a nontrivial unitary character $\psi : F \to \mathbb{T}$. Given $a \in F$, define $\psi_a(x) := \psi(ax)$. The theorem says that this describes all of them.

Theorem 3.7. *The map $\Psi : F \mapsto \widehat{F}$ sending $a \mapsto \psi_a$ is an isomorphism of LCA groups.*

Proof. Ψ is an injective homomorphism (if $\psi_a \equiv 1$ then we need $a = 0$; but this means that $\psi(ax) = 1$ for all x, which can only happen if $a = 0$). Compare the original topology on F to the topology on F given by the subspace topology on $\Psi(F) \subset \widehat{F}$. A basis of neighborhoods of 0 in the latter consists of sets $\{a \in F : \psi_a(K) \subset U\} = \{a \in F : aK \subset \varphi^{-1}U\}$ (where K is compact and U is open, containing 1). We need to check:

(1) Given compact K and open $U \ni 1$, does there exist $\delta > 0$ such that $|a| < \delta \implies aK \subset \psi^{-1}U$?
(2) Given $\varepsilon > 0$, does there exist K, $U \ni 1$ such that $aK \subset \psi^{-1}U \implies |a| < \varepsilon$?

For (1), the answer is yes, because K is bounded and $\psi^{-1}U$ contains an open disk around 0 (so multiplying K by a small enough a will get it into this disk).

For (2), the answer is also yes: choose b such that $\psi(b) \neq 1$, and choose $U \ni 1$ so that $\psi(b) \notin U$, i.e. $b \notin \psi^{-1}U$. Choose K to be a closed disk centered at 0 of radius $\geq |b|/\varepsilon$. Then $aK \subset \psi^{-1}U$ implies $b \notin aK$, so $|b| > |a| \cdot \frac{|b|}{\varepsilon}$, so $|a| < \varepsilon$. (Idea: choose K so big that if a scales it into $\varphi^{-1}U$, a must have been really small.)

Since F is locally compact, F is complete, so $\Psi(F)$ is complete, so $\Psi(F)$ is closed in $\widehat{F}$. We want to show that $\Psi(F) = \widehat{F}$, or equivalently $\Psi(F)^\perp = 0$. There is an order-reversing bijection, given by $\perp$, between closed subgroups of F and closed subgroups of $\widehat{F}$. If $x \in \Psi(F)^\perp$, then $\psi_a(x) = 0$ for all a, so $\psi(ax) = 0$ for all a, so $x = 0$. □

There is a standard ψ on each of our favorite local fields F:

- If $F = \mathbb{R}$, $\psi(x) = e^{-2\pi i x}$

- If $F = \mathbb{Q}_p$, ψ is the map $\mathbb{Q}_p \twoheadrightarrow \mathbb{Q}_p/\mathbb{Z}_p \overset{\cong}{\leftarrow} \mathbb{Z}[p]/\mathbb{Z} \hookrightarrow \mathbb{R}/\mathbb{Z} \cong \mathbb{T}$. ψ is characterized by $\psi|_{\mathbb{Z}_p} = 1$ and $\psi(1/p^n) = e^{2\pi i/p^n}$ for all $n \geq 1$.
- If $F = \mathbb{F}_p((t))$, define $\psi(\sum a_i t^i) := e^{2\pi i a_i/p}$ (lifting a_i from $\mathbb{F}_p$ to $\mathbb{Z}$).

If F_0 is one of the three fields above, and ψ_0 is the standard character on F_0, and F is a finite separable extension of F_0, define the standard character on F by the composition $F \xrightarrow{\mathrm{Tr}_{F/F_0}} F_0 \xrightarrow{\psi_0} \mathbb{T}$. Since F/F_0 is separable, the trace map is surjective, so this is nontrivial. This describes ψ on all local fields.

There is a generalization of Schwartz functions: Schwartz functions on $\mathbb{R}^n$ (i.e. functions $\mathbb{R}^n \to \mathbb{C}^n$) are functions such that the partial derivatives decay rapidly. For arbitrary F, you don't want to talk about differentiable functions $F \to \mathbb{C}$, because it's unclear how to define the difference quotient in the derivative. So our cop-out is to use locally constant functions instead of C^∞ functions.

Definition 3.8. $f : F \to \mathbb{C}$ is called a *Schwartz-Bruhat function* if:

- it is a Schwartz function if $F = \mathbb{R}$ or $F = \mathbb{C}$; OR
- it is a locally constant function of compact support if F is nonarchimedean.

As before, use the notation $\mathscr{S} = \mathscr{S}(F)$ for the set of SB functions. These functions take complex values, so it is a $\mathbb{C}$-vector space.

If F is nonarchimedean and $f \in \mathscr{S}$, then *supp*(f) is covered by finitely many disjoint open disks on which f is constant. So f is a finite $\mathbb{C}$-linear combination of functions $\mathbb{1}_{D_i}$.

Lecture 4: February 19

RECALL: if you fix one nontrivial character, then you get all the other ones. We also defined Schwartz-Bruhat functions, which are Schwartz functions if $F = \mathbb{R}$ or $\mathbb{C}$, and locally constant with compact support if F is nonarchimedean.

Definition 4.1. Suppose F is nonarchimedean, and ψ is a nontrivial additive character. Look at ψ^{-1}(right half of $\mathbb{T}$); because F is nonarchimedean, this neighborhood contains a little subgroup, and that subgroup would have to map to a subgroup in $\mathbb{T}$. But there is no subgroup contained in the right half of $\mathbb{T}$ other than the trivial one. So $\psi|_{\mathfrak{p}^m} = 1$ for some $m \in \mathbb{Z}$. Choose the smallest such m. Then $\mathfrak{p}^m$ is called the *conductor* of ψ.

Fourier transform for local fields. Fix a field F, an additive character ψ, and a Haar measure dx on F. Given $f \in \mathscr{S}$, define

$$\widehat{f}(y) := \int_F f(x)\psi(xy)dx.$$

(Note: no complex conjugate.) It turns out that $\widehat{f} \in \mathscr{S}$.

Note that $\widehat{\widehat{f}}(x) = rf(-x)$ for some $r \in \mathbb{R}_{>0}$. We could arrange $r = 1$ by scaling dx, so that

$$f(x) = \int_F \widehat{f}(y)\overline{\psi(xy)}dy$$

for all $x \in F$.

Proposition 4.2. *The self-dual dx (wrt the standard ψ) is:*

- *if $F = \mathbb{R}$ then dx is the Lebesgue measure;*
- *if $F = \mathbb{C}$ then $dx = 2\cdot$ the Lebesgue measure;*
- *if F is nonarchimedean, then dx is such that* $\mathrm{vol}(\mathcal{O}) = (N\mathscr{D})^{-\frac{1}{2}}$ *where $\mathscr{D}$ is the different of F/F_0 (where F_0 is $\mathbb{F}_p$ or $\mathbb{F}_p((t))$).*

Proof. For $\mathbb{R}$, choose $f(x) = e^{-\pi x^2}$. Then $\widehat{f} = f$ and $\widehat{\widehat{f}}(x) = f(x) = f(-x)$. For $\mathbb{C}$, $f(z) = e^{-2\pi z\overline{z}}$; do the same thing.

If F is nonarchimedean, consider $f = \mathbb{1}_{\mathcal{O}}$. Then

$$\begin{aligned}\widehat{f}(y) &= \int_{\mathcal{O}} \psi(xy)dx \\ &= \begin{cases} \mathrm{vol}(\mathcal{O}) & \text{if } \psi|_{\mathcal{O}} = 1 \\ 0 & \text{otherwise.}\end{cases}\end{aligned}$$

$$\begin{aligned}\text{The first case holds} &\iff \psi(\mathcal{O}y) = 1 \\ &\iff \mathrm{Tr}_{F/F_0}(\mathcal{O}y) \subset \mathcal{O}_0 \\ &\iff y \in \mathscr{D}^{-1}\end{aligned}$$

Thus $\widehat{f} = (N\mathscr{D})^{-\frac{1}{2}}$. □

Multiplicative characters. I mean characters of $F^\times$, not necessarily unitary characters. Define

$$U := \{x \in F^\times \,:\, |x| = 1\} = \begin{cases} \{\pm 1\} & \text{if } F = \mathbb{R} \\ \mathbb{T} & \text{if } F = \mathbb{C} \\ \mathcal{O}^\times & \text{if } F \text{ is nonarchimedean.}\end{cases}$$

Then

$$|F^\times| = \{|x| \,:\, x \in F^\times\} = \begin{cases} \mathbb{R}^{x}_{>0} & \text{if } F \text{ is archimedean} \\ q^{\mathbb{Z}} & \text{if } F \text{ is nonarchimedean.}\end{cases}$$

I claim there is an exact sequence

$$1 \to U \to F^\times \xrightarrow{|\,|} |F^\times| \to 1$$

that is split (look at the second nontrivial map). Thus $F^\times \cong U \times |F^\times|$. Let $X(F^\times)$ be the group of characters of $F^\times$. Then $X(F^\times) = X(U) \times X(|F^\times|)$.

Definition 4.3. Say that $x \in X(F^\times)$ is *unramified* if $x|_U = 1$. (I.e. it is a pullback of a character of $|F^\times|$.)

Why unramified? In the nonarchimedean case, CFT says that there is a homomorphism $F^\times \to \mathrm{Gal}(F^{ab}/F)$ that is almost an isomorphism. More precisely, $U = \mathcal{O}^\times \to I$ is an isomorphism.

Definition 4.4. Suppose F is nonarchimedean, and $\chi \in X(F^\times)$. I have some neighborhoods $1+\mathfrak{p}^n$ of 1 (all contained in $\mathcal{O}^\times$, which I will think of as "$1+\mathfrak{p}^0$"). Then $\chi|_{1+\mathfrak{p}^m} = 1$ for some $m \in \mathbb{Z}_{\geq 0}$. Choose the smallest such m. Then define *conductor*$(\chi) = \mathfrak{p}^m$.

Proposition 4.5. *The unramified characters of $F^\times$ are $|\ \ |^s$ for $s \in \mathbb{C}$.*

Proof. Unramified characters correspond to characters of $|F^\times|$. If F is nonarchimedean, $|F^\times| \cong \mathbb{Z}$. It's pretty easy to figure out what the characters of $\mathbb{Z}$ are...

If F is archimedean, $|F^\times| \cong \mathbb{R}^\times_{>0} \cong \mathbb{R}$. What are the characters (not necessarily unitary) of $\mathbb{R}$? I.e. we're looking for additive-to-multiplicative homomorphisms $\chi : \mathbb{R} \to \mathbb{C}^\times$. But $\mathbb{R}_{>0}$ is simply connected, so every character factors through the universal cover $\mathbb{C}$ of $\mathbb{C}^\times$ (where the covering map $\mathbb{C} \to \mathbb{C}^\times$ is the exponential). So no we're looking for continuous homomorphisms $\mathbb{R} \to \mathbb{C} \cong \mathbb{R}^2$. The continuous homomorphisms $\mathbb{R} \to \mathbb{R}$ are just $x \mapsto ax$ (where does 1 go?). □

You can ask whether the character uniquely determines the value of s. If F is archimedean, then the answer is yes. If F is nonarchimedean, χ determines $|\varpi|^s = q^{-s}$ which only determines $s \pmod{\mathbb{Z} \cdot \frac{2\pi i}{\log q}}$. Note that $\sigma := \mathrm{Re}\, s$ *is* determined by χ; this is called the *exponent* of χ.

Theorem 4.6. *Every character of $F^\times$ is $\eta \cdot |\ \ |^s$ for some $\eta \in \widehat{U}$ and $s \in \mathbb{C}$.*

(All characters of U are unitary because U is compact.) Note that, in the real case, $\widehat{U} = \{1, sgn\}$ and in the complex case, $\widehat{U} = \mathbb{Z}$.

Corollary 4.7. *Every character of $\mathbb{R}^\times$ has the form*

$$\chi_{a,s}(x) = x^{-a}|x|^s$$

for some $a \in \{0, 1\}$ and $s \in \mathbb{C}$.

Every character of $\mathbb{C}^\times$ has the form

$$\chi_{a,b,s}(z) := z^{-a}\overline{z}^{-b}\|z\|^s$$

for some $a, b \in \mathbb{Z}$ with $\min(a,b) = 0$ and $s \in \mathbb{C}$. (the notation $\|z\|$ means it's the square of the usual absolute value)

Local L-factors. Now we will talk about L-factors and zeta integrals, which are functions of a character $\chi \in X(F^\times)$, not a complex number. By evaluating such a function on $\eta \cdot |\ \ |^s$ for a fixed η, you can get a function of a complex number s. Think about the set of all characters – this is a complex manifold. It has different slices (copies of $\mathbb{C}$), one for each value of η.

Recall that (up to some Γ factor) $\zeta(s)$ is related to $\zeta(1-s)$. What operation on characters sends $|\ \ |^s$ to $|\ \ |^{1-s}$?

Definition 4.8. If $\chi \in X(F^\times)$, define the *twisted dual* as $\chi^{-1}|\ \ |$.

As motivation, recall that

$$\zeta(s) = \prod_p (1-p^{-s})^{-1}.$$

We're trying to come up with an analog of $(1-p^{-s})^{-1}$ in terms of characters. If $\chi = |\ \ |^s$ on $\mathbb{Q}_p^\times$, then $p^{-s} = |\varpi|^s$. In general, if F is nonarchimedean and $x \in X(F^\times)$, define

$$L(\chi) = \begin{cases} (1-\chi(\varpi))^{-1} & \text{if } \chi \text{ is unramified} \\ 1 & \text{if } \chi \text{ is ramified.} \end{cases}$$

Define

$$\begin{aligned} L(\chi_{a,s}) &:= \Gamma_{\mathbb{R}}(s) := \pi^{-\frac{s}{2}}\Gamma(\tfrac{s}{2}) \\ L(\chi_{a,b,s}) &:= \Gamma_{\mathbb{C}}(s) := \Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1) \end{aligned}$$

To understand why you want to do this, you have to go into higher-dimensional characters… Just believe me, this is a good idea!

Also write

$$L(s,\chi) := L(\chi|\ \ |^s).$$

For fixed χ, this is a meromorphic function of s with no zeros. (The Gamma function has poles, but no zeros.)

Fix a multiplicative Haar measure $d^\times x$ on $F^\times$. Then

$$d^\times x = c\frac{dx}{|x|} \text{ for some } c \in \mathbb{R}_{>0}$$

i.e. $\int_{F^\times} f(x) d^\times x = \int_F f(x)\frac{c}{|x|}dx$ for all $f \in C_c(F^\times)$ (recall C_c means continuous functions with compact support).

Local zeta integrals. Given $f \in \mathscr{S}$ and $\chi \in X(F^\times)$, define

$$Z(f,\chi) := \int_{F^\times} f(x)\chi(x)d^\times x.$$

Theorem 4.9 (Meromorphic continuation and functional equation of the local zeta integral)**.** *Let $\chi = \eta|\ \ |^s$, where $\eta \in \widehat{F^\times}$, and $s \in \mathbb{C}$.*

(a) For $f \in \mathscr{S}$, $Z(f,\chi)$ converges for $\operatorname{Re} s > 0$.
(b) For $f \in \mathscr{S}$, $Z(f,\chi)$ (thought of as a function of s) extends to a meromorphic function on $\mathbb{C}$.
(c) The function $L(\chi)$ is the "gcd" of the $Z(f,\chi)$ as f varies. $\dfrac{Z(f,\chi)}{L(\chi)}$ is an entire function of s, and for each $s \in \mathbb{C}$, there exists $f \in \mathscr{S}$ such that $\dfrac{Z(f,\chi)}{L(\chi)}$ is nonvanishing at s.

(d) There exists an "ε-factor" $\varepsilon(\chi, \psi, dx)$ such that

$$\frac{Z(\widehat{f}, \chi^\vee)}{L(\chi^\vee)} = \varepsilon(\chi, \psi, dx)\frac{Z(f, \chi)}{L(\chi)} \text{ for all } f \in \mathscr{S}.$$

(Here $\chi^\vee$ is the twisted dual.) The point is that ε should be an "easy function" (e.g. 1). The surprising thing is that there's a single functional equation for all f. (remember that the Fourier transform depends on a choice of ψ and dx)

Recall that the first pole of Γ is at zero, and also $(1 - p^{-s})$ has problems when $s = 0$. So it makes sense that $s = 0$ is the cutoff.

Proposition 4.10 (Proof of convergence for $s > 0$)**.** *We'll prove absolute convergence.*

Lecture 5: February 24

We had $Z(f, \chi) := \int_{F^\times} f(x)\chi(x)dx$. Last time we proved that $\chi = \eta|\ \ |^s$ decays fast enough that $Z(f, \chi)$ converges for $\operatorname{Re} s > 0$.

We were trying to prove:

Theorem (Meromorphic continuation and functional equation of the local zeta integral)**.** Let $\chi = \eta|\ \ |^s$, where $\eta \in \widehat{F^\times}$, and $s \in \mathbb{C}$.

(a) For $f \in \mathscr{S}$, $Z(f, \chi)$ converges for $\operatorname{Re} s > 0$.
(b) For $f \in \mathscr{S}$, $Z(f, \chi)$ (thought of as a function of s) extends to a meromorphic function on $\mathbb{C}$.
(c) The function $L(\chi)$ is the "gcd" of the $Z(f, \chi)$ as f varies. $\dfrac{Z(f, \chi)}{L(\chi)}$ is an entire function of s, and for each $s \in \mathbb{C}$, there exists $f \in \mathscr{S}$ such that $\dfrac{Z(f, \chi)}{L(\chi)}$ is nonvanishing at s.
(d) There exists an "ε-factor" $\varepsilon(\chi, \psi, dx)$ such that

$$\frac{Z(\widehat{f}, \chi^\vee)}{L(\chi^\vee)} = \varepsilon(\chi, \psi, dx)\frac{Z(f, \chi)}{L(\chi)} \text{ for all } f \in \mathscr{S}.$$

(Here $\chi^\vee$ is the twisted dual.) The point is that ε should be an "easy function" (e.g. 1). The surprising thing is that there's a single functional equation for all f. (remember that the Fourier transform depends on a choice of ψ and dx)

Proof that $Z(f, \chi)$ and $\frac{Z(f\chi)}{L(\chi)}$ are holomorphic for $\operatorname{Re} s > 0$. For $\operatorname{Re} s > 0$, the derivative of $Z(f, \chi) = f(x)\eta(x)|x|^s d^\times x$ w.r.t. s exists because (due to absolute convergence, etc.) you can just differentiate under the integral sign – it's an exponential function of s. Since $L(\chi)$ has no zeros, $\frac{Z(f\chi)}{L(\chi)}$ is holomorphic too. □

Proof of the functional equation (in the region $0 < s < 1$ where both sides are defined) for one f (for each η).

Lemma 5.1. *For each η (unitary character of $F^\times$) there exists $f \in \mathscr{S}$ such that*

(a) $\frac{Z(f\chi)}{L(\chi)}$ *on* $\operatorname{Re} s > 0$ *is nonvanishing*

(b) $\frac{Z(\widehat{f}\chi^\vee)}{L(\chi^\vee)}$ *on* $\operatorname{Re} s < 1$ *is nonvanishing.*

(c) There exists a nonvanishing holomorphic function $\varepsilon(s) = \varepsilon(\chi, \psi, dx)$ *on all of* $\mathbb{C}$ *such that the functional equation holds on the strip* $0 < \operatorname{Re} s < 1$

Proof of Lemma 5.1. In all of this there is an implicit choice of ψ and dx. But changing this information just changes things by a constant; if you get it to work for one (ψ, dx) pair, you can easily make it work for a different pair by multiplying ε by an easy constant. So it suffices ot prove this for my favorite ψ and dx.

Case 1: $F = \mathbb{R}$, $\psi(x) = e^{-2\pi i x}$, $dx =$ Lebesgue, $d^\times x = \frac{dx}{|x|}$. (Note that changing the choice of $d^\times x$ changes both sides by the same factor.) η is a character of the group $\{\pm\}$; there are two possible ones: the identity character and the sign character. If $\eta = 1$, then choose $f(x) = e^{-\pi x^2}$ (it's a Schwartz function that is equal to its own Fourier transform). Plug everything in, and you get $Z(f, \chi) = L(\chi)$ and $Z(\widehat{f}, \chi^\vee) = L(\chi^\vee)$. So you can just set $\varepsilon = 1$. If η is the sign representation (i.e. $\eta(x) = x^{-1}|x|$). You can't choose $f = e^{-\pi x^2}$, because then the integral becomes zero. Instead, try $f = xe^{-\pi x^2}$. The rest is homework.

Case 2: $F = \mathbb{C}$, $\psi(z) = e^{-2\pi i(z+\overline{z})}$, $dx = 2\cdot$ Lebesgue, $d^\times x = \frac{dx}{\|x\|}$. Another calculation; read the official notes. η looks either like $z^{-a}\|z\|^{a/2}$ or $\overline{z}^{-b}\|z\|^{b/2}$. You can choose your isomorphism of F with $\mathbb{C}$ to guarantee one of these cases; suppose the first. Choose $f(z) = e^a e^{-2\pi z\overline{z}}$. Then $\varepsilon = (-1)^a$.

Case 3: F is nonarchimedean. Choose dx so that $\int_{\mathcal{O}} dx = 1$. Then $\int_{\mathfrak{p}^k} dx = q^{-k}$. Choose the obvious multiplicative measure $d^\times x = \frac{dx}{|x|}$. Then $\int_{\mathcal{O}^\times} d^\times x = 1 - q^{-1}$ and $\int_{1+\mathfrak{p}^k} d^\times x = q^{-k}$.

Proposition 5.2. *Given unitary characters $\omega : \mathcal{O}^\times \to \mathbb{T}$ and $\psi : \mathcal{O} \to \mathbb{T}$, define the Gauss sum*

$$g(\omega, \psi) := \int_{\mathcal{O}^\times} \omega(x)\psi(x) d^\times x.$$

Suppose ω has conductor $\mathfrak{p}^n$ with $n > 0$, and ψ has conductor $\mathfrak{p}^m$ (so $\omega|_{\mathfrak{p}^n} = 1$ and $\psi|_{\mathfrak{p}^m} = 0$, and n and m are the smallest such numbers). Then:

(1) If $m \neq n$, $g(\omega, \psi) = 0$.

(2) If $m = n$, $|g(\omega, \psi)|^2 = q^{-m}$ where $|\ \ |$ denotes the usual absolute value on $\mathbb{C}$.

Proof. (1) If $m > n$, I claim that the integral over each coset of $1 + \mathfrak{p}^n$ is zero. Because $\mathfrak{p}^n$ is the conductor of ω, ω is constant. A multiplicative coset of $1 + \mathfrak{p}^n$ can be thought of as an additive coset of $\mathfrak{p}^n$. But ψ is a nontrivial character on $\mathfrak{p}^n$; integrating a nontrivial character over a compact group is zero. If $m < n$, it's the other way around: ψ is constant, and ω is nontrivial.

(2) If $m = n > 0$ then

$$|g(\omega,\psi)|^2 = \int_{\mathcal{O}^\times} \omega(x)\psi(x)d^\times x\overline{\int_{\mathcal{O}^\times} \omega(y)\psi(y)d^\times y}$$
$$= \int_{\mathcal{O}^\times}\int_{\mathcal{O}^\times} \omega(xy^{-1})\psi(x-y)d^\times x d^\times y$$

Let $x = yz$; this preserves the measure because it's a sheaf transformation.

$$\int_{\mathcal{O}^\times}\int_{\mathcal{O}^\times} \omega(z)\psi(yz-y)d^\times y d^\times z$$
$$= \int_{\mathcal{O}^\times} \omega(z)h(z)d^\times z \text{ where } h(z) = \int_{\mathcal{O}^\times} \psi(yz-y)d^\times y$$
$$h(z) = \int_{\mathcal{O}^\times} \psi(y(z-1))dy$$
$$= \int_{\mathcal{O}^\times} \psi(y(z-1))dy - \int_{\mathfrak{p}} \psi(y(z-1))dy$$

The point of this is that the first part is integrating an (additive) character $y \mapsto \psi(y(z-1))$ over an (additive) subgroup. This depends on whether $\psi(y(z-1))$ is trivial or not, and that depends on z.

$$= \begin{cases} 1-q^{-1} & \text{if } v(z-1) \geq m \\ -q^{-1} & \text{if } v(z-1) = m-1 \\ 0 & \text{if } v(z-1) < m-1. \end{cases}$$

Because m is the conductor, it matters whether $z-1$ lands in $\mathfrak{p}^m$.

$$= 1_{1+\mathfrak{p}^m}(z) - q^{-1}\cdot 1_{1+\mathfrak{p}^{m-1}}(z)$$

Thus

$$|g(\omega,\psi)|^2 = \int_{1+\mathfrak{p}^m} \omega(z)d^\times z - q^{-1}\int_{1+\mathfrak{p}^{m-1}} \omega(z)d^\times z$$
$$= q^{-m} - 0 = q^{-m}.$$

(recall that both conductors are $m = n$, so the second term is an integral of a nontrivial character). □

Back to the proof of Lemma 5.1 in the nonarchimedean case. Assume η is ramified. Choose $\psi : F \to \mathbb{T}$ to be of conductor $\mathfrak{p}^0$. Assume η comes from a character of $\mathcal{O}^\times$ by defining $\eta(\varpi) = 1$. Assume η has conductor $\mathfrak{p}^n$ for $n > 0$ (if $n = 0$ then this would be the unramified case).

Choose $f := 2_{1+\mathfrak{p}^n}$, since that makes $Z(f,\chi) = \int_{1+\mathfrak{p}^n} \eta(x)|x|^s d^\times x$. Note that $x \in 1+\mathfrak{p}^n$ so $|x| = 1$. So this integral is $\int_{1+\mathfrak{p}^n} d^\times x = q^{-n} \neq 0$. So (a) is good. Also $L(\chi) = 1$. Next

$$\widehat{f}(y) = \int_{1+\mathfrak{p}^n} \psi(xy)dx = \int_{\mathfrak{p}^n} \psi((1+z)y)$$
$$= \psi(y)\int_{\mathfrak{p}^n}\int_{\mathfrak{p}^n} \psi(yz)dz.$$

Now we're integrating an additive character $z \mapsto \psi(yz)$ over a compact additive subgroup. The answer is $q^{-n}\psi(y)1_{\mathfrak{p}^{-n}}$. The answer depends on whether it's trivial.

For $\operatorname{Re} s < 1$,

$$\begin{aligned} Z(\widehat{f}, \chi^\vee) &= \int_{F^\times} \widehat{f}(x)\chi^\vee(x)d^\times \\ &= q^{-n}\int_{\mathfrak{p}^{-n}} \psi(x)\eta(x)^{-1}|x|^{1-sld^\times x} \end{aligned}$$

The idea is to break the integral into pieces where $|x|$ is constant.

$$= q^{-n}\sum_{k\geq -n}\int_{\mathfrak{p}^k-\mathfrak{p}^{k+1}} \psi(x)\eta(x)^{-1}(q^{-k})^{1-s}d^\times s$$

Even those these regions look like they're getting smaller (additively), the have the same *multiplicative* volume because they're multiplicative translates of each other.

$$\begin{aligned} &= q^{-n}\sum_{k\geq n} q^{-k(1-s)}\int_{\mathcal{O}^\times} \psi(\varpi^k z)\eta(\varpi^k z)^{-1}d^\times z \\ &= q^{-n}\sum_{k\geq n} q^{-k(1-s)}\int_{\mathcal{O}^\times} \psi(\varpi^k z)\eta(z)^{-1}d^\times z \text{ because } \eta(\varpi)=1 \end{aligned}$$

This is a Gauss sum

$$= q^{-n}\sum_{k\geq n} q^{-k(1-s)}g(\eta^{-1}, \psi_{\varpi^k})$$

Use Proposition 5.2; notice that $z \mapsto \psi(\varpi^k z)$ has conductor $\mathfrak{p}^{-k}$ and $z \mapsto (\eta(z))^{-1}$ has conductor $\mathfrak{p}^n$.

$$= q^{-n}q^{n(1-s)}g(\eta^{-1}, \psi_{\varpi^{-n}}) \neq 0.$$

So $\varepsilon := q^{n(1-s)}g(\eta^{-1}, \psi_{\varpi^{-n}})$. □

Proof of the functional equation. We have still only proved the functional equation for one f. Now we take an arbitrary g, and prove it still works by calculating the ratio of the two functional equation candidates.

Lemma 5.3. *Let $f, g \in \mathscr{S}$. Let $\chi = \eta|\ \ |^s$ for some $\eta \in \widehat{F^\times}$. If $0 < \operatorname{Re} s < 1$ then:*

$$Z(f,\chi)Z(\widehat{g},\chi^\vee) = Z(g,\chi)Z(\widehat{f},\chi^\vee).$$

Proof. I'll write out the LHS and show it's symmetric in f and g.

$$\begin{aligned} Z(f,\chi)Z(\widehat{g}\chi^\vee) &= \int_{F^\times} f(x)\chi(x)d^\times x\int_{F^\times}\left(\int_F g(z)\psi(yz)dz\right)\chi(y)^{-1}|y|d^\times y \\ &\overset{\text{Fubini}}{=} \int_{(F^\times)^3} f(x)g(z)\chi(xy^{-1})\psi(yz)|yz|d^\times xd^\times yd^\times z \\ &\overset{y=xt}{=} \int_{(F^\times)^3} f(x)g(z)\chi(t^{-1})\psi(txz)|tzy|d^\times xd^\times td^\times z \end{aligned}$$

It's symmetric! □

We now know that the functional equation holds in the strip $0 < \operatorname{Re} s < 1$. The RHS is holomorphic for $\operatorname{Re} s > 0$, and the LHS is holomorphic for $\operatorname{Re} s < 1$, and they agree on the overlap. So you can take those two functions, glue them together and get a big holomorphic function. We already checked that ε is a nonvanishing holomorphic function on the entire plane. $L(\chi)$ is meromorphic, so that proves the meromorphic continuation of $Z(f,\chi)$.

Lecture 6: February 26

We're done with local stuff, so now we'll prove the global functional equation, which is defined for adèles and idèles. Recall: we have a global field K, and for each absolute value $|\ \ |_v$ we have local data K_v, $\mathcal{O}_v$, $\mathfrak{p}_v$, k_v; the adèles are $\mathbb{A} = \prod_v'(K_v, \mathcal{O}_v)$ (whose basic opens look like $\prod U_v$, where $U_v = \mathcal{O}_v$ for all but finitely many v). We also have $\mathbb{A}^\times = \prod_v'(K_v^\times, \mathcal{O}_v^\times)$ whose basic opens look like $\prod U_v$ where $U_v = \mathcal{O}_v^\times$ for all but finitely many v.

There is an inclusion $K \subset \mathbb{A}$ that should be thought of as like $\mathbb{Z} \subset \mathbb{R}$: i.e. K is discrete and $\mathbb{A}/K$ is compact.

Proposition 6.1. *There is an isomorphism*

$$\widehat{\mathbb{A}} \to \prod_v{}'(\widehat{K}_v, \widehat{K_v/\mathcal{O}_v})$$

sending $\psi \mapsto (\psi|_{K_v})_v$. (Here $\widehat{\ }$ means Pontryagin dual, so $\widehat{K_v/\mathcal{O}_v}$ is the set of characters vanishing on $\mathcal{O}_v$.) In the other direction, send $(\psi_v) \mapsto \prod \gamma_v$ (the product converges because almost all of the factors are 1).

This says that giving ψ on $\mathbb{A}$ is the same as giving ψ_v on K_v for all v such that $\psi_v|_{\mathcal{O}_v} = 1$ for all almost all v.

Now we choose a standard additive character ψ on $\mathbb{A}$:

- If K is a number field, choose the standard ψ_v on K_v, and take $\psi = \prod \psi_v$.
- Now suppose K is the function field of some (smooth, projective, and geometrically integral) curve $X/\mathbb{F}_q$. Let Ω_X be the sheaf of Kähler differentials, and let Ω_K be the stalk at the generic point of X (which has residue field equal to K, so this is a 1-dimensional K-vector space – the vector space of meromorphic 1-forms). Define $\Omega_v = \Omega_K \otimes K_v = k_v((u))du$ (here u is a uniformizing parameter at v). You get a residue map
$$\mathrm{Res}_v : \Omega_v \to k_v \text{ sending } \sum a_i u^i du \mapsto a_{-1}.$$
A choice of nonzero global meromorphic 1-form $\omega \in \Omega_K$ gives rise to a root of unity
$$\psi_v(x) = \exp\left(\frac{2\pi i}{p} \cdot \mathrm{Tr}_{k_v/\mathbb{F}_p} \mathrm{Res}_v(x\omega)\right) \in \mathbb{C}^\times$$
for valuation v and $x \in K_v$.

  Define $\kappa_v = \mathrm{ord}_v\, \omega$ (the largest integer such that $\omega \in \mathfrak{p}_v^{\kappa_v}\Omega_{X,v}$). Then the conductor of ψ_v is $\mathfrak{p}_v^{-\kappa_v}$. (Why? ω vanishes to order κ_v, so if x vanishes to order $-\kappa_v$, then $x\omega$ will be a holomorphic 1-form, and the residue will be trivial.) Since $\kappa_v = 0$ for almost all v, we can take $\psi = \prod \psi_v$.

  (Technically all of this depends on a choice of ω... but it turns out it's OK.)

From now on, ψ will denote the standard additive character. For $a \in \mathbb{A}$, you can shift ψ by defining $\psi_a(x) = \psi(ax)$.

Corollary 6.2. *There is an isomorphism* $\mathbb{A} \overset{\cong}{\to} \widehat{\mathbb{A}}$ *sending* $a \mapsto \psi_a$.

Proof. Each ψ_v gives rise to an isomorphism $\Psi_v : K_v \to \widehat{K_v}$ (i.e. K_v is self-dual). For almost all v, ψ_v has conductor $\mathfrak{p}_v^0$, so $\mathcal{O}_v^\perp = \mathcal{O}_v$, so Ψ_v identifies $\mathcal{O}_v$ with $\widehat{K_v/\mathcal{O}_v}$. Now look at

$$\prod{}'(K_v, \mathcal{O}_v) \overset{\pi\Psi_v}{\to} \prod_v{}'(\widehat{K}_v, \widehat{K_v/\mathcal{O}_v}).$$

□

Proposition 6.3. $\psi|_K = 1$

Sketch of proof. The number field case of this is homework. The function field case boils down to the fact that, over an algebraically closed field, for any meromorphic 1-form η, $\sum_v \mathrm{Res}_v \eta = 0$. □

By your homework, $\widehat{\mathbb{A}/K} = K^\perp$ (characters of $\mathbb{A}$ that are trivial on K).

Corollary 6.4. $K \to \widehat{\mathbb{A}/K} = K^\perp$ *is an isomorphism.*

Proof.

(1) $K^\perp$ is discrete. (Proof: $\mathbb{A}/K$ is compact.)
(2) $K^\perp$ is a K-subspace of $\widehat{\mathbb{A}} = \mathbb{A}$. (Proof: if $\eta|_K = 1$ then $\eta_a|_K = 1$.)

By (1), $K^\perp/K$ is a discrete subgroup of $\mathbb{A}/K$, which is compact, so it's finite. By (2), $K^\perp/K$ is a K-vector space. K is infinite, so the only way this can happen is for $K^\perp/K = 0$. □

The Tamagawa measure on $\mathbb{A}$. Let dx_v be the self-dual measure on K_v (w.r.t. the Fourier inversion formula using the standard ψ_v).

Definition 6.5. The *Tamagawa measure* $dx = \prod dx_v$ on $\mathbb{A}$ is defined to be the Haar measure such that for each basic open set $\prod_v U_v$,

$$\int_{\prod U_v} dx = \prod \int_{U_v} dx_v.$$

(For almost all v, $U_v = \mathcal{O}_v$, so $\int_{U_v} dx_v$ is 1 in almost all cases. Hence this product makes sense.)

Look at the exact sequence $0 \to K \to \mathbb{A} \to \mathbb{A}/K \to 0$. Take the Tamagawa measure on $\mathbb{A}$; since K is a discrete set, we can put the counting measure on it. Thus there is an induced measure on $\mathbb{A}/K$ (just like you get a measure on $\mathbb{R}/\mathbb{Z}$). $\mathbb{A}$ is a LCA group, K is discrete, and $\mathbb{A}/K$ is compact, so it has finite measure.

Proposition 6.6. $\mathrm{vol}(\mathbb{A}/K) = 1$

I'll give a proof by direct calculation in the number field case. Later, we'll get a calculation-free proof using the Poisson summation formula.

Proof in the number field case. Let K be a number field. Define D to be a fundamental domain for the quotient $\mathbb{A}/K$, i.e. a measurable subset of $\mathbb{A}$ such that $\mathbb{A} = \bigsqcup_{\kappa\in K}(D+\kappa)$. Then $\mathrm{vol}(\mathbb{A}/K) = \mathrm{vol}(D)$.

By strong approximation, the composite map

$$\underbrace{\prod_{v|\infty} K_v}_{K_{\mathbb{R}}} \times \prod_{\text{finite } v} \mathcal{O}_v \subset \mathbb{A} \to \mathbb{A}/K$$

is surjective (you have an element of $\mathbb{A}$ that you're trying to approximate up to a factor of K). The kernel consists of things that are v-adically integral, for all v; i.e. the kernel is the ring of integers $\mathcal{O}_K$.

Let D_∞ be a fundamental domain for $K_{\mathbb{R}}/\mathcal{O}_K$. Then let $D = D_\infty \times \prod_{\text{finite } v} \mathcal{O}_v$; I claim this is a fundamental domain for the whole thing.

We have $\mathrm{vol}(D) = \mathrm{vol}(D_\infty)\prod_{\text{finite } v}\mathrm{vol}(\mathcal{O}_v)$. Last semester we calculated $\mathrm{vol}(D_\infty) = (\mathrm{disc}\,\mathcal{O}_K)^{\frac{1}{2}}$ (some people put a factor of 2^{-s}, but we don't have this here because we chose the "better" measure at the complex places). With respect to the self-dual measure, $\mathrm{vol}(\mathcal{O}_v) = (N\mathscr{D}_v)^{-\frac{1}{2}}$. Putting this all together, $\mathrm{vol}(D) = 1$. □

Adèlic Fourier transform. If $f_v \in \mathscr{S}(K_v)$, and $f_v = 1_{\mathcal{O}_v}$ for almost all v. Then we can define the product $\prod f_v : \mathbb{A} \to \mathbb{C}$ (just multiply all the values together).

Definition 6.7. A *Schwarz-Bruhat function* $f : \mathbb{A} \to \mathbb{C}$ is a finite $\mathbb{C}$-linear combination of these. Write $\mathscr{S} = \mathscr{S}(\mathbb{A})$ for the set of such functions.

These are the functions we're going to be taking Fourier transforms of.

Fix the standard ψ on the adèles, and the Tamagawa (self-dual) measure dx on $\mathbb{A}$. Given $f \in \mathscr{S}$, define

$$\widehat{f}(y) := \int_{\mathbb{A}} f(x)\psi(xy)dy.$$

Then $\widehat{f} \in \mathscr{S}$.

The above is for $\mathbb{A}$ and its Pontryagin dual $\mathbb{A}$. Now do it for K and its Pontryagin dual $\mathbb{A}/K$.

Functions on $\mathbb{A}/K$ are in 1-1 correspondence with K-periodic functions on $\mathbb{A}$. I can't talk about Schwarz-Bruhat functions, though, because periodic functions aren't 1 on almost all v.

Given $f \in \mathcal{L}^1(\mathbb{A}/K)$, define $\widehat{f} : K \to \mathbb{C}$ by

$$\widehat{f}(\kappa) := \int_D f(x)\psi(\kappa x)dx.$$

(Actually, there should be a factor of $\frac{1}{\text{vol}(D)}$, but this will turn out to be 1.) If $f \in \mathcal{L}^1(\mathbb{A}/K)$ and $\widehat{f} \in \mathcal{L}^1(K)$, then

$$f(x) = \sum_{\kappa \in K} \widehat{f}(\kappa)\overline{\psi(\kappa x)}.$$

(Aside: the Pontryagin dual of the counting measure on a discrete group, is the measure that gives measure 1 to the dual, which is compact.)

Poisson summation comes from comparing the two Fourier inversion formulas above.

Lemma 6.8. *If $f \in \mathscr{S}(\mathbb{A})$, then $\sum_{\kappa \in K} f(x+\kappa)$ converges absolutely and uniformly on compact subsets.*

Proof. Without loss of generality, assume that $f = \prod f_v$ (a general one is a linear combination of these). Every compact set in $\mathbb{A}$ is contained in a big box $\prod S_v$, where S_v is compact in K_v and equal to $\mathcal{O}_v$ for almost all v. At each nonarchimedean v, the set

$$\{\kappa_v \in K_v \;:\; f_v(S_v + \kappa_v) \text{ is not identically } 0\}$$

is v-adically bounded, and $|\kappa_v| \le 1$ for almost all v. For $x \in S$,

$$\sum_{\kappa \in K} f(x+\kappa) = \sum_{\kappa \in I} f(x+\kappa)$$

where I is some fractional ideal depending on S; here I is a lattice $\subset K_{\mathbb{R}}$. This converges well, etc. □

Theorem 6.9 (Poisson summation formula)**.** *If $f \in \mathscr{S}(\mathbb{A})$, then*

$$\sum_{\kappa \in K} f(\kappa) = \sum_{\kappa \in K} \widehat{f}(\kappa).$$

Lecture 7: March 3

Recall we had Fourier inversion formulas for $\mathbb{A} \longleftrightarrow \mathbb{A}$

$$\widehat{f}(y) = \int_{\mathbb{A}} f(x)\psi(xy)dx \quad \Longrightarrow \quad f(x) = \int_{\mathbb{A}} \widehat{f}(y)\overline{\psi(xy)}dy$$

(where ψ is the standard character and dx is the self-dual measure) and for $\mathbb{A}/K \longleftrightarrow K$:

$$\widehat{f}(\kappa) = \int_D f(x)\psi(\kappa x)dx \quad \Longrightarrow \quad f(x) = \sum_{\kappa \in K} \widehat{f}(\kappa)\overline{\psi(\kappa x)}$$

(where D is a fundamental domain, $f(x) \in \mathcal{L}(\mathbb{A}/K)$). We showed that if $f \in \mathscr{S}(A)$, then $\sum_{\kappa \in K} f(x+\kappa)$ converges absolutely and uniformly to a function in $\mathcal{L}^1(\mathbb{A}/K)$ (i.e. a K-periodic function).

Theorem 7.1 (Poisson summation formula)**.** *If* $f \in \mathscr{S}(\mathbb{A})$*, then*

$$\sum_{\kappa \in K} f(\kappa) = \sum_{\kappa \in K} \widehat{f}(\kappa).$$

The proof here is exactly the same as the proof of the Poisson summation formula for $\mathbb{Z} \subset \mathbb{R}$.

Proof. Define $F(x) = \sum_{\kappa \in K} f(x+\kappa)$; this is obviously a periodic function, so we can regard it as a function on $\mathbb{A}/K$. Then

$$\begin{aligned} \widehat{F}(\kappa) &= \int_D \sum_{\ell \in K} f(x+\ell)\psi(\kappa x)dx \\ &= \sum_{\ell \in K} \int_D f(x+\ell)\psi(\kappa x)dx \\ &= \sum_{\ell \in K} \int_{D+\ell} f(z)\underbrace{\psi(\kappa(z-\ell))}_{\psi(\kappa z)}dz \end{aligned}$$

(since κ acts trivially on elements of K)

$$\begin{aligned} &= \int_{\mathbb{A}} f(z)\psi(\kappa z)dz \\ &= \widehat{f}(\kappa). \end{aligned}$$

By the second Fourier inversion formula,

$$\underbrace{F(x)}_{\sum_{\kappa \in K} f(x+\kappa)} = \sum_{\kappa \in K} \underbrace{\widehat{F}(\kappa)}_{\widehat{f}(\kappa)} \overline{\psi(\kappa x)}.$$

Now set $x = 0$ to get $\sum_{\kappa \in K} f(\kappa) = \sum_{\kappa \in K} \widehat{f}(\kappa)$. □

There should have been a factor of $\frac{1}{\mathrm{vol}(D)}$ in the second Fourier inversion formula. So we should have gotten $\sum_{\kappa \in K} f(\kappa) = \sum_{\kappa \in K} \widehat{f}(\kappa)$. Applying this formula to $\widehat{f}$ instead of f, we get $\sum \widehat{f}(\kappa) = \frac{1}{\mathrm{vol}(D)} \sum_{\kappa \in K} f(-\kappa) = \sum_{\kappa \in K} f(\kappa)$. So $\left(\frac{1}{\mathrm{vol}(D)}\right)^2 = 1$ so $\mathrm{vol}(D) = 1$.

Riemann-Roch theorem. Let K be the function field of a curve X over $\mathbb{F}_q$. Then places v of K correspond to closed points on X. Then the divisor group is

$$\operatorname{Div} X = \text{free abelian group on the set of closed points.}$$

A typical divisor looks like $D = \sum_v d_v v$ where $d_v \in \mathbb{Z}$ and $d_v = 0$ for almost all v.

Define the *degree* of D to be $\sum_v d_v[k_v : \mathbb{F}_q] \in \mathbb{Z}$. Every $f \in K^\times$ gives rise to a divisor $\sum_v v(f)v$. Similarly, our chosen $\omega \in \Omega_K$ gives rise to a *canonical divisor* $\mathscr{K} = \sum \kappa_v \cdot v$, where κ_v is the order of vanishing of ω at v (this is only canonical up to multiplication by an element of $K^\times$).

Define

$$\mathcal{O}_{\mathbb{A}} := \prod_v \mathcal{O}_v \subset \mathbb{A}.$$

(This is like giving a Taylor expansion of a function at each point.) Given $D = \sum d_v \cdot v$, define

$$\mathcal{O}_{\mathbb{A}}(D) = \prod_v \mathfrak{p}_v^{-d_v} \subset \mathbb{A}.$$

Define

$$L(D) = K \cap \mathcal{O}_{\mathbb{A}}(D).$$

This is the set of rational functions f on X such that $v(f) \geq -d_v$. This is an $\mathbb{F}_q$-vector space. Algebraic geometers want to know about it!

Define $\ell(D) := \dim_{\mathbb{F}_q} L(D)$.

Example 7.2. Claim that $L(0) = \mathbb{F}_q$ (constant functions on the curve), and hence $\ell(0) = 1$.

Why? It's clear that constants satisfy this; the nontrivial part is saying that all holomorphic functions are constant. If $t \in K - \mathbb{F}_q$, then the $\frac{1}{t}$-adic valuation on $\mathbb{F}_q(t)$ extends to a place v of K for which $v(t) < 0$, so $t \notin L(0)$.

Define the *genus* of X to be $g := \ell(\mathscr{K}) \in \mathbb{Z}_{\geq 0}$.

Theorem 7.3 (Riemann-Roch)**.** *For any divisor D on X, then*

$$\ell(D) - \ell(\mathscr{K} - D) = \deg D + 1 - g.$$

Sketch of proof. The characteristic function $1_{\mathfrak{p}_v^{-d_v}}$ is a Schwarz-Bruhat function. Its Fourier transform ends up being $q_v^{d_v - \kappa/2} 1_{\mathfrak{p}_v^{\kappa v + d_v}}$ *(something's wrong!)*. The adèlic Fourier transform of $1_{\mathcal{O}_{\mathbb{A}}(D)}$ is $q_v^{\deg D - \deg \mathscr{K}/2} 1_{\mathcal{O}_{\mathbb{A}}(\mathscr{K} - D)}$. Apply the Poisson summation formula to $1_{\mathcal{O}_{\mathbb{A}}(D)}$:

$$\sum_{\kappa \in L(D)} 1 = q^{\deg D - \deg \mathscr{K}/2} \sum_{x \in L(\mathscr{K} - D)} 1$$

so

$$\ell(D) = \deg D - \frac{1}{2} \deg \mathscr{K}.$$

This gives

$$\ell(D) - \ell(\mathscr{K} - D) = \deg D + 1 - h$$

for some $h \in \mathbb{Z}$ independent of D. Take $h = 0$. □

Norm of an idèle. If $a \in \mathbb{A}^\times$, multiplication by a is an isomorphism $\mathbb{A} \xrightarrow{a} \mathbb{A}$. It's multiplying each local field component by $v(a)$. This induces a map of Haar measures sending dx to some other Haar measure $d(ax)$, and this has to be a multiple of dx. *Define* this multiple to be $|a|$.

If $a = (a_v)_v$ (where $a_v \in \mathcal{O}_v^\times$ for almost all v), then it's pretty easy to show that $|a| = \prod |a_v|_v$.

Theorem 7.4 (Product formula)**.** *If $a \in K^\times$ then $|a| = 1$.*

Tate's sneaky proof. a is an isomorphism $\mathbb{A} \to \mathbb{A}$ and $K \to K$. So it induces an isomorphism $\mathbb{A}/K \to \mathbb{A}/K$. We already know $\mathrm{vol}(\mathbb{A}/K) = 1$, but even if we didn't, this isomorphism shows that $\mathrm{vol}(\mathbb{A}/K) = |a| \,\mathrm{vol}(\mathbb{A}/K)$. □

Tate: "we can do nothing significant with the idèles until we embed the multiplicative group in it."

Idèle class character (a.k.a. Hecke character or Größencharakter). An idèle class character is a character $\chi : \mathbb{A}^\times \to \mathbb{C}^\times$ of the idèle group with the property that $\chi|_{K^\times} = 1$. It is equivalent to giving a character of $\mathbb{A}^\times/K^\times$ (the "idèle class group").

Example 7.5. If $s \in \mathbb{C}$, $|\ \ |^s$ is an idèle class character.

Example 7.6 (Idèle class character associated to a Dirichlet character)**.** If $K = \mathbb{Q}$, let χ be a Dirichlet character: $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ for some $N \geq 1$. The profinite completion of $\mathbb{Z}$ is $\widehat{\mathbb{Z}} := \varprojlim \mathbb{Z}/n\mathbb{Z} \cong \prod_{\text{primes } p} \mathbb{Z}_p$. This has a unit group $\widehat{\mathbb{Z}}^\times = \varprojlim (\mathbb{Z}/n\mathbb{Z})^\times$. There is a surjection onto $(\mathbb{Z}/N\mathbb{Z})^\times$, which we can then map to $\mathbb{C}^\times$ using χ. I claim that $\mathbb{A}^\times = \mathbb{Q}^\times \times \mathbb{R}^\times_{>0} \times \widehat{\mathbb{Z}}^\times$ (this uses the fact that $\mathbb{Q}$ has class number 1), so this surjects onto $\widehat{\mathbb{Z}}^\times$. Putting this all together, we get a map $\mathbb{A}^\times \twoheadrightarrow \widehat{\mathbb{Z}}^\times \twoheadrightarrow (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\chi} \mathbb{C}^\times$.

The advantage of Tate's approach is that it deals gracefully with the case when the class number is *not* 1.

Example 7.7. Given a 1-dimensional Galois representation $\mathrm{Gal}(K^s/K) \xrightarrow{\rho} \mathbb{C}^\times$. This factors through $\mathrm{Gal}(K^{ab}/K)$. Class field theory says that the latter is almost isomorphic to $\mathbb{A}^\times/K^\times$; in particular, there is an Artin homomorphism $\theta : \mathbb{A}^\times/K^\times \to \mathrm{Gal}(K^{ab}/K)$. The idèle class character is

$$\mathbb{A}^\times \twoheadrightarrow \mathbb{A}^\times/K^\times \xrightarrow{\theta} \mathrm{Gal}(K^{ab}/K) \to \mathbb{C}^\times.$$

Given an idèle class character, define its exponent $\sigma \in \mathbb{R}$ by

$$|\chi(a)| = |a|^\sigma.$$

(Warning: the RHS absolute value is the norm of the idèle, but the LHS absolute value is the usual complex absolute value.) For example, if $\chi = |\ \ |^s$ then the associated σ is $\mathrm{Re}\, s$.

You can also define the *twisted dual*:

$$\chi^\vee := \chi^{-1}|\ \ |.$$

You can define the local component of a character

$$\chi_v := \chi|_{K_v^\times}.$$

Giving all the χ_v's is equivalent to giving χ (but you can't take any random collection of χ_v's and expect them to assemble to get a character χ).

There is a split SES

$$1 \to \mathbb{A}_1^\times/K^\times \to \mathbb{A}^\times/K^\times \to |\mathbb{A}^\times| \to 1$$

(Here $\mathbb{A}_1^\times$ means norm 1 idèles.) So every character is a unitary character times something of the form $|\ |^s$.

You can look at the space of all idèle class characters. Given any χ, you can also make another character $\chi|\ |^s$. In this way, there is an action of $\mathbb{C}$. In the number field case, these are all different for different values of s. So you get a bunch of copies of $\mathbb{C}$, i.e. a big Riemann surface which we'll call $\mathcal{X}$, and you can talk about meromorphic functions etc. on it.

We need a multiplicative Haar measure on the idèles.

First attempt: we could try to define $d^\times x_v := \frac{dx_v}{|x_v|_v}$ and take $d^\times x = \prod_v d^\times x_v$. This doesn't work: if $\prod U_v$ is a basic open (so $U_v = \mathcal{O}_v^\times$ almost all the time), then $\text{vol}(\prod U_v) = \prod_v \text{vol}(U_v)$. But we normalized our measure such that $\text{vol}(\mathcal{O}_v, dx_v) = 1$ for almost all v, which means that $\text{vol}(\mathcal{O}_v^\times) = 1 - q_v^{-1}$. So the product $\prod_v \text{vol}(U_v)$ diverges to 0; every open set has measure 0.

Fix this by rescaling so that $\text{vol}(\mathcal{O}_v^\times) = 1$:

$$d^\times v = \begin{cases} \frac{dx_v}{|x_v|_v} & \text{if } v \text{ is archimedean} \\ (1-q^{-1})\frac{dx_v}{|x_v|_v} & \text{if } v \text{ is nonarchimedean.} \end{cases}$$

Then define $d^\times x = \prod_v d^\times x_v$.

Lecture 8: March 5

Last time we introduced the idèle class characters $\chi : \mathbb{A}^\times \to \mathbb{C}^\times$ such that $\chi|_{K^\times} = 1$, and $\mathcal{X}$, the set of all such (this forms a Riemann surface). We defined a multiplicative Haar measure on $\mathbb{A}^\times$ by fixing up the usual multiplicative Haar measure $\frac{dx}{|x_v|_v}$ in the nonarchimedean case so that $\text{vol}\,\mathcal{O}_v^\times = 1$.

We have a SES

$$0 \to \mathbb{A}_1^\times \to \mathbb{A}^\times \to |\mathbb{A}^\times| \to 1$$

(where $\mathbb{A}_1^\times$ means norm-1 elements). We want a measure on $\mathbb{A}_1^\times$, but we can't just restrict the measure on $\mathbb{A}^\times$, because then everything would have measure zero and that wouldn't be a Haar measure (think about restricting the usual measure on $\mathbb{R}^\times$ to $\{\pm 1\}$.)

Recall that $|\mathbb{A}^\times|$ is $\mathbb{R}^\times_{>0}$ if we're working over a number field, and $q^{\mathbb{Z}}$ if we're working over a function field. In the first case, define the measure on $|\mathbb{A}^\times|$ to be $\frac{dt}{t}$, and in the second case, define the measure to be $(\log q)\cdot$ the counting measure. We'll use the convention that $\frac{dt}{t}$ will mean "the measure on $\mathbb{A}^\times$."

Now we can define the measure d^*x on $\mathbb{A}_1^\times$ to make it compatible with the measure on the other things in the SES.

For $t \in |\mathbb{A}^\times|$, define
$$\mathbb{A}_t^\times := \{x \in \mathbb{A}^\times \; : \; |x| = t\};$$
this is a coset of $\mathbb{A}_1^\times$.

Look at the orbit space $\mathbb{A}_t^\times/K^\times$. This inherits the measure d^*x (here $K^\times$ had the counting measure). Define $V := \operatorname{vol}(\mathbb{A}_1^\times/K^\times)$; this is finite because $\mathbb{A}_1^\times/K^\times$ is a compact group.

Global zeta integrals. For $f \in \mathscr{S}(\mathbb{A})$ and $\chi \in \mathcal{X}$, define
$$Z(f, \chi) := \int_{\mathbb{A}^\times} f(x)\chi(x) d^\times x.$$
This is a generalization of the *completed* Riemann zeta function $\xi(s)$.

Given χ, you can define a new character $x \mapsto |\chi(x)|$; this is equal to $| \;\; |^\sigma$ for some $\sigma \in \mathbb{R}$. If $\chi = \eta| \;\; |^s$ where η is unitary and $s \in \mathbb{C}$, then $\sigma = \operatorname{Re} s$.

Theorem 8.1 (Meromorphic continuation and functional equation for global zeta integrals)**.**

(a) $Z(f, \chi)$ converges for χ of exponent $\sigma > 1$
(b) $Z(f, \chi)$ extends to a meromorphic function on the entire Riemann surface $\mathcal{X}$. In fact, it's holomorphic except for
  - *a simple pole at $| \;\; |^0$ with residue $-Vf(0)$,*
  - *a simple pole at $| \;\; |^1$ with residue $V\widehat{f}(0)$.*

(c) $Z(f, \chi) = Z(\widehat{f}, \chi^\vee)$ as meromorphic functions of $\chi \in \mathcal{X}$.

Proof of convergence for $\sigma > 1$. We'll reduce to the case of Dedekind zeta functions. f is a Schwarz-Bruhat function, a linear combination of $\prod f_v$, where $f_v = 1_{\mathcal{O}_v}$ for almost all v. Reduce to the case where $f = \prod f_v$. Now we may replace f and χ by their absolute values, so $\chi = | \;\; |^\sigma$. Now
$$Z(f, \chi) = \prod_v Z(f_v, | \;\; |_v^\sigma).$$
For almost all v, $f_v = 1_{\mathcal{O}_v}$ and $Z(f_v, | \;\; |_v^\sigma) = (1 - q_v^{-\sigma})^{-1}$.

Question: does $\prod_{\substack{\text{nonarch.} \\ v}} (1 - q_v^{-\sigma})^{-1}$ converge? If K is a number field of degree d, then this is $\zeta_K(\sigma)$.
$$\prod_{v | \infty} (1 - q_v^{-\sigma})^{-1} \leq \prod_{\substack{\text{prime} \\ p}} (1 - p^{-\sigma})^{-d} = (\sum_{n \geq 1} n^{-\sigma})^{-d} < \infty.$$
That was the number field case. In the function field case, the idea is to reduce from K to $\mathbb{F}_q(t)$.
$$\prod_{\substack{\text{monic irred.} \\ \text{polyn. Q}}} (1 - (q^{\deg Q})^{-\sigma})^{-1} = \prod_{n \geq 1} (1 - q^{-n\sigma})^{-N_n}$$

where N_n is the number of monic irreducible polynomials in $\mathbb{F}_q[t]$ of degree n. We need a bound for N_n, but we don't need a very good bound: $N_n \leq q^n$. So this is

$$\sum_{n\geq 1} N_n q^{-n\sigma} \leq \sum_{n\geq 1} q^n q^{-n\sigma} < \infty$$

if $\sigma > 1$. □

What does $\mathbb{A}^\times$ look like? Break it up into cosets $\mathbb{A}_t^\times$. Then $K^\times$ is a discrete subgroup of $\mathbb{A}_1^\times$. By Fubini's theorem, we can integrate in whatever order we want, and we're going to first integrate over each coset, and then integrate over the t's.

For $\sigma > 1$, let $Z_t(f, \chi) = \int_{\mathbb{A}_t^\times} f(x)\chi(x)d^*x$. Then $Z(f, \chi) = \int_{|\mathbb{A}^\times|} Z_t(f, \chi)\frac{dt}{t}$. We'll prove that this "slice zeta function" also has a functional equation.

(Recall our strategy in the Riemann zeta function case was to write $\xi(s) = \int_0^\infty \left(\frac{\theta(t)-1}{2}\right) t^{s/2}\frac{dt}{t}$, and then prove that θ had a functional equation.)

Lemma 8.2. *If $\sigma > 1$, then*

$$Z_t(f, \chi) + f(0)\int_{\mathbb{A}_t^\times/K^\times} \chi(x)d^*x = Z_{1/t}(\widehat{f}, \chi^\vee)\widehat{f}(0)\int_{\mathbb{A}_{1/t}^\times/K^\times} \chi^\vee(x)d^*x.$$

Proof. Choose a fundamental domain for the action of $K^\times$ on $\mathbb{A}_t^\times$. We'll do the integral for each piece. But to make it nice, I'll translate all the pieces back to one piece: so the integration variable x just ranges over one fundamental domain, but $f(x)\chi(x)$ gets translated by a for each a.

$$Z_t(f, \chi) = \int_{\mathbb{A}_t^\times/K^\times} \sum_{a\in K^\times} f(ax)\chi(ax)d^*x$$

χ is an idèle class character, so $\chi(a) = 1$ since $a \in K^\times$

$$= \int_{\mathbb{A}_t^\times/K^\times} \Big(\sum_{a\in K^\times} f(ax)\Big)\chi(x)d^*x$$

This looks like the Poisson summation formula, but it should be a sum over K, not $K^\times$. Add in the missing term.

$$Z_t(f, \chi) + f(0)\int_{\mathbb{A}_t^\times/K^\times} \chi(x)d^*\chi = \int_{\mathbb{A}_t^\times/K^\times} \Big(\sum_{a\in K} f(ax)\Big)\chi(x)d^*x$$

By the form of the Poisson summation formula on the homework,

$$= \int_{\mathbb{A}_t^\times/K^\times} \frac{1}{|x|}\sum_{a\in K} \widehat{f}(a/x)\chi(x)d^*$$

$$\overset{x=y^{-1}}{=} \int_{\mathbb{A}_{1/t}^\times/K^\times} |y|\sum_{a\in K} \widehat{f}(ay)\chi(y^{-1})d^*y$$

$$= \int_{\mathbb{A}_{1/t}^\times/K^\times} \sum_{a\in K} \widehat{f}(ay)\chi^\vee(y)d^*y$$

Notice that this looks like the second line above, except with $\chi^\vee$ and $\widehat{f}$ instead of χ and f.

$$= Z_{1/t}(\widehat{f}, \chi^\vee) + \widehat{f}(0) \int_{\mathbb{A}^\times_{1/t}/K^\times} \chi^\vee(y) d^*y.$$

□

Lemma 8.3.

$$\int_{\mathbb{A}_t^\times/K^\times} \chi(x) d^\times x = \begin{cases} Vt^s & \textit{if } \chi \textit{ is trivial on } \mathbb{A}_1^\times/K^\times, \textit{ i.e. } \chi = |\ \ |^s \\ 0 & \textit{otherwise.} \end{cases}$$

Given the SES $0 \to \mathbb{A}_1^\times/K^\times \to \mathbb{A}^\times/K^\times \to |\mathbb{A}^\times| \to 1$, if you have a character on $\mathbb{A}^\times/K^\times$ that comes from the trivial character on $\mathbb{A}_1^\times/K^\times$, then you know it comes from a character of $|\mathbb{A}^\times|$, and you know what those are.

Back to proving the theorem.

Proof of the analytic continuation. Assume K is a number field. (In the official notes, the function field case will be done too.)

$$Z(f, \chi) = \underbrace{\int_0^1 Z_t(f, \chi) \frac{dt}{t}}_{J(f,\chi)} + \underbrace{\int_1^\infty Z_t(f, \chi) \frac{dt}{t}}_{I(f,\chi)}$$

We want to fix this so it converges for $\sigma < 1$. $I(f, \chi)$ converges (to a holomorphic function) everywhere on $\mathcal{X}$ because $|\chi|$ gets smaller as σ becomes smaller, so the convergence just gets better as σ decreases. (Recall that $Z_t(f, \chi) = \int f(x)\chi(x)d^*x$, and the absolute value of $\chi(x)$ is t^σ.) (This is analogous to the $\xi(s)$ computation we did in Lecture 1.)

The problematic thing is $J(f, \chi)$.

$$J(f, \chi) = \int_0^1 Z_t(f, \chi) \frac{dt}{t}$$

Use the functional equation (Lemmas 8.2 and 8.3)

$$= \int_0^1 Z_{1/t}(\widehat{f}, \chi^\vee) \frac{dt}{t} + \underbrace{\int_0^1 \left(V\widehat{f}(0) \left(\tfrac{1}{t}\right)^{1-s} - Vf(0)t^s \right) \frac{dt}{t}}_{\text{if } \chi = |\ \ |^s}$$

$$\overset{u=\frac{1}{t}}{=} \underbrace{\int_1^\infty Z_u(\widehat{f}, \chi^\vee) \frac{du}{u}}_{I(\widehat{f},\chi^\vee)} + V\widehat{f}(0) \int_0^1 t^{s-1} \frac{dt}{t} - Vf(0) \int_0^1 t^s \frac{dt}{t}$$

Now add $I(f, \chi)$ to both sides, and do the two integrals above:

$$Z(f, \chi) = I(f, \chi) + I(\widehat{f}, \chi^\vee) + \frac{V\widehat{f}(0)}{s-1} - \frac{Vf(0)}{s}$$

This RHS defines the meromorphic continuation. The first two terms are holomorphic on all of $\mathcal{X}$, it has simple poles at $s = 0$ and $s = 1$, and you can see the residues. □

Proof of the functional equation. This analytic continuation is visibly symmetric. You have to be careful because $\widehat{\widehat{f}}(x) = f(-x)$, not $f(x)$. Nonetheless, I claim that $I(\widehat{\widehat{f}}, \chi^{\vee\vee}) = I(f, \chi)$. Do a change of variables $x \mapsto -x$ in the integral; now $\chi(x)$ becomes $\chi(-x)$, but that's OK because $\chi(-x) = \chi(x)$ (recall that χ is an idèle class character). The second two terms in the meromorphic continuation are symmetric w.r.t. $s \mapsto 1 - s$. □

Next time: applications of this main theorem to Dedekind zeta functions and Hecke L-functions. Compare this to the product of the local functional equations (these are not the same, and the difference is something in terms of the local L-factors).

References for Galois cohomology:

- Atiyah and Wall's article in Cassels/ Frölich
- Milne's notes on class field theory (there's a big chapter in there about Galois cohomology)
- Serre's book *Galois cohomology*

Lecture 9: March 10

Finishing up Tate's thesis. RECALL: we had a local functional equation

$$\frac{Z(\widehat{f}, \chi^\vee)}{L(\chi^\vee)} = \varepsilon(\chi)\frac{Z(f, \chi)}{L(\chi)}$$

(for fixed ψ and dx) and a global functional equation

$$Z(\widehat{f}, \chi^\vee) = Z(f, \chi).$$

Today, we'll get information about the global situation from the local situation. (You don't get the global thing by just producting together the local things, but they're related.)

Definition 9.1. For any idèle-class character χ, using the standard ψ and the Tamagawa measure, define

$$\varepsilon(\chi) := \prod_v \varepsilon(\chi_v).$$

(What is χ_v? Recall that there's a copy of $K_v^\times$ inside of $\mathbb{A}^\times$; then given $\chi : \mathbb{A}^\times \to \mathbb{C}^\times$, define $\chi_v = \chi|_{K_v^\times}$.) It will turn out that this product always converges. Similarly, define

$$L(\chi) := \prod_v L(\chi_v)$$

when the product converges.

You proved on the homework that this doesn't depend on the choice of ψ. (The choice of dx doesn't really matter either.)

Theorem 9.2.

(1) $\varepsilon(\chi)$ converges to a nonvanishing holomorphic function on $\mathcal{X}$.

(2) *$L(\chi)$ converges for $\sigma > 1$, and extends to a meromorphic function on $\mathscr{X}$, and is holomorphic outside $|\ \ |^0$ and $|\ \ |^1$. (Recall that $|\chi| = |\ \ |^\sigma$ for some $\sigma \in \mathbb{R}$, and that is called the exponent.)*

(3) *$L(\chi) = \varepsilon(\chi)L(\chi^\vee)$.*

Proof. Recall that $\mathscr{X}$ is just a bunch of copies of $\mathbb{C}$, so we can prove this one component at a time: restrict attention to one component $\mathscr{X}_0$ of $\mathscr{X}$. (This means we're fixing one idèle class character χ and looking at the family $\{|\ \ |^s\chi\}$.) By local calculations,

- $\varepsilon(\chi_v)$ is a nonvanishing holomorphic function on $\mathscr{X}_0$ equal to 1 for all but finitely many v. (By something on the homework, these correspond to unramified characters. Recall that $\varepsilon = Ae^{Bs}$ on each $\mathscr{X}_0$. $\chi|_{\prod_{\text{nonarch. } v}\mathcal{O}_v^\times}$ has open kernel, so χ_v is unramified for almost all v. (A character on a profinite group to $\mathbb{C}^\times$ has to factor through a finite group, hence has open kernel.))

We can find $f_v \in \mathscr{S}(K_v)$ with $f_v = 1_{\mathcal{O}_v}$ for almost all v such that:

- $\frac{Z(f_v,\chi_v)}{L(\chi_v)}$ is a nonvanishing holomorphic function on $\mathscr{X}_0$, equal to 1 for almost all v, and
- the local functional equation holds for all v.

Taking the product over v, and setting $f = \prod f_v \in \mathscr{S}(\mathbb{A})$

- $\varepsilon(\chi)$ is a nonvanishing holomorphic function on $\mathscr{X}_0$
- $\prod_v \frac{Z(f_v,\chi_v)}{L(\chi_v)}$ is a nonvanishing holomorphic function on $\mathscr{X}_0$, so the properties of $L(\chi)$ in (2) follow from that of $Z(f,\chi)$.
- $$\frac{Z(\widehat{f},\chi^\vee)}{L(\chi^\vee)} = \varepsilon(\chi)\frac{Z(f,\chi)}{L(\chi)}$$
  Divide by the global functional equation to get
  $$\frac{1}{L(\chi^\vee)} = \varepsilon(\chi)\frac{1}{L(\chi)}.$$

□

To get meromorphic functions of $s \in \mathbb{C}$ fix an idèle-class character χ and define

$$\varepsilon(s,\chi) := \varepsilon(\chi|\ \ |^s)$$
$$L(s,\chi) := L(\chi|\ \ |^s)$$

Then

$$L(s,\chi) = \varepsilon(s,\chi)L(1-s,\chi^{-1})$$

Recall $(\chi|\ \ |^s)^\vee = \chi^{-1}|\ \ |^{1-s}$.

In Example 7.7, we talked about the diagram

$$\begin{tikzcd}
 & & \mathrm{Gal}(K^s/K) \arrow[d] \arrow[rd, "\rho"] & \\
\mathbb{A}^\times \arrow[r] & \mathbb{A}^\times/K^s \arrow[r, "\theta"] & \mathrm{Gal}(K^{ab}/K) \arrow[r, dotted] & \mathrm{Gal}(\mathbb{C}) = \mathbb{C}^\times
\end{tikzcd}$$

θ becomes an isomorphism is you replace Galois groups with Weil groups.

$$\begin{tikzcd}
& & W_K \arrow[d] \arrow[rd] & \\
\mathbb{A}^\times \arrow[r] & \mathbb{A}^\times/K^s \arrow[r, "\theta"] & W_K^{ab} \arrow[r, dotted] & GL_1(\mathbb{C}) = \mathbb{C}^\times
\end{tikzcd}$$

There is a correspondence

$$\{\text{idèle class characters}\} \longleftrightarrow \{\text{1-dim. reps of } W_K\}.$$

You can consider n-dimensional representations of W_K, and try to redo all of this theory. It turns out that you can get all the n-dimensional representations out of 1-dimensional ones (tensoring them together, tensoring with $|\ \ |^s$, induced representations). So n-dimensional L-functions are just products of Hecke L-functions. It's not so hard to show that the n-dimensional L-functions are holomorphic. The hard part is actually showing that it doesn't matter how you decompose your n-dimensional character.

Is there a similar correspondence relating n-dimensional representations of W_K to… something? It relates to $GL_n(\mathbb{A})$ but is tricky to state correctly. This is Langlands!

(Reference? see references in the official notes.)

Now for something completely different.

Group cohomology. Let G be a group, and $\mathbb{Z}G$ be the group ring, i.e. the set of finite formal sums $\sum_{g \in G} a_g g$. If G is a noncommutative group, then this is a noncommutative ring.

Definition 9.3. A *G-module* is a left $\mathbb{Z}G$-module, i.e. an abelian group A equipped with a left G-action $G \times A \to A$ satisfying

- $1 \cdot a = a$
- $g(a+b) = ga + gb$ for all $g, h \in G$
- $(gh)a = g(ha)$ for all $a, b \in A$

Let Mod_G denote the category of all G-modules.

Examples 9.4.

- $\mathbb{Z}$ with the trivial action
- If L/K is a Galois extension of fields, then $\mathrm{Gal}(L/K)$ acts on $L^\times$, or $E(L)$ (where E is any elliptic curve, or even any commutative group scheme over K).
- If $A, B \in \mathrm{Mod}_G$, then $\mathrm{Hom}(A, B)$ (the set of abelian group homomorphisms $A \to B$) has G-action
$$(g\varphi)(a) = g\varphi(g^{-1}a).$$

The way to remember this is to draw the picture

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "g"] & B \arrow[d, "g"] \\ A \arrow[r] & B \end{tikzcd}$$

and define $g\varphi$ to be the morphism on the bottom. (Note that $g : A \to A$ is invertible, since g has an inverse!)

Definition 9.5. If $A \in \mathrm{Mod}_G$, then define A^G to be the subgroup of G-invariants, i.e. the set $\{a \in A \,:\, ga = a \;\forall g \in G\}$.

Example 9.6. $\mathrm{Hom}(A, B)^G = \mathrm{Hom}_G(A, B)$, the group of *$G$-module homomorphisms $A \to B$*.

In general, $\mathrm{Hom}_G(\mathbb{Z}, A) \cong \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A) \cong A^G$ (canonical isomorphisms).

Proposition 9.7. *If $0 \to A \to B \to C \to 0$ is an exact sequence of G-modules, then $0 \to A^G \to B^G \to C^G$ is exact (i.e. the fixed-points functor is left-exact).*

Proof. $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, -)$ is left exact. □

The whole point of cohomology is to deal with the fact that this is not an exact functor.

Definition 9.8. Let $H \subset G$ be a subgroup, and A be an H-module. We want to come up with a G-module. There's a ring homomorphism $\mathbb{Z}H \to \mathbb{Z}G$, so you can talk about $\mathbb{Z}G \otimes_{\mathbb{Z}H} A$, but actually we care more about $\mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, A)$, so we call that one the *(co)induced module* and notate it $\mathrm{Ind}_H^G A$.

Note that, to specify homomorphisms out of $\mathbb{Z}G$, it suffices to specify homomorphisms out of G. So $\mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, A)$ is $\cong$ to the set of functions $\varphi : G \to A$ such that $\varphi(hg) = h\varphi(g)$ for all $h \in H$ and $g \in G$. Give this the G-action

$$(g\varphi)(s) = \varphi(sg)$$

for all $g, s \in G$.

As a special case, if $H = \{1\}$ then write

$$A^* := \mathrm{Ind}^G A := \mathrm{Ind}_{\{1\}}^G A.$$

$\mathrm{Ind}_H^G(-)$ is a functor $\mathrm{Mod}_H \to \mathrm{Mod}_G$, and it turns out to be exact.

I'll tell you five different ways to say what cohomology is. The official one will be definition 2. First, why should cohomology take values in Ab? Because A^G is essentially just an abelian group – there's no interesting G-action left.

Definition 9.9 (Definition #1 of $H^q(G, A)$)**.** $(H^q(G, -))_{q=0,1,2,\dots}$ is the unique sequence of functors $\text{Mod}_G \to \text{Ab}$ equipped with *connecting* (or *coboundary*) homomorphisms

$$\delta = \delta_q : H^q(G, C) \to H^{q+1}(G, A)$$

defined functorially for exact sequences $0 \to A \to B \to C \to 0$ such that

(1) $H^0(G, A) = A^G$

(2) For each $0 \to A \to B \to C \to 0$,

$$\begin{aligned} 0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \\ \xrightarrow{\delta} H^1(G, A) \to H^1(G, B) \to H^1(G, C) \\ \xrightarrow{\delta} H^2(G, A) \to \dots \end{aligned}$$

is exact.

(3) If $A = \text{Ind}^G B$ for some abelian group B, then it's *acyclic*, i.e. $H^q(G, A) = 0$ for $q > 0$.

It's not obvious that something like this exists. But it isn't hard to show that these properties characterize the cohomology groups uniquely: use "dimension-shifting" to construct $H^q(G, A)$. Start with a G-module A, forget the G-action, and induce back up; call this A^*. There is a natural injection $A \hookrightarrow A^*$ sending $a \mapsto (g \mapsto ga)$. Let B be the quotient, so we have a SES

$$0 \to A \to A^* \to B \to 0$$

where A^* is an induced thing. So the long exact sequence breaks up into a bunch of 2-term exact sequences, i.e. isomorphisms $H^{q+1}(A) \cong H^q(B)$ for $q \geq 1$, and $H^1(A) \cong \text{coker}((A^*)^G \to B^G)$.

Definition 9.10 (Definition #2 (official definition) of $H^q(G, A)$)**.** Define $(H^q(G, -))_{q \geq 0}$ are the *right derived functors* of the left exact functor $A \mapsto A^G$.

What does this mean? First a definition.

Definition 9.11 (Injective modules)**.** Let R be a ring and I be a R-module. Say that I is *injective* if, given a diagram of solid arrows

$$\begin{tikzcd} & I \\ M \arrow[r, hook] \arrow[ur] & N \arrow[u, dotted] \end{tikzcd}$$

a dotted lift exists. (I.e. homomorphisms to I can be extended.) Other equivalent definitions:

- Every $I \hookrightarrow M$ has a splitting $M \to I$.
- Every short exact sequence $0 \to I \to M \to N \to 0$ splits (so $M = I \oplus N$).
- $\text{Hom}(-, I)$ is exact (this ends up implying that there's no higher cohomology, i.e. $H^q(G, I) = 0$ for all $q \geq 0$).

In order to define right derived functors out of a category, you need there to be enough injectives – i.e. that every object A injects into an injective object.

Proposition 9.12. Mod_G *has enough injectives.*

Given a left exact functor F from one abelian category to another such that the first category has enough injectives, Grothendieck came up with a procedure for forming the right derived functors of F.

To compute $H^q(G, A)$ first choose an injective resolution of A, i.e. an exact sequence

$$0 \to A \to I^0 \to I^2 \to \dots$$

where I^i are injective modules for $\mathbb{Z}G$. (Note: the resolution is $I^0 \to I^1 \to \dots$, not $A \to I^0 \to \dots$.) (Saying that a category has "enough injectives" means that there's always an injection $A \hookrightarrow I^0$ where I^0 is injective.) Now take G-invariants of the resolution:

$$(I^0)^G \overset{d_0}{\to} (I^1)^G \overset{d_1}{\to} (I^2)^G \overset{d_2}{\to} \dots. \tag{9.1}$$

This is not necessarily exact anymore, but it is a complex: $d_n \circ d_{n+1} = 0$. So even though we might have ker = im, we still have im ⊂ ker. Measure the failure of exactness by defining

$$H^q(G, A) := \frac{\ker d_q}{\operatorname{im} d_{q-1}}.$$

This is the q^{th} cohomology of (9.1).

This is the same as $\mathrm{Ext}_{\mathbb{Z}G}(\mathbb{Z}, A)$.

Lecture 10: March 12

Problem set 5 may be turned in until Friday March 19.

Last time, we talked about how to compute $H^q(G, A)$ as the q^{th} right derived functor of the left exact functor $(-)^G : \mathrm{Mod}_G \to \mathrm{Ab}$: take an injective resolution $0 \to A \to I^0 \to I^1 \to \dots$, take G-invariants of that, and then take the q^{th} cohomology of $0 \to (I^0)^G \overset{d_0}{\to} (I^1)^G \overset{d_1}{\to} (I^2)^G \overset{d_2}{\to} \dots$.

(Note that the (co)-induced modules J are *acyclic*, which means that $H^q(G, J) = 0$ for all $q \geq 1$. Also note that $H^0(G, A) = A^G$.)

Alternatively, because $\mathrm{Hom}_G(\mathbb{Z}, A) \cong A^G$, we have $H^q(G, A) = \mathrm{Ext}^1_{\mathbb{Z}G}(\mathbb{Z}, A)$. You can compute this using a projective resolution of $\mathbb{Z}$. Free modules are projective.

Definition 10.1 (Definition #3 of $H^q(G, A)$)**.** Choose a free (or more generally, projective) resolution of $\mathbb{Z}$ as a G-module:

$$\underbrace{\dots \to P_2 \to P_1 \to P_0}_{\text{projective resolution of } \mathbb{Z}} \to \mathbb{Z} \to 0.$$

Apply $\mathrm{Hom}_G(-, A)$ to get a complex

$$0 \to \mathrm{Hom}_G(P_0, A) \to \mathrm{Hom}_G(P_1, A) \to \dots$$

and define $H^q(G, A)$ to be the q^{th} cohomology of this complex.

Example 10.2 (Example of a projective resolution $P_\bullet$ of $\mathbb{Z}$)**.** Define $P_i = \mathbb{Z}[G^{i+1}]$ with G-action as follows: $s \in G$ acts on basis elements by $s(g_0, \dots, g_i) = (sg_0, \dots, sg_{i+1})$. I should also tell you what the differentials are; it's the usual thing from algebraic topology where you have alternating sums and forget one thing at a time. This is called the *standard complex*.

Definition 10.3 (Definition #4 of $H^q(G, A)$)**.** Define the group of q-cochains $C^q(G, A)$ to be the set of functions $G^q \to A$ (*not* necessarily homomorphisms). (If $q = 0$ then $C^0(G, A) := A$.) These can be made into a complex

$$0 \to C^0(G, A) \overset{d}{\to} C^1(G, A) \overset{d}{\to} C^2(G, A) \to \dots$$

If you know what the differentials in the standard complex are, you can figure out exactly what the differentials are here. For example:

- If $a \in C^0(G, A)$ then $da \in C^1(G, A)$ is the map $g \mapsto ga - a$.
- If $\xi \in C^1(G, A)$, then $(d\xi) : (g, h) \mapsto g\xi_h - \xi_{gh} + \xi_g$.

Let $Z^q(G, A) = \ker d_q$ ("q-cocycles") and $B^q(G, A) = \operatorname{im} d_{q-1}$ ("q-coboundaries"). Then define

$$H^q(G, A) := Z^q(G, A) \Big/ B^q(G, A).$$

So now you have a concrete way of doing calculations in low degrees.

Important example 10.4. Suppose G acts trivially on an abelian group A. Then for $\xi \in C^2(G, A)$,

$$\begin{aligned} \xi \in Z^1(G, A) &\iff g\xi_h = \xi_{gh} + \xi_g &&\iff \xi \text{ is a homomorphism } G \to A \\ \xi \in B^1(G, A) &\iff \xi = (g \mapsto ga - a = 0) &&\iff \xi = 0 \end{aligned}$$

So $H^1(G, A) = \operatorname{Hom}(G, A)$.

Definition 10.5 (Definition #5 of $H^q(G, A)$)**.** You can relate all of this to the singular cohomology of a big topological space BG. (Read Gelfand-Manin, *Methods of homological algebra*.)

Lemma 10.6 (Shapiro's lemma)**.** *Let $H \subset G$ be a subgroup, and $A \in \mathrm{Mod}_H$. Then $H^q(G, \mathrm{Ind}_H^G A) \cong H^q(H, A)$ for all $q \geq 0$.*

Proof. If $P_\bullet$ is a resolution of $\mathbb{Z}$ by free $\mathbb{Z}G$-modules, then it's a resolution of $\mathbb{Z}$ by free $\mathbb{Z}H$-modules. (G is a union of cosets of H, and think of $\mathbb{Z}G$ is a direct sum of copies of $\mathbb{Z}H$, so $\mathbb{Z}G$ is a free $\mathbb{Z}H$-module.) So we need to show that

$$\mathrm{Hom}_G(P_i, \mathrm{Ind}_H^G A) \to \mathrm{Hom}_H(P_i, A)$$

is an isomorphism; you can just check using the definitions. □

If $H = \{1\}$, then $H^0(H, A) = A$, and $H^q(H, A) = 0$ for $q > 0$. (You want a projective resolution of $\mathbb{Z}$ as a $\mathbb{Z}$-module; just take $0 \to \mathbb{Z} \to \mathbb{Z} \to 0$.) So $H^q(G, \mathrm{Ind}^G A) = 0$ for $q > 0$, i.e. $\mathrm{Ind}^G A$ is acyclic. This explains why we used $\mathrm{Ind}^G A$ in the first definition. (It turns out that, to compute $H^q(G,A)$, it suffices to use any acyclic (not necessarily injective) resolution of A.)

Definition 10.7. If $H \subset G$ is a subgroup, any $A \in \mathrm{Mod}_G$ can be considered as an H-module by forgetting. There are *restriction maps* $\mathrm{Res} : H^q(G,A) \to H^q(H,A)$ induced by (using Definition 10.3) restriction of cochains $G^q \to A$ to $H^q \to A$.

Alternatively, apply $H^q(G,-)$ to $A \to \mathrm{Ind}_H^G A$ and then apply Shapiro's lemma on the right.

There's also a map in the other direction, but it only works if $(G:H)$ is finite.

Definition 10.8. If $(G:H) = n < \infty$ then there are *corestriction maps* $\mathrm{Cor} : H^q(H,A) \to H^q(G,A)$ defined by dimension-shifting; this is an inductive procedure, and the base case $A^H = H^0(H,A) \to H^0(G,A) = A^G$ is given by $\mathrm{Cor}(a) \mapsto \sum_{g\in G/H} ga$ (sum over a set of coset representatives).

Proposition 10.9. $\mathrm{Cor} \circ \mathrm{Res} = n$ *(i.e. the multiplication-by-n map) as maps $H^q(G,A) \to H^q(G,A)$.*

Proof. This is obvious for $q = 0$: take a G-invariant element a, forget that it's G-invariant, and take the sum $\sum_{g\in G/H} ga$ (but $ga = a$). Now say the magic words "dimension shifting." (I.e. use the exact sequence $0 \to A \to A^* \to B \to 0$.) □

If $\#G = n < \infty$, then you can take $H = \{1\}$. We know that, for the trivial group, everything is acyclic. So $\mathrm{Cor} \circ \mathrm{Res}$ factors through $H^q(H,A) = 0$. But we just proved that this is the multiplication-by-n map. This shows that

Proposition 10.10. *If $\#G = n$, then $H^q(G,A)$ is killed by n for $q \geq 1$.*

Definition 10.11. If $H \lhd G$ is a normal subgroup, there are *inflation maps* $\mathrm{Inf} : H^q(G/H, A^H) \to H^q(G,A)$. This factors through $H^q(G,A^H)$. You can define this on cochains, etc. (If I gave you all the details of everything, you'd be bored out of your skulls.)

Proposition 10.12 (Inflation-restriction sequence for H^1)**.** *If $H \lhd G$ is normal and $A \in \mathrm{Mod}_G$, then*

$$0 \to H^1(G/H, A^H) \overset{\mathrm{Inf}}{\to} H^q(G,A) \overset{\mathrm{Res}}{\to} H^q(H,A)$$

is exact.

This is just a definition-chase. (See, e.g. Silverman *Arithmetic of Elliptic curves.*) This is just the beginning of the Hochschild-Serre spectral sequence:

$$E_2^{p,q} = H^q(G/H, H^q(H,A)) \implies H^{p+q}(G,A).$$

In general, spectral sequences arise when you have two left-exact functors: you could either take the right derived functors of each, or compose the two left exact functors and take the right derived functors of this composition. These are related by a spectral sequence.

Homology. Let's reverse all the arrows!

The *augmentation ideal* $I_G \subset \mathbb{Z}G$ is the kernel of the map $\mathbb{Z}G \to \mathbb{Z}$ sending $g \mapsto 1$. This is the ideal generated by $\{g-1 : g \in G\}$. Instead of taking G-invariants, take G-*coinvariants*: just as A^G is the largest G-invariant subgroup, A_G is the largest quotient on which G acts trivially.

Definition 10.13. For $A \in \mathrm{Mod}_G$, define $A_G = A/(ga \sim a) = A/I_G A$.

To define homology, instead of taking right derived functors of Hom, take left derived functors of $\otimes$.

Definition 10.14. Define the q^{th} homology group:

$$H_q(G, A) := H_q(P_\bullet \otimes_{\mathbb{Z}G} A).$$

Facts:

- $H_0(G, A) = A_G$
- If $0 \to A \to B \to C \to 0$ is an exact sequence of G-modules, you get a long exact sequence
$$\cdots \to H_q(G, B) \to H_q(G, C) \xrightarrow{\partial} H_0(G, A) \to H_0(G, B) \to H_0(G, C) \to 0.$$
- If $A = \mathbb{Z}G \otimes B$ ("induced," not "coinduced") for some abelian group B, then $H_q(G, A) = 0$ for all $q \geq 1$.

Next time: if G is finite, you can attach this LES to the cohomology LES and make the biggest LES you've ever seen. We'll also talk about cup products.

Lecture 11: March 17

Problem set 5 deadline extended to Friday, March 20. Problem set 6 is due Monday, March 30.

Recall: for $A \in \mathrm{Mod}_G$, we had the following explicit descriptions of 0-dimensional (co)homology:

$$H^0(G, A) = A^G := \{a \in A : ga = a \; \forall g \in G\}$$

$$H^0(G, A) = A_G := A/I_G A \text{ where } I_G = \ker(\mathbb{Z}G \overset{g \mapsto 1}{\to} \mathbb{Z})$$

(I_G) is the ideal of $\mathbb{Z}G$ generated by $\{s - 1 : s \in G\}$.

Tate cohomology groups. Let G be a finite group. Let $N = \sum_{g \in G} g \in \mathbb{Z}G$. For any G-module A, there is a map $A \xrightarrow{N} A$ (multiplication by N). If $s \in G$, then $N(s-1) = 0$, so $I_G A \subset \ker N$. Since $sN = N$, we also have $\operatorname{im} N \subset A^G$. Therefore, N induces a map

$$H^0(G, A) = A/I_G A \xrightarrow{N^*} A^G = H^0(G, A).$$

Define

$$\widehat{H}_0(G, A) = \ker N^* = \ker(N : A \to A)/I_G A$$

$$\widehat{H}^0(G,A) = \operatorname{coker} N^* = A^G/NA$$

Now I'll write $H(A)$ instead of $H(G,A)$ (etc.) but it means the same thing.

Theorem 11.1. *If $0 \to A \to B \to C$ is a short exact sequence of G-modules, then there's an exact sequence*

$$\begin{aligned}\cdots \to H_1(B) \to H_1(C) \to \widehat{H}_0(A) \to \widehat{H}_0(B) \to \widehat{H}_0(C)\\ \to \widehat{H}^0(A) \to \widehat{H}^0(B) \to \widehat{H}^0(C) \to H^1(A) \to H^1(B) \to \dots\end{aligned}$$

Define $\widehat{H}^n(A) := H^n(A)$, and $\widehat{H}^{-n}(A) := \widehat{H}^{-n+1}(A)$ for $n > 0$. Then the exact sequence above is the LES of $\widehat{H}^\bullet$.

Question: why is this cohomology? Is it derived functors of something?

Answer: well, it smells like cohomology...

Proof. N^* are functorial. Use the "extended snake lemma":

$$\begin{tikzcd}
 & & \ker \arrow[r] & \ker \arrow[r] & \ker \arrow[dddll] & & \\
\dots \arrow[r] & H_1(C) \arrow[r] & H^0(A) \arrow[r] \arrow[d, "N^*"] & H_0(C) \arrow[r] \arrow[d, "N^*"] & 0 & & \\
 & 0 \arrow[r] & H^0(A) \arrow[r] & H^0(B) \arrow[r] & H^0(C) \arrow[r] & H^1(A) \arrow[r] & \dots \\
 & & \operatorname{coker} \arrow[r] & \operatorname{coker} \arrow[r] & \operatorname{coker} \arrow[ur] & &
\end{tikzcd}$$

□

Proposition 11.2. *If $A = \mathbb{Z}G \otimes B$ for some abelian group B, then $\widehat{H}^q(A) = 0$ for all $q \in \mathbb{Z}$.*

Proof. By the HW, induced = coinduced if G is finite (which we're assuming – none of this makes sense when G is infinite). A is coinduced, so $H^q(A) = 0$ for all $q \geq 1$. A is induced, so $H_q(A) = 0$ for all $q \geq 1$. So $\widehat{H}^q(A) = 0$ for all $q \leq -2$. So it suffices to check the ones in the middle.

It remains to check $\widehat{H}^0$ and $\widehat{H}_0$. Elements of A look like $\sum_{g\in G} g \otimes b_g$ for $b_g \in B$. The G-action essentially permutes the b_g's; invariants are the elements where all the b_g's are equal – i.e. things in the image of the norm. So $A^G = NA$ (recall we already had $NA \subset A^G$). So $H^0 = 0$.

Suppose $a = \sum_{g\in G} g \otimes b_g \in \ker(N : A \to A)$; that is,

$$\sum_{h\in G} h \sum_{g\in G} g \otimes b_g = 0 \in A = \mathbb{Z}G \otimes B$$

so $\sum_{g\in G} b_g = 0$ in B. Then $a = \sum_{g\in G}(g-1)(1\otimes b_g) \in I_G A$. Thus $\widehat{H}_0 = 0$. □

This is good news, because now you can do dimension shifting: given A, come up with an injection of A into an induced module B, so the LES above turns into a sequence of isomorphisms. More precisely:

Corollary 11.3. *If $0 \to A \to A^* \to C \to 0$ (where $A^* = \mathrm{Ind}_A^G$) is exact, then $\widehat{H}^q(C) \cong \widehat{H}^{q+1}(A)$ for all $q \in \mathbb{Z}$.*

So if you know something about $\widehat{H}^0$(all modules) then you can prove it for all integers. E.g. you can define the induction and restriction maps and prove Shapiro's lemma for $\widehat{H}^*$.

Alternative construction of $\widehat{H}^q$. Choose a resolution of $\mathbb{Z}$ by finite free $\mathbb{Z}G$-modules

$$\cdots \to P_1 \to P_0 \to \mathbb{Z} \to 0$$

(remember the resolution is $\cdots \to P_1 \to P_0$). As abelian groups, these just look like $\mathbb{Z}^n$. Now take $\mathrm{Hom}(-, \mathbb{Z})$, which preserves dimension of the free modules, but reverses the arrows.

$$0 \to \mathbb{Z} \to P_0^* \to P_1^* \to \dots$$

This is still exact, since P_i is $\mathbb{Z}$-free of finite rank. We can splice these two exact sequences together: "just cut out the $\mathbb{Z}$" and consider the composition $P_0 \to \mathbb{Z} \to P_0^*$:

$$\cdots \to P_1 \to P_0 \to P_0^* \to P_1^*.$$

This is called the *complete resolution*, which we renumber as:

$$P_\bullet : \qquad \cdots \to P_1 \to P_0 \to P_{-1} \to P_{-2} \to \dots$$

(i.e. $P_{-1} := P_0^*$). This is weird; it doesn't look like it's resolving anything. Apply the functor $\mathrm{Hom}_G(P_\bullet, A)$, which gives a complex.

Proposition 11.4. *$\widehat{H}^q(G,A)$ = the q^{th} cohomology of the complex $\mathrm{Hom}_G(P_\bullet, A)$ for all $q \in \mathbb{Z}$.*

Proof. Omitted. (Mess of homological algebra.) □

Finite cyclic groups. We'd assumed through all of this that G is finite. Now let's specialize further to the case where $G \cong \mathbb{Z}/n\mathbb{Z} = \langle s \rangle$.

Come up with a resolution of $\mathbb{Z}$ as follows. Start with $\mathbb{Z}G \to \mathbb{Z} \to 0$. Then the augmentation ideal is principal, generated by $s-1$. So we can continue this to $\mathbb{Z}G \xrightarrow{s-1} \mathbb{Z}G \to \mathbb{Z} \to 0$. The kernel is the image of the norm map, so continue this to $\mathbb{Z}G \xrightarrow{N} \mathbb{Z}G \xrightarrow{s-1} \mathbb{Z}G \to \mathbb{Z} \to 0$. The kernel of N is the place where the coefficients add up to zero, so that's the augmentation ideal again. That is, we get a sequence

$$\dots \xrightarrow{N} \mathbb{Z}G \xrightarrow{s-1} \mathbb{Z}G \xrightarrow{N} \mathbb{Z}G \xrightarrow{s-1} \mathbb{Z}G \to \mathbb{Z} \to 0.$$

Form the complete resolution using this:

$$\cdots \to \underbrace{\mathbb{Z}G}_{P_1} \overset{s-1}{\to} \underbrace{\mathbb{Z}G}_{P_0} \overset{N}{\to} \underbrace{\mathbb{Z}G}_{P_{-1}} \overset{s-1}{\to} \mathbb{Z}G \overset{N}{\to} \mathbb{Z}G \to \ldots.$$

So

$$\widehat{H}^{2q}(A) = \widehat{H}^0(A) = A^G/NA = \ker(s-1)/\operatorname{im}(N)$$
$$\widehat{H}^{2q+1}(A) = \widehat{H}_0(A) = \ker(N : A \to A)/I_G A = \ker(N)/\operatorname{im}(s-1)$$

If $0 \to A \to B \to C \to 0$ is exact, then we get an exact hexagon

$$\begin{tikzcd}
 & \widehat{H}^0(A) \arrow[r] & \widehat{H}^0(B) \arrow[dr] & \\
\widehat{H}^1(C) \arrow[ur] & & & \widehat{H}^0(C) \arrow[dl] \\
 & \widehat{H}^1(B) \arrow[ul] & \widehat{H}^1(A) \arrow[l] &
\end{tikzcd}$$

Cup products. Now we're back to the case of arbitrary G. Let $A, B \in \text{Mod}_G$. Then we get another G-modules $A \otimes_{\mathbb{Z}} B$ with G-action $g(a \otimes b) = ga \otimes gb$. Then there is an obvious G-module homomorphism

$$A^G \otimes B^G \to (A \otimes B)^G.$$

This defines a map on H^0. Using dimension shifting, one obtains homomorphisms

$$H^p(A) \otimes H^q(B) \to H^{p+q}(A \otimes B) \text{ for all } p, q \geq 0$$

which we write $a, b \mapsto a \cdot b$ or $a \cup b$ satisfying *supercommutivity*:

$$b \cdot a = (-1)^{|a||b|} a \cdot b$$

(identifying $B \otimes A$ with $A \otimes B$). You can also do this for $\widehat{H}$ for all $p, q \in \mathbb{Z}$ if G is finite.

If one has a G-equivariant pairing $A \times B \to C$ written $a, b \mapsto a \cdot b$ (i.e. a bilinear map such that $g(a \cdot b) = (ga) \cdot (gb)$ (e.g. the Weil pairing on elliptic curves)), then one has a G-module homomorphism $A \otimes B \to C$ and the cup products can be composed with $H^{p+q}(A \otimes B) \to H^{p+q}(C)$ to give $H^p(A) \otimes H^q(B) \to H^{p+q}(C)$.

Profinite groups. We want to apply this to Galois groups. But if you just do it naïvely, you get the wrong answers, because you're losing the fact that e.g. $\text{Gal}(\overline{Q}/\mathbb{Q})$ is a profinite group that has a topology.

Reminders about profinite groups: suppose $(I, \leq)$ is a nonempty partially ordered set with the property that for all $i_1, i_2 \in I$ there exists i such that $i \geq i_1$ and $i \geq i_2$. Let G_i be a finite group for each $i \in I$, and for every $i \geq j$, there is a homomorphism $\varphi_{ij} : G_i \to G_j$ and these respect composition, etc.. As elements of i get bigger, the G's go the left (like when you define the p-adics). (Or, you could think of a poset as a category where the objects are the elements of the set, and there is a morphism for each $\leq$ relation; then we're talking about a functor $I \to Grp$.)

You can form the inverse limit

$$G := \varprojlim G_i = \{(g_i) \in \prod G_i \,:\, \varphi_{ij}(g_i) = g_j \ \forall i \geq j\}.$$

Give each G_i the discrete topology (so it's compact); $\prod G_i$ has the product topology, hence also compact. We're imposing closed conditions, so G is also compact. There is a basis of neighborhoods around the identity given by $(\pi_i^{-1}(1))_{i \in I}$, where $\pi_i : G \to G_i$ is the i^{th} projection.

Open subgroups of G are just $\pi_i^{-1}(\text{some } G_i)$. (I.e. every open subgroup comes from some finite level.) Open subgroups have finite index (which isn't surprising because G is compact). Closed subgroups are harder to describe.

Example 11.5. If L/K is any Galois extension of fields (not necessarily finite), then $\mathrm{Gal}(L/K) = \varprojlim \mathrm{Gal}(L_i/K)$ where the limit is taken over finite Galois extensions L_i/K contained in L, ordered by inclusion.

Special case: if K is any field, then $\mathrm{Gal}(K^{sep}/K)$ can be described this way.

There is a correspondence

$$\big\{\text{fields } K' \text{ between } K \text{ and } L\big\} \longleftrightarrow \{\text{closed subgroups } H \subset \mathrm{Gal}(L/K)\}$$

$$K' \mapsto \mathrm{Gal}(L/K')$$

$$L^H \leftarrow\!\shortmid H$$

Example 11.6. Let G be any group. Define $\widehat{G} = \varprojlim_H G/H$ where the limit is taken over all normal subgroups H of finite index. Then the ordering is by reverse inclusion. As a special case, we've already seen $\widehat{\mathbb{Z}}$ (profinite completion of $\mathbb{Z}$).

Alternatively, you can take the *pro-p completion*, where you do the same thing but only use H of p-power index. If you do this to $\mathbb{Z}$, you get $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. By the Chinese Remainder Theorem, $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$.

Example 11.7. Any compact Lie group over $\mathbb{Q}_p$ is profinite, e.g. $SL_n(\mathbb{Z}_p)$, $Sp_{2n}(\mathbb{Z}_p)$.

Next time: "supernatural numbers."

Lecture 12: March 19

Recall: last time we were talking about profinite groups: $G = \varprojlim_{i \in I} G_i$ where G_i are finite. WLOG assume $G \twoheadrightarrow G_i$ (if not you can replace G_i by the image of the i^{th} projection, and get the same inverse limit). $U_i = \ker(G \to G_i)$ is an open subgroup of G.

If you have a profinite group G, but you forgot which inverse system it came from, you can always recover one possible system, namely the open normal subgroups $U \subset G$.

Definition 12.1. A supernatural number is a formal product $\prod_{p \text{ prime}} p^{n_p}$ where $n_p \in \{0, 1, 2, \dots\} \cup \{\infty\}$. (Note that there is no requirement that only finitely many exponents are nonzero!)

You can define multiplication, gcd, lcm, | in the obvious way.

Reference: Serre, *Galois cohomology.*

If G is a profinite group $\varprojlim G_i$, then define $\#G = \operatorname{lcm}\#G_i$. If $H \leq G$ is a closed subgroup then define $(G : H) = \operatorname{lcm}_{\substack{U \subset G \\ \text{open, normal}}} (G/U : H/(H \cap U))$.

Proposition 12.2. *If $K \subset H \subset G$ then $(G : K) = (G : H)(H : K)$.*

Definition 12.3. A *pro-p-group* G is an inverse limit of finite p-groups. Equivalently, it's a profinite group G such that $\#G = p^n$ (where n could be ∞, e.g. $\mathbb{Z}_p$).

Definition 12.4. Let $H \leq G$ be a closed subgroup. H is a *Sylow p-subgroup* if H is a pro-p group and $p \nmid (G : H)$.

(In the finite case, you can define Sylow subgroups as a subgroup whose order has the maximal power of p, but that doesn't work if the exponent is ∞.)

Proposition 12.5. *Every profinite group G has a Sylow p-subgroup.*

Also you get the usual Sylow theorems that they're all conjugate (but not the one about index. . .)

Proof. Let $P(U)$ be the set of Sylow p-subgroups of G/U. By the usual Sylow theorem, this is not an empty set. If $U \subset V$, then there is a surjection $G/U \to G/V$, which gives an induced map $P(U) \to P(V)$. So $\varprojlim P(U) \neq \emptyset$ (a directed inverse limit of nonempty sets is nonempty). So we can choose a compatible system of Sylow subgroups $H_U \in P(U)$.

Let $H = \varprojlim H_U \subset \varprojlim G/U$; this is obviously a pro-p group since it's an inverse limit of p-groups. At each stage the index is prime to p. So H is a Sylow p-subgroup of G. □

Discrete G-modules. Let G be a profinite group. Let $A \in \mathrm{Mod}_G$.

Definition 12.6. A is a *discrete G-module* if one of the following equivalent conditions holds:

(1) $G \times A \to A$ is continuous, where G has the usual profinite topology (where the U_i's are declared to be open) and A is given the discrete topology.
(2) For all $a \in A$, $\mathrm{Stab}_G(a)$ is an open subgroup
(3) $A = \bigcup_{\substack{U \leq G \\ \text{open normal}}} A^U$

(Note: "normal" in the last point doesn't matter so much. If H has finite index in G, you can find a normal subgroup $\subset H$ that also has finite index: take the intersection of all the conjugates, or take $\ker(G \to \mathrm{Aut}(G/H))$. So the system of finite index normal subgroups is cofinal in the system of finite subgroups, so it gives the same inverse limit.)

Definition 12.7. Let $\mathcal{M}od_G$ denote the category of discrete G-modules.

Cohomology of profinite groups. Let $G = \varprojlim G_i$ be a profinite group, and let $A \in \mathcal{M}od_G$. I'll give a few equivalent definitions of $H^q(G, A)$. The difference from before is that these involve the topology.

Definition 12.8 (Definition #1 of $H^q(G, A)$ for profinite G)**.** Let $C^q(G, A)$ be the set of *continuous* functions $G^q \to A$. These form a complex $0 \to C^0 \overset{d_0}{\to} C^1 \overset{d_1}{\to} C^2 \to \dots$ (same differential as before). As before, define the group of continuous q-cocycles $Z^q(G, A) := \ker d_q$ and the group of continuous q-coboundaries $B^q(G, A) = \operatorname{im} d_{q-1}$. Define $H^q(G, A) = Z^q(G, A)/B^q(G, A)$.

Definition 12.9 (Definition #2 of $H^q(G, A)$ for profinite G)**.** Define

$$H^q(G, A) := \varinjlim_{\substack{U \leq G \\ \text{open normal}}} H^q(G/U, A^U)$$

where for $U \subset V$, the map $H^q(G/V, A^V) \to H^q(G/U, A^U)$ is inflation. (Note that G/U is a finite group, and that you can't define this to be $\varinjlim H^q(G/U, A)$ because G/U doesn't act on A, only on A^U.)

In the previous definition, cocycles have to come from some cocycle on G/U.

In general, if $G = \varprojlim G_i$, $A_i \in \mathrm{Mod}_{G_i}$, and $A = \varinjlim A_i$, then $H^q(G, A) = \varinjlim H^q(G_i, A_i)$.

Definition 12.10 (Definition #3 of $H^q(G, A)$ for profinite G)**.** Show that $\mathcal{M}od_G$ has enough injectives, and define $H^q(G, -)$ as the q^{th} right derived functor of the functor $\mathcal{M}od_G \to \mathrm{Ab}$ sending $A \mapsto A^G$.

You could also forget that G is profinite and compute it the old way; this gives a different answer. Why? The only difference between this derived functor definition and the previous one is that the source categories are different, so the injectives are going to be totally different. "So $H^q(G, A) \neq H^q(G, A)$."

Cohomological dimension. Reference: Serre's *Galois cohomology*

Let G be a profinite group, and p a prime.

Definition 12.11. The *cohomological dimension* is $cd_p(G) :=$ the smallest integer n such that, for all torsion (every element of A has finite order) $A \in \mathcal{M}od_G$ and for all $q > n$, $H^q(G, A)[p^\infty] = 0$ (this means p^∞-torsion). (Equivalently, it has no p-torsion.)

There's no guarantee that this exists: for most groups, you can get arbitrarily high cohomology. If it doesn't exist, define $cd_p := +\infty$.

Recall, using restriction and corestriction, we showed that $H^q(G/U, A^U)$ for $q \geq 1$ is killed by $\#G/U$. So $H^q(G, A) = \varinjlim_U H^q(G/U, A^U)$ is (for $q \geq 1$) a limit of torsion groups, hence torsion itself. There's a structure theorem for torsion abelian groups T: $T \cong \bigoplus_p T[p^\infty]$ where $T[p^n] = \{t \in T \,:\, p^n t = 0\}$ and $T[p^\infty] = \bigcup_{n \geq 1} T[p^n]$.

Definition 12.12. Strict cohomological dimension $scd_p(G)$ is the smallest integer n such that for *all* $A \in \mathcal{M}od_G$, and for al $q > n$, $H^q(G, A)[p^\infty] = 0$.

Definition 12.13. Define $cd(G) := \sup_p cd_p(G)$ and $scd(G) := \sup_p scd_p(G)$ (this is choosing an n that works for all primes simultaneously).

Obviously, $sdc_p \geq cd_p(G)$. But we can say more:

Proposition 12.14. *Either* $scd_p(G) = cd_p(G)$ *or* $cd_p(G) + 1$.

Proof. We need to show that $scd_p \leq cd_p + 1$. Given $A \in \mathcal{M}od_G$, we have SES's $0 \to A[p] \to A \xrightarrow{p} pA \to 0$ and $0 \to pA \to A \to A/pA \to 0$ (where $A[p] \subset A$ is the p-torsion in A) gotten by breaking up the four-term exact sequence $A[p] \to A \xrightarrow{p} A \to A/pA$. If $q > cd_p(G) + 1$, then $H^q(A[p])[p^\infty] = 0$ and $H^{q-1}(A/pA)[p^\infty] = 0$ (by definition of cd_p). Because of the LES associated to the first SES, we have an exact sequence

$$0 \to H^q(A)[p^\infty] \to H^q(pA)[p^\infty] \to H^q(A)[p^\infty],$$

but the second map is also an injection due to the LES associated to the second SES. This composition is just multiplication by p. So $H^q(A)[p^\infty] = 0$. □

Facts 12.15. Let k be a field. Let $G = G_k := \mathrm{Gal}(k^{sep}/k)$.

condition on k	$cd_p(G)$	$scd_p(G)$	comment
$k = k^{sep}$	0	0	
k is finite	1	2	$G = \widehat{\mathbb{Z}}$ (limit of finite groups)
$[k : \mathbb{Q}_\ell] < \infty$	2	2	G is known (but complicated[2])
$\mathbb{R}$, for $p \neq 2$	0	0	$G = \mathbb{Z}/2$
$\mathbb{R}$, for $p = 2$	∞	∞	$G = \mathbb{Z}/2$
$[k : \mathbb{Q}] < \infty$ and $p \neq 2$ or k is totally imaginary	2	2	
$[k : \mathbb{Q}] < \infty$, and *not* the above conditions	∞	∞	
k is a function field of a curve / alg. closed field	1	2	
global function fields	see $[k : \mathbb{Q}] < \infty$	see $[k : \mathbb{Q}] < \infty$	

Lecture 13: March 31

Recall $L(\chi)$ was the "gcd" of $Z(f, \chi)$. But gcd's are only defined up to invertible elements. For $K = \mathbb{R}$ and $\chi = |\ \ |^s$ we defined $L(\chi) := \pi^{-s/2}\Gamma(s/2)$. Is there anything special about this choice? No, according to Deligne (but it makes the ε-factor nice.)

Nonabelian cohomology. Let G be a profinite group.

In the usual notion of G-module, if you forget the G-action, you have an abelian group. We want a more general notion.

Definition 13.1. A *G-group* A is a G-set A with a group structure compatible with the action of G: ${}^g(ab) = ({}^g a)({}^g b)$

Definition 13.2. If A is a G-set,

$$H^0(G, A) := A^G := \{a \in A \ : \ {}^g a = a\}.$$

Definition 13.3. If A is a G-group, then $H^1(G, A) = \{\text{1-cocycles}\}/\sim$, where 1-cocycles are continuous functions $\xi : G \to A$ such that $\xi_{gh} = \xi_g \cdot {}^g\xi_h$ for all $g, h \in G$, and $\xi \sim \eta$ (say these are "cohomologous") if there exists $b \in A$ such that $\xi_g = b^{-1}\eta_g {}^g b$ for all $g \in G$.

(If you want to read about H^2, see the book by Giraud.)

You can't use the usual definition of "differs by a coboundary" because the ξ's don't even form a group. Also, $H^1(G, A)$ is not necessarily a group. But at least it's a pointed set (a set with a distinguished element); the special point is the equivalence class of $\xi : G \to A$ sending $g \mapsto 1$.

Even though these aren't groups, you can still talk about exact sequences.

Definition 13.4. Say that $(S, s) \xrightarrow{f} (T, t) \xrightarrow{g} (Y, u)$ is an *exact sequence of pointed sets* if $f(s) = t$, $g(t) = u$, and $g^{-1}(u) = f(S)$.

We want to define a long exact sequence associated to a short exact sequence, but it's not going to be very long, because H^2 doesn't exist...

If $G = \varprojlim_{\substack{U \text{ open} \\ \text{normal}}} G/U$, then we have

$$H^q(G, A) = \varinjlim_{\substack{U \text{ open} \\ \text{normal}}} H^q(G/U, A^U) \text{ for } q = 0, 1$$

and $H^q(G, -)$ is a functor for $q = 0, 1$.

Let A be a G-subgroup of a G-group B. A might not necessarily be normal, so B/A is a G-set, not a G-group. Then there exists an exact sequence of pointed sets

$$1 \to H^0(G, A) \to H^0(G, B) \to H^0(G, B/A) \to H^1(G, A) \to H^1(G, B).$$

If A is normal, then you can add $H^1(G, B/A)$ to the end of this. But you're stuck, because A might not be abelian. If $A \subset \text{center}(B)$, then you can add on $H^2(G, A)$. If B is nonabelian, now you're really stuck.

Vague general principle 13.5. Let X be an object of algebraic geometry over a field k. Let X_L denote the same object base-changed over a Galois extension L/k. Then you can define an (L/K)*-form (twist) of* X to be an object Y over k such that $Y_L \cong X_L$.

Then there is a correspondence

$$\{(L/K)\text{-twists of } X\} / k\text{-isomorphism} \longleftrightarrow H^1(\text{Gal}(L/k), \text{Aut}(X_L))$$

sending $X_L \xrightarrow{\varphi} Y_L$ to the cohomology class of the function $g \mapsto \varphi^{-1} \cdot {}^g\varphi$. It looks like a coboundary, but it's usually not, since φ isn't an automorphism; however, it is at least a cocycle.

Twists $X_L \xrightarrow{\cong} Y_L$ don't come with a choice of isomorphism φ; it turns out that changing φ changes the function to a cohomologous one. Going backwards is harder; this works if our "objects" satisfy descent (e.g. for quasi-projective varieties).

Example 13.6. Let X be the elliptic curve $y^2 = x^3 + 1$ over $\mathbb{Q}$, and Y be the elliptic curve $7y^2 = x^3 + 1$ over $\mathbb{Q}$. These are not isomorphic, but if $L = \mathbb{Q}(\sqrt{7})$ or $L = \overline{\mathbb{Q}}$, then $X_L \cong Y_L$. So Y is an (L/K)-twist of X.

Proposition 13.7. *Let L/K be a Galois extension of fields, and $G = \text{Gal}(L/k)$. Then*

(a) $H^q(G, L) = 0$ for all $q \geq 1$ (here we're thinking of L as a G-module under addition).
(b) If $[L : k] < \infty$, the $\widehat{H}^q(G, L) = 0$ for all $q \in \mathbb{Z}$.

Proof. (b) The key to this is the normal basis theorem, which says that L/k is generated by one element and its Galois conjugates; in other words, $L \cong KG$ as a KG-module. Recall that $KG = \mathbb{Z}G \otimes_{\mathbb{Z}} K$, i.e. L is an induced module. But the Tate cohomology of an induced module is zero.

(a) $H^q = \widehat{H}^q$ for $q \geq 1$, so if $[L : k]$ is finite, then (a) is done. If $[L : k]$ is infinite, then use the fact that profinite cohomology is the direct limit of finite cohomology, so

$$H^q(G, L) = \varinjlim_{\substack{K \subset L_i \subset L \\ L_i/k \text{ finite Galois}}} H^q(\mathrm{Gal}(L_i/k), L_i),$$

which is the direct limit of zero. □

Theorem 13.8 ("Hilbert's" theorem 90). *If L/K is a Galois extension of fields, then*

$$H^1(\mathrm{Gal}(L/k), L^\times) = 0.$$

(Why is Hilbert in quotes? It was theorem 90 in a book written by Hilbert. Actually, he didn't state it for general cohomology, but gave a more concrete version for cyclic extensions. Noether should get credit for some formulation of this.)

One proof involves explicitly constructing a coboundary. I'll give a more conceptual proof, that also has the advantage that it generalizes nicely.

Recall that a finite étale k-algebra is a finite product L of finite separable field extensions of k. (This is the same as saying that $\operatorname{Spec} L \to \operatorname{Spec} k$ is a finite étale morphism.) Why care? You want to take a field extension L/k and tensor up by k', but then $L \otimes_k k'$ is not necessarily a field; instead, it's an étale k-algebra.

Theorem 13.9 (Grothendieck). *Let $G_k = \mathrm{Gal}(k_s/k)$, where k_s is the separable closure. There exists an equivalence of categories*

$$\left\{ \begin{matrix} \textit{finite } G_k\textit{-sets} \\ \textit{morphisms of } G_k\textit{-sets} \end{matrix} \right\}^{op} \longleftrightarrow \left\{ \begin{matrix} \textit{étale } k\textit{-algebras} \\ k\textit{-homomorphisms} \end{matrix} \right\}$$

sending $S \mapsto \mathrm{Hom}_{G_k\text{-sets}}(S, k_s) = \mathrm{Hom}_{sets}(S, k_s)^{G_k}$. In the other direction, send $L \mapsto \mathrm{Hom}_{k\text{-alg}}(L, k_s)$.

Example 13.10. Suppose that the G_k-set S is transitive (exactly one orbit). Fix $s \in S$, and let $H := \mathrm{Stab}_{G_k}(s)$. Then H is an open subgroup of G_k, and $S \cong G_k/H$ as G_k-sets (where the isomorphism $G_k/H \to S$ takes $g \mapsto gs$). S corresponds to the étale algebra $\mathrm{Hom}_{G_k\text{-sets}}(G_k/H, k_s) = (k_s)^H$ (a finite separable extension of k in k_s). In general, a finite G-set is $S = \bigsqcup S_i$ where S_i is transitive. If the S_i's correspond to L_i's, then S corresponds to the finite étale algebra $\prod L_i$.

If S has trivial G_k-action, then S corresponds to $\prod_{s \in S} k$.

Pet peeve: don't write $k \oplus k$, because the map $k \hookrightarrow k \oplus k$ sending $\alpha \mapsto (\alpha, 0)$ isn't a ring homomorphism; the natural maps are *out* of this object, so it should be called $k \times k$.

Definition 13.11. Let L be an étale k-algebra with a left action of a finite group G. If $\Omega \supset k$ is a field extension, then $L \otimes_k \Omega$ is an étale Ω-algebra with left G-action, and so is $\prod_{g \in G} \Omega = \mathrm{Hom}_{\mathrm{sets}}(G, \Omega)$, where the left G-action comes from the right translation action of G on G.

Call L a *Galois étale k-algebra with Galois group G* if for some field extension $\Omega \supset k$,

$$L \otimes_k \Omega \cong \prod_{g \in G} \Omega$$

as Ω-algebras with G-action.

Note: you have to specify the group in advance; unlike Galois field extensions, the "Galois group" is not determined by the other data.

Example 13.12. Let $L = k \times k \times k \times k$; this has actions of $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (permutation of coordinates). These make L into a Galois étale k-algebra with different Galois groups. Note: $\mathrm{Aut}(L/k) \cong S_4$, so that doesn't help.

You don't have to check all possible field extensions; if any Ω works, then the separable closure of Ω also works.

Lecture 14: April 2

Suppose L/k is a finite Galois extension with Galois group G. Let W be an L-vector space. A G-action on W is *semilinear* if $\sigma(\ell w) = ({}^\sigma \ell)({}^\sigma w)$ for all $\sigma \in G$, $\ell \in L$, and $w \in W$ (and the action respects addition).

Example 14.1. G acts coordinate-wise on L^n. More generally, if V is a k-vector space, $V \otimes_k L$ is an L-vector space with a semilinear G-action.

W^G is a k-vector space.

If you know $V \otimes_k L$ with its G-action, how can you recover V?

Lemma 14.2. *Suppose V is a k-vector space. Then the k-linear map $V \to (V \otimes_k L)^G$ sending $v \mapsto v \otimes 1$ is an isomorphism.*

Proof. If $V = k$, this is just $L^G = k$. Any V is a direct sum of copies of k, and the formation of the map respects direct sums. □

Lemma 14.3. *Let W be an L-vector space with semilinear action. Then the L-linear map $W^G \otimes L \to W$ sending $w \otimes \ell \mapsto \ell w$ is an isomorphism.*

Proof. We will show that the same holds for Galois étale extensions L/k (here L is no longer a field). The point is that now you can do base-change. Apply $-\otimes_k \Omega$ to k, L, W. Rename Ω as L. Thus we reduce to the case $L = \prod_{g\in G} k$ (here W is an L-module with semilinear G-action). Modules over a direct product also break up: if $e_g := (0, \dots, 0, 1, 0, \dots, 0)$ with the 1 in the g^{th} spot, and $W_g = e_g W$, then $W = \prod_{g\in G} W_g$. An element $g \in G$ maps e_g to e_1 and hence provides an isomorphism $W_g \overset{\cong}{\to} W_1$. Then $W^G =$ the diagonal image of $W_1 \to \prod_{g\in G} W_g$ (invariants are tuples where the coordinates are all the same). $W^G \otimes_k L \to W$ is the direct sum of $W^G \otimes_k ke_g \to W_g$, and the latter maps are isomorphisms since both sides are just the g^{th} spot. □

Theorem 14.4. *The functors*

$$\{k\text{-vector spaces}\} \underset{G\text{-invariants}}{\overset{-\otimes_k L}{\longleftrightarrow}} \{L\text{-vector spaces with semilinear } G\text{-action}\}$$

are inverse equivalences of categories.

This is what we just proved (well, you need things to be functorial, but that's clear...). This also generalizes in several ways: e.g. quasiprojective varieties over L equipped with a semilinear G-action are equivalent to quasiprojective varieties over k. This is useful where L is algebraically closed, so it's easier to construct things over L, but you want things over k.

Corollary 14.5. *There is only one n-dimensional L-vector space with semilinear G-action, up to isomorphism (here this is an isomorphism of L-vector spaces that respects the semilinear G-action).*

We've almost proved Hilbert Theorem 90 at this point, using the $n = 1$ case above. We can do better: we can prove the GL_n case.

Theorem 14.6. *Let L/k be a Galois extension of fields with Galois group G. Then*

$$H^1(G, GL_r(L)) = \{0\}.$$

(Hilbert Theorem 90 is the $r = 1$ case of this, also with the assumption that L/k is abelian.)

Notation: sometimes people write $H^1(k, GL_r) := H^1(\text{Gal}(k_s/k), GL_r(k_s)) = \{0\}$. Actually, this is a little more than notation – it's étale cohomology.

Proof. First reduce to the case where G is finite, by doing the usual trick of writing profinite cohomology as the limit of the cohomology of finite groups.

Given a 1-cochain $\xi : G \to GL_r(L)$, let $W_\xi = L^r$ equipped with the G-action $G \times L^r \to L^r$ sending $(\sigma, w) = \xi_\sigma(\sigma w)$ (idea: the difference between any semilinear G-action and the standard one is L-linear).

Exercise (homework): this describes a semilinear G-action (i.e. $(\sigma\tau) * w = \sigma * (\tau * w)$) iff ξ is a 1-cocycle.

Exercise (homework): $W_\xi \cong W_{\xi'} \iff \xi$ and ξ' are cohomologous.

Conclusion: there exists a bijection

$$H^1(G, GL_r(L)) \longleftrightarrow \{r\text{-dimensional } L\text{-vector spaces with semilinear } G\text{-action}\} / \cong .$$

But we said there is only one of these... □

Alternative proof. Another proof: take the cohomology LES associated to $1 \to SL_r(L) \to GL_r(L) \overset{\det}{\to} \mathbb{G}_m(L) \to 1$ (note that $\mathbb{G}_m(L) = L^\times$):

$$GL_r(k) \overset{\det}{\to} k^\times \to H^1(SL_r(L)) \to H^1(GL_r(L)) = \{0\}.$$

□

Aside: $H^1(k, O_n)$ is the group of quadratic forms of rank n over k (up to $\cong$). $H^1(k, PGL_r)$ is the group of twists of $\mathbb{P}^{r-1}$, equivalently twists of $M_r(k)$ (matrix group). (Matrix automorphisms are given by conjugation, but conjugating by scalars doesn't do anything.) The long exact sequence for $1 \to \mathbb{G}_m \to GL_r \to PGL_r \to 1$ goes all the way to H^2 because $\mathbb{G}_m$ is central:

$$\cdots \to \underbrace{H^1(k, GL_r)}_{\{1\}} \to H^1(k, PGL_r) \to H^2(k, \mathbb{G}_m) = H^2(\mathrm{Gal}(k_s/k), k_s^\times).$$

(The last thing is called the Brauer group.) See Serre's book on local fields. For generalizations, see Bjorn's secret notes on k-points: math.mit.edu/~poonen/papers/Qpoints.pdf.

Kümmer theory. Let k be a field, $G = \mathrm{Gal}(k_s/k)$, $n \geq 1$, and $\mathrm{char}\, k \nmid n$. Assume that the group μ_n of n^{th} roots of 1 in k_s is contained in k. Then there is an exact sequence

$$1 \to \mu_n \to k_s^\times \overset{(-)^n}{\to} k_s^\times \to 1$$

(you can find n^{th} roots (i.e. surjectivity) because $x^n - a$ is a separable polynomial). The resulting LES is:

$$1 \to \mu_n \to k^\times \overset{(-)^n}{\to} k^\times \to H^1(G, \mu_n) \to \underbrace{H^1(G, k_s^\times)}_{0}.$$

This says that there's an isomorphism $k^\times/(k^\times)^n \overset{\cong}{\to} H^1(G, \mu_n)$. Use the assumption that $\mu_n \subset k$ to say that G acts trivially here.

Fact 14.7. If A is a G-module, and G acts trivially on A, then $H^1(G, A) = \mathrm{Hom}_{cts}(G, A)$ (just Hom in the finite case). (If A is nonabelian, then this is not quite true.)

So $k^\times/(k^\times)^n \cong \mathrm{Hom}_{cts}(G, \mu_n)$. Explicitly, this sens $a \mapsto (g \mapsto {}^g\sqrt[n]{a}/\sqrt[n]{a})$.

Look at $k_s/L/k$, where $G = \mathrm{Gal}(k_s/k)$ and $\mathbb{Z}/n\mathbb{Z} = \mathrm{Gal}(L/k)$. Giving a surjection $G \to \mathbb{Z}/n\mathbb{Z}$ describes the cyclic extensions.

Aside about class field theory: suppose you have a finite abelian extension L/k. Look at

$$\begin{tikzcd}
& L(\zeta_n) \arrow[dl, dash, "\text{Kummer ext.}"'] \arrow[dr, dash] & \\
k(\zeta_n) \arrow[dr, dash] & & L \arrow[dl, dash] \\
& k &
\end{tikzcd}$$

Issue in class field theory: which Kummer extensions are in L?

Tracing through definitions shows that L/k is a cyclic extension of degree dividing n, so G_L is the kernel of a homomorphism $G_k \to \mathbb{Z}/n\mathbb{Z}$. Then $L = k(\sqrt[n]{a})$ for some $a \in k^\times$.

14.1. Artin-Schreier theory. Let k be a field of characteristic p. There is a SES

$$0 \to \mathbb{F}_p \to k_s \xrightarrow{\mathscr{P}} k_s \to 0$$

where $\mathscr{P} : x \mapsto x^p - x$. The LES is:

$$\cdots \to k/\mathscr{P}(k) \to H^1(k, \mathbb{F}_p) \to H^1(k, k_s)$$

but the last term is zero, as k_s is an induced module. So $k/\mathscr{P}(k) \cong H^1(k, \mathbb{F}_p) = \mathrm{Hom}_{cts}(G, \mathbb{F}_p)$ as before.

Every $\mathbb{Z}/p\mathbb{Z}$-extension of k is of the form $k(\alpha)$, where $\alpha^p - \alpha = b$ for some $b \in k$.

What about $\mathbb{Z}/p^r\mathbb{Z}$? It's not characteristic p, so it doesn't sit inside a characteristic p field; but, it sits inside the Witt ring. Alternatively, you can think of $\mathbb{Z}/p^r\mathbb{Z}$ as a tower of Artin-Schreier extensions. But, you have to be careful how you do this; this is called Artin-Schreier-Witt theory.

14.2. Elliptic curves (or higher-dimensional analogue, abelian varieties). Let k be a global field, and A an abelian variety over k. (This is a smooth projective connected k-variety equipped with a commutative group structure.) The analogue of the n^{th} power map is $A \xrightarrow{n} A$ mapping $a \mapsto \underbrace{a + a + \cdots + a}_{n}$. This is a morphism.

Claim 14.8. *Assume $n \geq 1$ and $\operatorname{char} k \nmid n$. Then $A \xrightarrow{n} A$ is surjective.*

Proof. The derivative at 0 is $T_0 A \xrightarrow{n} T_0 A$, which is an isomorphism. So the image of $A \xrightarrow{n} A$ is g-dimensional. The image is also a projective variety, because it's the image of a projective variety. Hence, the image is $= A$.

Define $A[n]$ as the kernel in

$$0 \to A[n] \to A(k_s) \xrightarrow{n} A(k_s) \to 0$$

($A[n]$ is the group of n-torsion points). You get an injection $A(k)/nA(k) \to H^1(k, A[n])$. Unfortunately, there's no Hilbert Theorem 90 in this case. Mordell-Weil says that $A(k)/nA(k)$

is finitely generated. Prove it's finite by proving that the image is contained in a particular finite subgroup of $H^1(k, A[n])$ called the Selmer group.

Look at Silverman's *Arithmetic of elliptic curves* for the EC case, or Serre's *Lectures on the Mordell-Weil theorem.* □

Lecture 17: April 14

Let K be a field, $G_K = \mathrm{Gal}(K_s/K)$, and L a topological field. Recall that a Galois representation is just a continuous homomorphism $G_K \to GL(V)$ for some finite-dimensional L-vector space V.

Theorem 17.1. *If G_K is finite, it's either trivial or $\mathbb{Z}/2\mathbb{Z}$ (e.g. for $\mathbb{R}$).*

Last time, we saw that if L is discrete or $L = \mathbb{C}$, then $\rho(G_K)$ is finite.

Proposition 17.2. *Any Galois representation $\rho : G_K \to GL_n(\overline{\mathbb{Q}}_p)$ has image contained in $GL_n(L)$ for some finite extension $L/\mathbb{Q}_p$.*

Proof. The set of degree n extensions of $\mathbb{Q}_p$ in $\overline{\mathbb{Q}_p}$ is finite. (Proof: break this up into unramified followed by totally ramified extensions. There are a finite number of unramified extensions because they corresponds to residue field extensions. Totally ramified extensions come from adjoining an Eisenstein polynomial. If you vary the coefficients, the assignment of Eisenstein polynomial ↦ field is locally constant. But the space of these is compact.)

Also, the set of finite extensions of $\mathbb{Q}_p$ in $\overline{\mathbb{Q}_p}$ is countable, say $\{L_1, L_2, \dots\}$. So $\bigcup L_i = \overline{\mathbb{Q}_p}$, and $\bigcup GL_n(L_i) = GL_n(\overline{\mathbb{Q}}_p)$. Apply ρ^{-1} to this to get $\bigcup \rho^{-1} GL_n(L_i) = G_K$. L_i is complete, hence closed in $\overline{\mathbb{Q}_p}$. $GL_n(L_i)$ is closed in $GL_n(\overline{\mathbb{Q}}_p)$, and $H_i := \rho^{-1} GL_n(L_i)$ is closed in G_K. You want one of these to be all of G_K.

Let μ be the Haar measure on G_K with $\mu(G_K) = 1$. Then $\mu(H_i) > 0$ for some H_i. Then this H_i has finite index in G_K: otherwise, you would have infinite cosets all with the same measure of H_i. Let S be a set of coset representatives for H_i. This is finite. This means that $G_K = \langle H_i, S\rangle$. Apply ρ to get $\rho(G_K) = \langle \rho(H), \rho(S)\rangle$. By definition of H_i, we have $\rho(H_i) \subset GL_n(L_i)$, so $\langle \rho(H_i), \rho(S)\rangle \subset GL_n(L)$ for some finite extnsion L of L_i.

Alternatively, if H_i has infinite index, $\overset{\circ}{barH_i} = \emptyset$ (i.e. H_i is nowhere dense). The Baire category theorem says that $\bigcup H_i$ is nowhere dense in G_K, hence $\neq G_K$. □

The point of this is that, when we restrict to finite extensions $L/\mathbb{Q}_p$, we're not losing anything.

Two representations ρ, ρ' are isomorphic if they're conjugate by some element of GL_n:

$$\begin{tikzcd}
 & GL_n(L) \arrow[dd, "\text{conjugation}"] \\
G_K \arrow[ur, "\rho"] \arrow[dr, "\rho'"'] & \\
 & GL_n(L)
\end{tikzcd}$$

Irreducible representations are ones that have no nontrivial subrepresentations.

Given (V, ρ), you might not be able to write it as a direct sum of irreducible things, but the next best thing is that there is a composition series $V = V_r \supset \ldots \supset V_2 \supset V_1 \supset V_0 = \{0\}$ such that each V_i is a subrepresentation and each quotient $W_i := V_i/V_{i-1}$ is irreducible.

Theorem 17.3 (Jordan-Hölder)**.** *Changing the composition series for V gives the same W's (but possibly in a different order).*

Definition 17.4. The *semisimplification* of V is $V^{ss} := \bigoplus_{i=1}^{r} W_i$ (and the corresponding representation is denoted ρ^{ss}).

You don't need this if working over $\mathbb{C}$, because every finite-dimensional representation over $\mathbb{C}$ breaks up as a direct sum. But if we have an arbitrary topological field, you can have more interesting representations.

Example 17.5. If $L = \mathbb{Q}_p$, consider a representation $\lambda : G_K \twoheadrightarrow \mathbb{Z}_p$ (e.g. if K is finite, then this could be $G_K = \widehat{\mathbb{Z}} = \prod_\ell \mathbb{Z}_\ell \twoheadrightarrow \mathbb{Z}_p$). Let $\rho = \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}$. I.e. $\rho : G_k \to GL_2(\mathbb{Q}_p)$ where $g \mapsto \begin{bmatrix} 1 & \lambda(g) \\ 0 & 1 \end{bmatrix}$. If $V = \mathbb{Q}_p \times \mathbb{Q}_p$ then we have a composition series $V \supset V_1 \supset \{0\}$ where $V_1 = \mathbb{Q}_p \times \{0\}$. G acts trivially on V_1 and on V/V_1. Then $\rho^{ss} \cong \mathbb{1} \oplus \mathbb{1} \ncong \rho$.

Idea: the semisimplification "zeroes out the blocks above the diagonal." The trace and the characteristic polynomial are the same as in the original representation. There's a sort of converse to this.

Theorem 17.6 (Brauer-Nesbitt)**.** *Let ρ, ρ' be representations $G_K \to GL_n$. Then $\rho^{ss} \cong (\rho')^{ss}$ if and only iff $\rho(g)$ and $\rho'(g)$ have the same characteristic polynomial for all $g \in G_K$.*

If $\operatorname{char} L = 0$ or if $\operatorname{char} L > n$, then $\rho^{ss} \cong (\rho')^{ss}$ iff $\operatorname{tr} \rho(g) = \operatorname{tr} \rho'(g)$ for all $g \in G_K$.

Proof. Skipped. There's too much representation theory at MIT as it is. □

Proposition 17.7. *Suppose $[L : \mathbb{Q}_\ell] < \infty$. Let $\mathcal{O}$ be the valuation ring, and k the residue field of L. Every $\rho : G_K \to GL_n(L)$ can be conjugated by an element of $GL_n(L)$ to get $\rho : G_K \to GL_n(\mathcal{O})$. Then $\overline{\rho} : G_K \to GL_n(k)$ is defined.*

But the way of conjugating might not be unique, so you might get different $\overline{\rho}$'s.

Proposition 17.8. *If $\rho, \rho' : G_K \to GL_n(L)$ are isomorphic (conjugate by an element of $GL_n(L)$) and take values in $GL_n(\mathcal{O})$, then $\overline{\rho}$, $\overline{\rho'}$ have the same semisimplification.*

Proof. $\rho(g)$, $\rho'(g)$ have the same characteristic polynomial in $\mathcal{O}[x]$ (because they're conjugate) for any g, and therefore $\overline{\rho}(g)$, $\overline{\rho'}(g)$ have the same characteristic polynomial in $k[x]$. So now we can apply Theorem 17.6. □

Tate twists. Let k be a field with $\operatorname{char} k \nmid n$. Let $\mu_n = \{\zeta \in k_s^\times : \zeta^n = 1\}$. Then there's a homomorphism $\varepsilon : G_K \to (\mathbb{Z}/n\mathbb{Z})^\times$ taking $\sigma \mapsto$ the a such that $\sigma(\zeta) = \zeta^a$ for all $\zeta \in \mu_n$.

Define G_K modules

$$\begin{aligned}
\mathbb{Z}/n\mathbb{Z}(1) &:= \mu_n \text{ but with group law written additively} \\
\mathbb{Z}/n\mathbb{Z}(j) &:= \underbrace{\mu_n \otimes \ldots \otimes \mu_n}_{j \text{ copies}} \\
\mathbb{Z}/n\mathbb{Z}(0) &:= \mathbb{Z}/n\mathbb{Z} \text{ with trivial action} \\
\mathbb{Z}/n\mathbb{Z}(-j) &:= \operatorname{Hom}(\mathbb{Z}/n\mathbb{Z}(j), \mathbb{Z}/n\mathbb{Z}) \text{ for } -j \leq -1
\end{aligned}$$

(The (1) means that there's something funny going on with the Galois action.)

Then for any j, $\mathbb{Z}/n\mathbb{Z}(j)$ is still a cyclic group of order n on which $\sigma \in G_K$ acts as multiplication by $\varepsilon(\sigma)^j$.

If $\ell \neq \operatorname{char} k$ is prime, then define

$$\begin{aligned}
\mathbb{Z}_\ell(j) &:= \varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z}(j) \\
\mathbb{Q}_\ell(j) &:= \mathbb{Z}_\ell(j) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell
\end{aligned}$$

Example 17.9. If $k = \mathbb{Q}$, and $\zeta_{\ell^n} := e^{2\pi i/\ell^n} \in \overline{\mathbb{Q}} \subset \mathbb{C}$ then $\zeta = (\zeta_{\ell^n}) \in \mathbb{Z}_\ell(1)$.

Definition 17.10. If $G_K \to GL(V)$ is an n-dimensional Galois representation over $\mathbb{Q}_\ell$, then $V(j) := V \otimes \mathbb{Q}_\ell(j)$ is another one.

Finite fields. Let k be a finite field. It has a unique extension k_n of degree n. Consider the "geometric" Frobenius $\mathrm{Frob} : \overline{k} \to \overline{k}$ sending $x \mapsto x^{1/\#k}$; this is the inverse of the usual ("arithmetic") Frobenius. (Why geometric? This comes from étale cohomology.)

$\mathbb{Z}$ has dense image in $\widehat{\mathbb{Z}}$ because it surjects onto each finite quotient. There are isomorphisms

$$\begin{tikzcd}
\mathrm{Frob}^{\mathbb{Z}} \arrow[d, hook, "\substack{\text{dense}\\ \text{image}}"'] & \mathbb{Z} \arrow[l] \arrow[d, hook] \\
G_K \cong \varprojlim \mathrm{Gal}(k_n/k) \cong \varprojlim \mathbb{Z}/n\mathbb{Z} = & \widehat{Z}
\end{tikzcd}$$

where the top map sends $1 \mapsto \mathrm{Frob}$.

Idea: "G_k is topologically generated by Frobenius" (i.e. $\mathrm{Frob}^{\mathbb{Z}}$ is dense in G_K). Equip $\mathbb{Z}$ with the discrete topology; this is not the subspace topology in $\widehat{\mathbb{Z}}$.

Local fields. Suppose $[L : \mathbb{Q}_p] < \infty$. We have a valuation $v : K \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$, and a uniformizer ϖ. Let k be the residue field. Then we have an absolute value $|\ \ | : K \to \mathbb{R}_{\geq 0}$ with $|\varpi| = \frac{1}{\#k}$.

Recall, the inertia group was the kernel in $1 \to I \to G_K \to \underbrace{G_k}_{\widehat{\mathbb{Z}}} \to 1$. We have

$$\begin{tikzcd}
1 \arrow[r] & I \arrow[r] \arrow[d, equal] & W \arrow[r] \arrow[d, hook, "\substack{\text{dense}\\ \text{image}}"] & \mathrm{Frob}^{\mathbb{Z}} \arrow[r] \arrow[d, hook, "\substack{\text{dense}\\ \text{image}}"] & 1 \\
1 \arrow[r] & I \arrow[r] & G_K \arrow[r] & \underbrace{G_k}_{\widehat{\mathbb{Z}}} \arrow[r] & 1
\end{tikzcd}$$

where W (the Weil group) is the pullback of the right-hand square. Concretely, it's

$$\{\sigma \in G_K \text{ whose image in } G_K \text{ is an integer power of Frob}\}.$$

Think of it as an approximation to the Galois group in the same way that $\mathbb{Z}$ is an approximation to $\widehat{\mathbb{Z}}$.

Give W the topology such that I is open in W, where I has its usual topology. I is one of a $\mathbb{Z}$'s-worth of cosets in W. Note that W is a topological group that is not profinite or compact (all the I-cosets form an open cover that has no finite subcover).

One usually defines abelianization as $W^{ab} := W/[W,W]$. But this is the wrong notion for topological groups: you only want to consider closed subgroups. So we define the abelianization instead as

$$W^{ab} := W/\overline{[W,W]}.$$

You can reformulate local class field theory in terms of Weil groups. You have two exact sequences

$$\begin{tikzcd}
1 \arrow[r] & \mathcal{O}^\times \arrow[r] \arrow[d, "\sim"'] & K^\times \arrow[r, "v"] \arrow[d, "\sim"', "\theta"] & \mathbb{Z} \arrow[r] \arrow[d, "\sim"'] & 0 \\
1 \arrow[r] & I(K^{ab}/K) \arrow[r] & W^{ab} \arrow[r] & \mathrm{Frob}^{\mathbb{Z}} \arrow[r] & 0
\end{tikzcd}$$

where θ is the local Artin homomorphism. On elements, this sends

$$\begin{tikzcd}
\dots & \varpi \arrow[r] \arrow[d] & 1 \arrow[d] \\
\dots & \mathrm{Frob} \arrow[r] & \mathrm{Frob}
\end{tikzcd}$$

Define an absolute value $W \twoheadrightarrow W^{ab} \cong K^\times \xrightarrow{|\ |} \mathbb{R}^\times_{>0}$. According to the diagram, $\sigma \in W$ induces $x \mapsto x^{|\sigma|}$ on the residue field $\overline{k}$.

Lecture 18: April 16

Last time, we were talking about the situation where $[K : \mathbb{Q}_p] < \infty$, there is a valuation $v : K \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ with absolute value $|\ \ | : K \to \mathbb{R}_{\geq 0}$, uniformizer ϖ with $|\varpi| = \frac{1}{\#k}$ where k is the residue field (normalized w.r.t. the Haar measure).

The Galois group G_K of K_s/K acts on $G_k \cong \widehat{\mathbb{Z}}$. Look at the subgroup of G_k generated by Frob, and define W to be the pullback, i.e. the set of $\sigma \in G_K$ whose image in G_k is an integer power of Frobenius.

$$\begin{tikzcd}
1 \arrow[r] & I \arrow[r] \arrow[d, equal] & W \arrow[r] \arrow[d, hook] & \mathrm{Frob}^{\mathbb{Z}} \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & I \arrow[r] & G_K \arrow[r] & \underbrace{G_k}_{\widehat{\mathbb{Z}}} \arrow[r] & 1
\end{tikzcd}$$

I also defined an absolute value on W via $W \twoheadrightarrow W^{ab} \cong K^\times \xrightarrow{|\ |} \mathbb{R}^\times_{>0}$.

If you have a representation $G_K \to GL_n$, you can get a representation $W \hookrightarrow G_K \to GL_n$ of W. Even though the topology on W is kind of different, $W \hookrightarrow G_K$ is a homomorphism (the topology on W is stronger). Since the image of W is dense in G_K, you can recover the original representation $G_K \to GL_n$. So there is an inclusion

$$\underbrace{\left\{\text{continuous homomorphisms } G_K \to \mathbb{C}^\times\right\}}_{\text{finite-image characters of } K^\times} \subset \underbrace{\{\text{continuous homomorphisms } W \to \mathbb{C}\}}_{\text{characters of } K^\times}$$

More inclusions: finite-image characters $\subset$ unitary characters $\subset$ characters of $K^\times$.

Let $P \subset I$ be the Sylow p-subgroup of the inertia group I ("wild inertia"). We have a tower

$$\begin{tikzcd}
G \arrow[d, dash] & K_s \arrow[d, dash, "P"'] \\
I \arrow[d, dash] & K^{tr} = K^{unr}(\varpi^{1/n} \ : \ n \text{ is not divisible by } p) \arrow[d, dash, "I/P"'] \\
P \arrow[d, dash] & K^{unr} = K(\zeta \ : \ n \text{ is not divisible by } p) \arrow[d, dash, "G/I"'] \\
\{1\} & K
\end{tikzcd}$$

Here K^{tr} is the maximal tamely ramified extension. Recall the correspondence between Galois groups and fields is order-reversing, so $G = \mathrm{Gal}(K_s/K)$, $I = \mathrm{Gal}(K_s/K^{unr})$, etc.

$$G/I = \mathrm{Gal}(K^{unr}/K) \cong \mathrm{Gal}(\overline{k}/k) \cong \mathbb{Z}$$

You can choose the last isomorphism so Frob $\leftarrow\!\shortmid$ 1. I/P is called the tame quotient of the inertia group.

$$I/P = \mathrm{Gal}(K^{tr}/K^{unr}) \cong \varprojlim_{(n,p)=1} \mathrm{Gal}(K^{unr}(\varpi^{1/n})/K^{unr}) \cong \prod_{\ell \neq p} \mathbb{Z}_\ell(1)$$

Note that $\mathrm{Gal}(K^{unr}(\varpi^{1/n})/K^{unr}) \cong \mu_n =: \mathbb{Z}/n\mathbb{Z}(1)$ via the map sending $\sigma \mapsto \sigma(\varpi^{1/n})/\varpi^{1/n}$.

There is a surjection $\prod_{\ell \neq p} \mathbb{Z}_\ell(1) \twoheadrightarrow \mathbb{Z}_\ell(1)$. This is the largest pro-ℓ quotient of I. Let t_ℓ denote the surjection $I \twoheadrightarrow I/P \cong \ldots \twoheadrightarrow \mathbb{Z}_\ell(1)$.

There's more than just a sequence of inclusions of groups; the quotients interact with each other.

$$1 \to \underbrace{\mathrm{Gal}(K^{tr}/K^{unr})}_{\prod_{\ell \neq p} \mathbb{Z}_\ell(1)} \to \mathrm{Gal}(K^{tr}/K) \to \underbrace{\mathrm{Gal}(K^{unr}/K)}_{\mathrm{Frob}^{\widehat{\mathbb{Z}}}} \to 1$$

The middle group is a semidirect product, that can be specified by the action of the quotient. There is a conjugation action of the subgroup on itself, but the subgroup is abelian, so that's a stupid action. The conjugation action of the quotient restricts to an action on the subgroup. This equals the action in which Frob acts as multiplication-by-$\frac{1}{q}$.

If $w \in W$ and $\sigma \in I$ then $t_\ell(w\sigma w^{-1}) = |w| t_\ell(\sigma)$. Under the local class field theory map, Frob $\mapsto \varpi$. So $|\mathrm{Frob}| = \frac{1}{\#k}$.

Theorem 18.1 (Grothendieck's ℓ-adic monodromy theorem)**.** *Suppose $L/\mathbb{Q}_\ell$ is a finite extension, and suppose V is a finite-dimensional L-vector space, and suppose ρ is an ℓ-adic representation of W (i.e. a continuous homomorphism $\rho : W \to GL(V)$). Then there exists a nilpotent $N \in (\mathrm{End}\, V)(-1)$ such that*

$$\rho(\sigma) = \exp(t_\ell(\sigma)N)f \tag{18.1}$$

or all σ in some (finite-index) open subgroup of I.

(Note that t_ℓ is twisted by 1, and N is twisted by -1, so $t_\ell(\sigma)N$ is just a scalar times a matrix.)

Thus ρ can be described by giving N, a subgroup, and finitely many values of ρ.

Remark 18.2. If N is unique, then it is W-invariant. (W acts on V, hence it acts on End V by conjugation, and hence it also acts on the twist.)

$$\rho(w)N\rho(w)^{-1} = |w|N$$

for all $w \in W$.

Proof of Theorem 18.1. I is profinite, hence compact, so I stabilizes some full $\mathcal{O}$-lattice $\Lambda \subset V$. Without loss of generality assume I've chosen a basis, so we can write this inclusion as $\mathcal{O}^n \subset L^n$. Look at $\rho|_I : I \to GL_n(\mathcal{O})$.

Let $U_2 = 1 + \ell^2 M_n(\mathcal{O})$. This is an open normal subgroup of $GL_n(\mathcal{O})$. Let $I' = (\rho|_I)^{-1}U_2$. This is open in I; this will be the subgroup in the statement of the theorem.

Replace K by a finite extension K', replace G_K by a subgroup $G_{K'}$, replace $W = W_K$ by its subgroup $W_{K'} = W \cap G_{K'}$, and replace $I = I_K$ by the subgroup $I_{K'} = I \cap G_{K'}$. Since the $(G_{K'})$ form a basis of neighborhoods of 1 in G_K, and the topology on I is induced from that of G_K, we can choose K' so that $I_{K'} \subset I'$. So do all the replacements above, and notice that proving the new statement still suffices to prove the theorem. So ρ now maps I to U_2.

We will now prove (18.1) for all $\sigma \in I$. We have $\rho|_I : I \to U_2$. I claim that U_2 is a pro-ℓ-group; that is because it has a filtration, and the quotients are pro-ℓ. This homomorphism has to kill a big part of I, e.g. all the wild inertia. So $\rho|_I$ has to factor through the maximal pro-ℓ quotient:

$$\begin{tikzcd} I \arrow[rr] \arrow[dr, "t_\ell"'] & & U_2 \\ & \mathbb{Z}_\ell(1) \arrow[ur, dotted, "\varphi"'] & \end{tikzcd}$$

I need a lemma. Let's forget about the twists for now; they only affect the Galois action.

Lemma 18.3. *Every continuous homomorphism $\varphi : \mathbb{Z}_\ell \to U_2$ has the form $\varphi(x) = \exp(xN)$ for some matrix $N \in \ell^2 M_n(\mathcal{O})$.*

Proof. exp is a map $\ell^2 M_2(\mathcal{O}) \to 1 + \ell^2 M_n(\mathcal{O}) =: U_2$; there is a log map going the other way. These are bijections, not homomorphisms: recall that $e^{A+B} = e^A e^B$ only if A and B commute.

If N exists, then $\varphi(1) = \exp N$. So define $N := \log \varphi(1)$. Then for any $x \in \mathbb{Z}$, $\exp(xN) = \exp(N)^x = \varphi(1)^x = \varphi(x)$ (the exponential map does respect multiplication of integers because they commute with each other). This is what we want, but this is just for integers x. By continuity, this also holds for ℓ-adic integers. □

Lemma 18.3 now says that there exists $N \in \ell^2 M_n(\mathcal{O})(-1)$ (the -1 is because of the twist in $\mathbb{Z}_\ell(1)$) such that $\rho(\sigma) = \exp(t_\ell(\sigma)N)$ for all $\sigma \in I$.

The only things we haven't done are uniqueness (left for homework) and nilpotence of N. This will come from the extra structure of how Frobenius acts on things. Recall: if $w \in W$ and $\sigma \in I$, then $t_\ell(w\sigma w^{-1}) = |w| t_\ell(\sigma)$. Use this to express $\rho(w\sigma w^{-1}) = \exp(t_\ell(w\sigma w^{-1})N)$. But since ρ is a representation, $\rho(w\sigma w^{-1}) = \rho(w)\rho(\sigma)\rho(w)^{-1}$, so it's conjugate to $\rho(\sigma) = \exp(t_\ell(\sigma)N)$. All of these matrices are in U_2. Applying log to the above, we get that $t_\ell(w\sigma w^{-1})N = |w| t_\ell(\sigma)N$ is conjugate to $t_\ell(\sigma)N$. Choose $w = \text{Frob}$, and choose σ such that $t_\ell(\sigma) \neq 0$ (this is OK because t_ℓ surjects onto $\mathbb{Z}_\ell(1)$).

So $q^{-1}N$ is conjugate to N. Conjugate matrices have the same eigenvalues. If λ is any eigenvalue of N, $\sigma^{-1}\lambda$ is an eigenvalue of N, and that implies that $q^{-2}\lambda$ is an eigenvalue, etc. Matrices can't have infinitely many eigenvalues, so the only possibility is for $\lambda = 0$. That is, every eigenvalue of N is 0, so N is nilpotent. □

This proof can be found in the appendix to Serre-Tate, 1968.

There's an even more useful version of this theorem. This only describes the representation on an open subgroup. You can divide out by the "infinite part" and get a representation that's the trivial representation on this subgroup. You get a new representation with an open kernel, so it's continuous w.r.t. the discrete topology. The idea is that you can separate the representation into two pieces, one with discrete topology, and one given by an exponential.

Definition 18.4. Let E be any field of characteristic zero (no topology, just a field). A Weil-Deligne representation over E is a pair (r, N) where:

- r is a continuous homomorphism $W \to GL_n(V)$, for some finite-dimensional E-vector space V with the discrete topology (r being continuous means that $\ker r \supset$ some open subgroup of I);
- $N \in \operatorname{End} V$ is such that $r(w)Nr(w)^{-1} = |w|N$ for all $w \in W$.

Such an N must be nilpotent, by the same argument as in the proof of Theorem 18.1. This is basically an enhancement of a Weil group.

Lecture 19: April 23

Recall, last time we had a local field K of residue characteristic p, and a residue field k of size q. Let $G = \operatorname{Gal}(K_s/K)$, and W be the Weil group of K. We have an absolute value on W defined by $W \twoheadrightarrow W^{ab} \overset{\substack{\text{local}\\ \text{CFT}}}{\cong} K^\times \xrightarrow{|\ |} \mathbb{R}$.

Define $t_{s,\ell}$:

$$\begin{tikzcd}
I \arrow[r, two heads] \arrow[rrd, "t_{s,\ell}"] & I/P \cong \prod_\ell \mathbb{Z}_\ell(1) \arrow[r, two heads] & \mathbb{Z}_\ell(1) \\
& & \mathbb{Z}_\ell \arrow[u]
\end{tikzcd}$$

where the map $\mathbb{Z}_\ell \to \mathbb{Z}_\ell(1)$ sends $1 \mapsto \zeta$.

Recall we had

$$\begin{tikzcd}
1 \arrow[r] & I \arrow[r] \arrow[d, equal] & W \arrow[r] \arrow[d, hook] & \mathrm{Frob}^{\mathbb{Z}} \arrow[r] \arrow[d, hook] & 1 \\
1 \arrow[r] & I \arrow[r] & G \arrow[r] & \mathrm{Frob}^{\widehat{\mathbb{Z}}} \arrow[r] & 1
\end{tikzcd}$$

Suppose L is a finite extension of $\mathbb{Q}_\ell$, and $\mathcal{O}$ is the valuation ring of L. Suppose E is any field of characteristic 0.

Definition 19.1. A Weil-Deligne representation over E is a pair (r, N) where

- r is a continuous homomorphism $W \to GL(V)$, where V is some finite-dimensional E-vector space with discrete topology (continuous means that $\ker r \supset$ some open subgroup of I);
- $N \in \operatorname{End} V$ is such that $r(w)Nr(w)^{-1} = |w|N$ for all $w \in W$.

Just as in Grothendieck's monodromy theorem, this implies that N is nilpotent (there's a conjugate of N that's $= q^{-1}N$, so you get an infinite decreasing string of eigenvalues).

Remark 19.2. "Conjugation respects exponentiation": if A and B are matrices, then $B\exp(A)B^{-1} = \exp(BAB^{-1})$. In general, you need the caveat that this only works when this converges, but you don't need to worry about convergence in our situation, because we're dealing with nilpotent matrices.

Theorem 19.3 (Deligne's classification of ℓ-adic representations of W)**.** *Choose a generator ζ of $\mathbb{Z}_\ell(1) := \varprojlim \mu_{\ell^n}$ (this is free of rank 1 as a $\mathbb{Z}_\ell$-module). Choose* Frob $\in W$ *(by the diagram above, it's well-defined modulo an element of the inertia group I). Then there exists an equivalence of categories*

$$\{\ell\text{-adic representations of } W \text{ over } L\} \overset{WD_{\zeta,\mathrm{Frob}}}{\longrightarrow} \{\text{Weil-Deligne representations over } L\}$$

(where L has the ℓ-adic topology on the left, and the discrete topology on the right). Let ρ be the representation that corresponds to (r, N); it is characterized by

$$\rho(\mathrm{Frob}^n \sigma) = r(\mathrm{Frob}^n \sigma) \exp(t_{s,\ell}(\sigma) N)$$

for all $n \in \mathbb{Z}$ and $\sigma \in I$.

This is basically just a repackaging of Grothendieck's ℓ-adic monodromy theorem. This is nontrivial because the r's in Weil-Deligne representations are much more restrictive, because the topology is discrete.

If ζ' and Frob$'$ are any other choices, then $WD_{\zeta,\mathrm{Frob}} \cong WD_{\zeta',\mathrm{Frob}'}$, i.e. there is a unique isomorphism

$$\begin{tikzcd}
 & (r, N) \arrow[dd, "\cong"', "\exists!"] \\
\rho \arrow[ur] \arrow[dr] & \\
 & (r', N')
\end{tikzcd}$$

Sketch of proof. We've already said what the map is in the ← direction. Given r, N, a calculation shows that ρ so defined is an ℓ-adic representation (i.e. you have to show it's a homomorphism).

Conversely, given ρ, use Grothendieck's ℓ-adic monodromy theorem to find

- a finite index $I' \subset I$ such that $\rho(\sigma) = \exp(t_{s,\ell}(\sigma)N)$ for all $\sigma \in I'$
- $N \in \operatorname{End} V$

and define $r(w) = \rho(w)\exp(t_{\ell,\sigma}(\mathrm{Frob}^{-n} w)N)$, where n is chosen so that $\mathrm{Frob}^{-n} w \in I$. Then $r(w) = \mathbb{1}_V$ for all $w \in I'$. Thus r has open kernel. Then (a few details skipped here) $r(N)$ is a Weil-Deligne representation. □

What if we only want representations of G instead of W? Note that $W = I \rtimes \mathrm{Frob}^{\mathbb{Z}}$ and $G = I \rtimes \mathrm{Frob}^{\widehat{\mathbb{Z}}}$. (The topology that $\widehat{Z}$ induces on $\mathbb{Z}$ is that things are getting close to 0 if they are getting more and more divisible, so e.g. $n! \to 0$.)

Given a representation of G, you can always compose to get a representation of W. But you can't go the other way, even by using limits, because the topology is wrong.

Example 19.4. Consider $\rho : W \twoheadrightarrow W/I \cong \mathbb{Z} \to L^\times$ sending Frob $\mapsto 1 \mapsto \ell^{-1}$ (where ℓ is the uniformizer of L).

I claim that it's impossible to extend ρ to a continuous homomorphism $G \to L^\times$. Look at the sequence $\mathrm{Frob}^{n!}$; I claim that this converges to $1 \in G$. This is a profinite group; so you just have to check that this goes to 1 in each finite quotient. This is obvious because each we're looking at finite groups, and eventually the order of the finite group will divide $n!$, so $g^{n!} = 1$ in that finite group. If ρ extends, then $\rho(\mathrm{Frob}^{n!})$ should converge to $\rho(1) = 1$. But $\rho(\mathrm{Frob}^{n!}) = \ell^{-n!}$, and that doesn't converge.

Proposition 19.5. *For $A \in GL_n(\mathbb{Q}_\ell)$, TFAE:*

(1) the characteristic polynomial of A is in $\mathcal{O}[x]$ and $\det A \in \mathcal{O}^\times$;
(2) $AM = M$ for some full (i.e. rank-n) $\mathcal{O}$-lattice $M \leq L^n$;
(3) $A \in C \cdot GL_n(\mathcal{O})C^{-1}$ for some $C \in GL_n(L)$;
(4) the homomorphism $\mathbb{Z} \to GL_n(L)$ sending $m \mapsto A^m$ extends to a continuous homomorphism $\widehat{\mathbb{Z}} \to GL_n(L)$.

Definition 19.6. Say that A is *bounded* if it satisfies the conditions of Proposition 19.5.

"Your success in life is determined by how much linear algebra you know."

Proof. Let $f(x) = x^n + a_{n-1}x^{n=1} + \cdots + a_0$ be the characteristic polynomial of A. Cayley-Hamilton says that $f(A) = 0$, so $A^n = -a_{n-1}A^{n-1} - \cdots - a_0 \cdot \mathbb{1}$.

(1) $\implies$ (2) Let J be any full $\mathcal{O}$-lattice in L^n. Let $M = J + AJ + A^2J + \cdots + A^{n-1}J$ (motivation: if $J \subset M$ then $AJ \subset M$ etc.). This is clearly a finitely-generated $\mathcal{O}$-module; it contains J which has rank n, but is $\subset L^n$ so can't be higher rank. Then $AM = AJ + A^2J + \cdots + A^nJ \subset M$ because A^n is a linear combination of lower powers. You can apply this same argument to the characteristic polynomial of A^{-1}; since $\det A \in \mathcal{O}^\times$, $\det A^{-1} \in \mathcal{O}^\times$ as well, so the same argument shows that $A^{-1}M \subset M$, so $M \subset AM$. Thus $M = AM$.

(2) $\implies$ (1) Choose an $\mathcal{O}$-basis of M. Compute the characteristic polynomial of A, and $\det A$, w.r.t. this basis. Get that the characteristic polynomial of $A \in \mathcal{O}[x]$ and $\det A \in \mathcal{O}$. Apply the same to A^{-1} to get $\det A \in \mathcal{O}^\times$.

(2) $\iff$ (3) Every full $\mathcal{O}$-lattice is $C \cdot \mathcal{O}^n$ for some $C \in GL_n(L)$. Then $\mathrm{Stab}_{GL_n(L)}(C \cdot \mathcal{O}^n) = C\ GL_n(\mathcal{O})C^{-1}$.

(3) $\implies$ (4) Without loss of generality, conjugate to assume $A \in GL_n(\mathcal{O})$. Since $GL_n(\mathcal{O})$ is itself a profinite group, the homomorphism extends.

(4) $\implies$ (2) $\widehat{\mathbb{Z}}$ is compact and existence of the extension means it acts on L^n. So it stabilizes a lattice in L^n. One of the elements acts by A, so A stabilizes a lattice. □

Proposition 19.7. *For continuous $r : W \to GL_n(L)$, TFAE:*

(1) $r(w)$ is bounded for all $w \in W$
(2) $r(w)$ is bounded for some $w \in W \backslash I$
(3) $\overline{r(W)}$ is compact (this is the closure of $r(W)$ in $GL_n(L)$, where L has the ℓ-adic topology)

Lecture 20: April 28

Recall: we had an equivalence of categories between ℓ-adic representations of W over L and Weil-Deligne representations over L, sending $\rho \leftrightarrow (r, N)$. This depended on a choice of Frob $\in W$ and a generator ζ for $\mathbb{Z}_\ell(1)$ over $\mathbb{Z}_\ell$. The point is that ℓ-adic representations are complicated, because L has the ℓ-adic topology, and Weil-Deligne representations are easier, because there L is just considered with the discrete topology. The subset of ℓ-adic representations that come from Galois representations depended on the notion of boundedness: recall that $A \in GL_n(L)$ is *bounded* iff $AM = M$ for some full $\mathcal{O}$-lattice M in L^n.

Proposition 20.1. *For continuous $r : W \to GL_n(L)$ with open kernel, TFAE:*

(1) $r(w)$ is bounded for all $w \in W$;
(2) $r(w)$ is bounded for some $w \in W \backslash I$ (where I is the inertia group);
(3) $\overline{r(W)}$ is compact (this is the closure of $r(W)$ in $GL_n(L)$, where L has the ℓ-adic topology);
(4) $r(W)$ stabilizes some full lattice.

Proof. (1) $\implies$ (2) Trivial.

(2) $\implies$ (3) $\overline{r(I \cdot w^{\mathbb{Z}})} = r(I) \cdot \overline{r(w)^{\mathbb{Z}}}$. I is closed, so $r(I)$ is compact, and $\overline{r(w)^{\mathbb{Z}}}$ is compact since $r(w)$ is bounded. This proves that $r(I \cdot w^{\mathbb{Z}})$ is compact.

But I wanted $\overline{r(W)}$. Recall $W = I \cdot \text{Frob}^{\mathbb{Z}}$, so $I \cdot w^{\mathbb{Z}}$ has finite index in W. So $\overline{r(W)}$ consists of finitely many cosets of $\overline{r(I \cdot w^{\mathbb{Z}})}$, hence is compact.

(3) $\implies$ (4) $\overline{r(W)}$ is compact, so it stabilizes a lattice; $r(W) \subset \overline{r(W)}$ does too.

(4) $\implies$ (1) Each $r(w)$ stabilizes the lattice. □

Here's a variant of Deligne's theorem:

Theorem 20.2. *There is an equivalence of categories*

$$\{\ell\text{-adic rperesentations of } G \text{ over } L\} \longleftrightarrow \{\text{bounded Weil-Deligne representations over } L\}.$$

Proof. Suppose ρ is an ℓ-adic representation of W that corresponds to a Weil-Deligne representation (r, N) under Theorem 19.3. Recall that $G = I \rtimes \text{Frob}^{\widehat{\mathbb{Z}}}$ and $W = I \rtimes \text{Frob}^{\mathbb{Z}}$.

$$\rho \text{ extends to } G = I \rtimes \text{Frob}^{\widehat{\mathbb{Z}}} \iff \rho|_{\text{Frob}^{\mathbb{Z}}} \text{ extends to } \rho|_{\text{Frob}^{\widehat{\mathbb{Z}}}}$$
$$\overset{\text{Prop. 20.1}}{\iff} r \text{ is bounded}$$

$$\overset{\text{Def.}}{\iff} (r, N) \text{ is bounded}$$

(For the second $\iff$, go back to the definition of the correspondence between ρ and (r, N).) □

Definition 20.3. A *unipotent* matrix is a matrix of the form $\mathbb{1}+$ a nilpotent matrix. Equivalently, all its eigenvalues are 1.

If $\operatorname{char} k = 0$, then there is a bijection

$$\{\text{nilpotent } n \times n \text{ matrices}\} \underset{\log}{\overset{\exp}{\rightleftarrows}} \{\text{unipotent } n \times n \text{ matrices}\}.$$

(Why do you need characteristic zero? These things are defined by power series with denominators.) Note that these might not necessarily be homomorphisms, if the matrices don't commute.

Corollary 20.4. *Given a unipotent matrix A and $m \geq 1$, there exists a unique unipotent B such that $B^m = A$.*

Proof. To construct B, take the log, divide by m, and then take the exponential. □

Suppose $k = \overline{k}$. Recall, any $A \in M_n(k)$ is conjugate to a block matrix, where each block has some diagonal entries $\lambda_1, \dots, \lambda_n$ and 1's on the off-diagonal. (This is called *Jordan canonical form.*) (E.g. the identity matrix is a bunch of 1×1 blocks.) You can write this as a sum:

$$\begin{bmatrix} \lambda_1 & 1 & 0 \\ & \lambda_2 & 1 \\ & & \lambda_3 \end{bmatrix} = \begin{bmatrix} \lambda_1 & & \\ & \lambda_2 & \\ & & \lambda_3 \end{bmatrix} + \begin{bmatrix} 0 & 1 & \\ & 0 & 1 \\ & & 0 \end{bmatrix}$$

To check whether two Jordan form matrices commute, you can check block-by-block.

So A can be written as a sum of a diagonalizable matrix + a nilpotent matrix, and these two commute. There is a unique way of doing this.

Now relax the assumption that $k = \overline{k}$, and just assume k is a perfect field (it is important for the field extensions to be separable). The problem is that you won't get the diagonalizable component, because maybe the eigenvalues aren't in k. Let V be a finite-dimensional k-vector space.

Definition 20.5. $A \in \operatorname{End} V$ is semisimple if V is a semisimple k-modules; i.e. it's a direct sum of simple $k[A]$-modules, where "simple" means "irreducible" (no nontrivial proper submodules).

If $k = \overline{k}$, the only simple modules are 1-dimensional, so in this case, semisimple $\iff$ diagonalizable.

Theorem 20.6 (Additive Jordan decomposition)**.** *Any $A \in \operatorname{End} V$ has a unique decomposition $A = S + \mathcal{N}$, where S is semisimple, $\mathcal{N}$ is nilpotent, and $S\mathcal{N} = \mathcal{N}S$.*

(I'm using $\mathcal{N}$ to distinguish between this and the Weil-Deligne N.)

Theorem 20.7 (Multiplicative Jordan decomposition)**.** *Any $A \in GL(V)$ has a unique factorization $A = S \cdot U$, where S is semisimple, U is unipotent, and $SU = US$.*

Remarks 20.8.

- You can do both of these by base-changing to $\overline{k}$.
- The S is the same in both.
- S, $\mathcal{N}$, and U can be expressed as polynomials over k in A.
- The decomposition is respected if an algebra homomorphism $GL(V) \to GL(V)$ is applied.
- Every eigenvector of A is also:
  - ◦ an eigenvector of S with the same eigenvalue
  - ◦ an eigenvector of $\mathcal{N}$ with eigenvalue 0
  - ◦ an eigenvector of U with eigenvalue 1.
- If $A = SU$ is a multiplicative decomposition, then $A^n = S^n U^n$ is a multiplicative decomposition of A^n (since S and U commute)

Let (r, N) be a Weil-Deligne representation. r is a representation of W with open kernel, and N is a nilpotent endomorphism. Write $r(\mathrm{Frob}) = S \cdot U$, where S is semisimple and U is unipotent. (The Weil-Deligne N has nothing to do with the additive decomposition.)

Lemma 20.9. *U and N commute.*

Proof. Consider the conjugation action of $GL(V)$ on $\mathrm{End}(V)$ (i.e. sending $A \mapsto CAC^{-1}$). This is itself a representation. Since $r(\mathrm{Frob})Nr(\mathrm{Frob})^{-1} = q^{-1}N$, N is an eigenvector of $r(\mathrm{Frob})$. So it's also an eigenvector of U, with eigenvalue 1. This means that $UNU^{-1} = 1 \cdot N$. □

Lemma 20.10. *U commutes with $r(w)$ for all $w \in W$.*

Proof. Exercise 10.1(b) says there exists $j \geq 1$ such that $r(\mathrm{Frob}^j) \in$ the center of $r(W)$. The unipotent component is U^j (which is a polynomial in $r(\mathrm{Frob}^j)$). So U^j centralizes $r(W)$ (i.e. it commutes with every element of $r(W)$). Now I claim that U also centralizes $r(W)$: just take j^{th} roots (which are unique) of the previous statement (alternatively, take the log, divide by j, and take exp, which all preserve the fact that your matrix commutes with everything). □

Lemma 20.11.

(1) The unipotent component of $r(\mathrm{Frob}^n\sigma)$ is U^n (here $n \in \mathbb{Z}$ and $\sigma \in I$).
(2) The unipotent component of $r(\mathrm{Frob}^n\sigma)\exp(aN)$ is U^n for all $n \in \mathbb{Z}\backslash\{0\}$, $\sigma \in I$, $a \in E$. (Excluding 0 is important: if $n = 0$ and $\sigma = 1$, then $\exp(aN)$ is its own unipotent component.)

Proof. (1) $r(\mathrm{Frob}^n\sigma)$ has a positive integer power equal to $r(\mathrm{Frob})^m$ for some $m \in \mathbb{Z}$. (This is again by homework, at least for $n \neq 0$. If $n = 0$, use the fact that $r(I)$ is a finite group (by compactness of I), so some power of it is 1.)

So the conclusion is true for $r(\mathrm{Frob})^m$ and any power, hence true for any rot of this.

(2) $r(\mathrm{Frob}^n\sigma)\exp(aN)$ is a conjugate of $r(\mathrm{Frob}^n\sigma)$ by $\exp(bN)$ for suitable $b \in E$. By (1), the unipotent component is a conjugate of U^n by $\exp(bN)$. Since U commutes with N (Lemma 20.9), it commutes with any power series in N, in particular $\exp(bN)$. So this is just U^n. □

Define $r^{ss} : W \to GL(V)$ by

$$r^{ss}(\mathrm{Frob}^n\sigma) = r(\mathrm{Frob}^n\sigma)U^{-n}.$$

(Here V is the same E-vector space as in $r : W \to GL(V)$.)

Remarks 20.12.

- By Lemma 20.10, r^{ss} is a homomorphism.
- Like r, it has open kernel, since $r^{ss}|_I = r|_I$.
- (r^{ss}, N) is another Weil-Deligne representation.
  (r conjugates N in the right way; you need to show that the power of U doesn't mess it up, but that's OK because U commutes with N.)

The Weil-Deligne representation (r^{ss}, N) is called the *Frobenius semi-simplification of* (r, N). So we've forced Frobenius to become semisimple. In fact, it makes almost everything semisimple.

Definition 20.13. Say (r, N) is Frobenius-semisimple if $r^{ss} = r$.

Some equivalent conditions for this:

- $U = 1$
- $r(\mathrm{Frob})$ is semisimple
- $r|_{\langle \mathrm{Frob} \rangle}$ is semisimple
- r is semisimple
- $r(w)$ is semisimple for some $w \in W \backslash I$

Why? Use the fact that $\langle r(\mathrm{Frob}) \rangle$ has finite index in $r(W)$ and $\mathrm{char}\, E = 0$. If you have a matrix that isn't semisimple, e.g. $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, it won't become semisimple by raising to a finite power.

So you just have to check Frobenius. Actually, you can check *any* element outside the inertia group: if $w \in W - I$, all of the above is equivalent to $r(w)$ being semisimple.

If $E = L$, Lemma 20.11 allows us to add an extra equivalent condition: $\rho(w)$ is semisimple for all $w \in W \backslash I$, where ρ corresponds to (r, N).

Lecture 21: April 30

Recall we defined the Frobenius semisimplification of a Weil-Deligne representation r. The point is to make $r(\text{Frob})$ semisimple; if $r(\text{Frob}) = S \cdot U$, then you kill the U part by defining $r^{ss}(\text{Frob}^n \sigma) := r(\text{Frob}^n \sigma)U^{-n}$. Last time, we showed that (r, N) is Frobenius semisimple iff $r^{ss} = r$ iff r is semisimple iff $r(\text{Frob})$ is semisimple.

Example 21.1. Let V_{Sp} be a vector space with basis $e_0, \dots, e_{n-1}$ over any E of characteristic 0. Define $r_{Sp} : W \to GL(V)$ by $r_{Sp}(w)e_i = |w|^i e_i$. Then define $N = N_{Sp} \in \operatorname{End} V_{Sp}$ by: $Ne_0 = e_1$, $Ne_1 = e_2$, $\dots Ne_{n-1} = 0$. Then (r_{Sp}, N_{Sp}) is a Weil-Deligne representation.

There's a generalization of this: let $r : W \to GL(V)$ be a representation with open kernel. Define $\mathcal{V} = V \oplus \dots \oplus V$. Let $w \in W$ act on $\mathcal{V}$ by $r(w)$, $|w|r(w)$, $\dots$, $|w|^{n-1}r(w)$. Let N act on $\mathcal{V}$ by right shift (N applied to something in in the first copy of V is the same element, but in the second copy of V, etc.). This is called $Sp_n(r)$. In fact, $Sp_n(r) = (r \otimes r_{Sp}, 1 \otimes N_{Sp}) = (r, 0) \otimes Sp_n$.

Proposition 21.2. *The indecomposable (i.e. ones you can't write as a nontrivial direct sum)*[3] *Frobenius-semisimple Weil-Deligne representations are $Sp_n(r)$ for irreducible representations $r : W \to GL(V)$ and $n \geq 1$.*

Reference: Antwerp II (see official reference list), Deligne's $GL(2)$ article, Proposition 3.13(ii).

Sketch of proof. Let (r, N) be a Frobenius semisimple Weil-Deligne representation on vector space V. So r is semisimple. Let n be the smallest integer such that $N^n = 0$. For $i = 0, 1, \dots, n$ define $K_i = \ker N^i$. By definition of Weil-Deligne representations, K_i is a subrepresentation of V. You get a chain of subrepresentations $0 = K_0 \subset K_1 \subset \cdots \subset K_n = V$.

Start by writing $K_n = K_{n-1} \oplus Z_n$ where Z_n is a subrepresentation.

Claim 21.3. *$N : Z_n \to NZ_n$ is an isomorphism of vector spaces, and $K_{n-2} \cap NZ_n = 0$ (this implies that NZ_n and K_{n-2} are direct summands of K_{n-1}).*

Proof of claim. If $z_n \in Z_n$ satisfies $Nz_n \in K_{n-2}$, then $N^{n-2}(Nz_n) = 0$ so $z_n \in K_{n-1}$. But we also assumed it's in Z_n, so $z_n = 0$. In addition to showing the second part of the claim, this also shows N acts injectively.

By the commutation relation on WD representations, $r(w)Nz_n = |w|Nr(w)z_n$, so $Z_n \otimes |\ \ | = NZ_n$ as representations of W. □

So you can keep going, writing

$$K_{n-1} = K_{n-2} \oplus NZ_n \oplus Z_{n-1}$$
$$K_{n-2} = K_{n-3} \oplus N^2 Z_n \oplus NZ_{n-1} \oplus Z_{n-2}$$

[3] This is weaker than irreducible, because you might have $0 \subset W \subset V$ but if W doesn't have a complement, then you might not be able to write $V = W \oplus ??$.

$$\vdots$$

$$K_1 = \{0\} \oplus N^{n-1} Z_n \oplus N^{n-2} Z_{n-1} \oplus \ldots \oplus Z_1$$

So the direct summands of K_n are all the pieces $N^a Z_b$.

Conclusion: $V \cong K_n = Sp_n(Z_n) \oplus Sp_{n-1}(Z_{n-1}) \oplus \ldots \oplus Sp_1(Z_1)$. If V is indecomposable, then $V \cong Sp_n(Z_n)$ and Z_n is indecomposable. Since r is semisimple, indecomposable = irreducible.

You also have to check that the Sp_n's are actually indecomposable, but that's not too hard so I'll skip it. □

Local Langlands.

Now all representations are over $\mathbb{C}$.

Lemma 21.4 (Schur's lemma)**.** *Let G be a group, and let $\rho : G \to GL(V)$ be a finite-dimensional irreducible representation over $\mathbb{C}$. If $A : V \to V$ is a map of representations (i.e. $A \in \operatorname{End} V$ commutes with $\rho(g)$ for all $g \in G$), then $A = \lambda \cdot \mathbb{1}_V$ for some $\lambda \in \mathbb{C}$.*

Proof. Let λ be any eigenvalue of A. Then $A - \lambda \cdot \mathbb{1}$ commutes with $\rho(g)$ for all g, so $\ker(A - \lambda)$ is a subrepresentation of V, so it has to be 0 or V. It can't be 0 because λ actually had an eigenvector, so $\ker(A - \lambda) = V$. This means that A is multiplication by λ. □

Reference for local Langlands stuff: lecture notes for a summer school by Wedhorn (see official reference list).

Definition 21.5. Let $\pi : GL_n(K) \to GL(V)$, where K is a nonarchimedean local field of residue field characteristic p (e.g. a finite extension of $\mathbb{Q}_p$)[4] and V is a (possibly infinite-dimensional) $\mathbb{C}$-vector space. Say that π is *admissible* if:

- For every V, $\operatorname{Stab}(v)$ is an open subgroup in $GL_n(Kj)$. (This condition is often written "π is *smooth*".) I.e., $V = \bigcup_{\text{open } H \leq GL_n(K)} V^H$.
- For every open subgroup $H \leq GL_n(K)$, V^H is finite-dimensional.

Proposition 21.6. *If $\pi : GL_n(K) \to GL(V)$ is an irreducible admissible representation, then for each $z \in K^\times =$ (center of $GL_n(K)$), $\pi(z) = \omega(z) \cdot \mathbb{1}_V$ for some $\omega(z) \in \mathbb{C}^\times$.*

Proof. Homework (basically a variant of Schur's lemma). □

Definition 21.7. Call $\omega : K^\times \to \mathbb{C}^\times$ is the *central character* of π.

[4] There's also local Langlands for the archimedean case ($\mathbb{R}$ and $\mathbb{C}$) and it's easier than the case we'll discuss.

Corollary 21.8. $\dim V \leq \chi_0$.

Now, time for the *local Langlands correspondence for $GL_n(K)$*!

Theorem 21.9 (Harris-Taylor, as restated by Henniart)**.** *Let K be a local field of residue characteristic p.*

There is a unique sequence of bijections

$$\mathscr{A}_n := \underbrace{\left\{ \begin{array}{c} \textit{irreducible admissible} \\ \textit{representations of } GL_n(K) \end{array} \right\}}_{\text{“automorphic/ } GL_n \text{ side”}} \xrightarrow{rec_n} \underbrace{\left\{ \begin{array}{c} n\textit{-dim. Frobenius semisimple} \\ \textit{Weil-Deligne representations}/\mathbb{C} \end{array} \right\}}_{\text{“Galois side”}} =: \mathscr{G}_n$$

for $n \geq 0$ such that

1. *$rec_1 : \{$characters $K^\times \to \mathbb{C}^\times\} \to \{1$-dim. representations $W \to \mathbb{C}^\times\}$ is composition $W \twoheadrightarrow W^{ab} \cong K^\times$ by local CFT. (Notes on why $\mathscr{A}_1$ and $\mathscr{G}_1$ are as advertised: by Schur's lemma, representations on the left are 1-dimensional because $GL_1 = K^\times$ is abelian; $N = 0$ on the right because there's only one 1×1 nilpotent matrix, so you can forget about $N \ldots$.)*
2. *For $\pi_1 \in \mathscr{A}_{n_1}$, $\pi_2 \in \mathscr{A}_{n_2}$ and any additive character $\psi : K \to \mathbb{C}^\times$ (note ψ determines a self-dual dxon K),*
$$L(\pi_1 \times \pi_2, s) = L(rec_{n_1}(\pi_1) \otimes rec_{n_2}(\pi_2), s)$$
$$\varepsilon(\pi_1 \times \pi_2, s, \psi) = \varepsilon(rec_{n_1}(\pi_1) \otimes rec_{n_2}(\pi_2), s, \psi)$$
(All this stuff is to be defined, but think of it as a generalization of the character L-functions (i.e. the $n = 1$ case here) that we defined in the Tate's thesis part of the course.)
3. *For $\pi \in \mathscr{A}_n$, $\chi \in \mathscr{A}_1$,*
$$rec_n(\pi\chi) = rec_n(\pi) \otimes rec_1(\chi)$$
4. *There is a commutative diagram:*
$$\begin{tikzcd} \mathscr{A}_n \arrow[r, "rec_n"] \arrow[d, "\substack{central\\ char.}"'] & \mathscr{G}_n \arrow[d, "\substack{compose\ with\\ \det: GL_n(\mathbb{C}) \to \mathbb{C}^\times}"] \\ \mathscr{A} \arrow[r, "rec_1"] & \mathscr{G}_1 \end{tikzcd}$$
5. *There is a commutative diagram*
$$\begin{tikzcd} \mathscr{A}_n \arrow[r, "rec_n"] \arrow[d, "dual"'] & \mathscr{G}_n \arrow[d, "dual"] \\ \mathscr{A}_n \arrow[r, "rec_n"] & \mathscr{G}_n \end{tikzcd}$$
(I've not explained what dual means.)

The automorphic side is supposed to be the "easy side" – $GL_n(K)$ is supposed to be something you know. The RHS is the "hard side", because it involves the Weil group, which involves the Galois group.

Trivial case: if $n = 0$, then $GL_n(K) = 0$, so $\mathscr{A}_n$

Lecture 22: May 5

$$\begin{aligned}\pi : GL_n(K) \to GL(V) \text{ is smooth } &\iff \text{ for every } v \in V,\ \mathrm{Stab}_{GL_n(K)}(V) \text{ is open in } GL_n(K)\\ &\iff GL_n(K) \times V \to V \text{ is continuous for the discrete topology on } V\end{aligned}$$

Definition 22.1. Let $\pi : GL_n(K) \to GL(V)$ be an admissible representation. The *smooth dual (contragredient)* of V is

$$V^\vee = \left\{\lambda \in \mathrm{Hom}(V, \mathbb{C}) \,:\, \mathrm{Stab}_{GL_n(K)}(\lambda)\right\} \text{ is open.}$$

The non-obvious condition here is just to make sure that this is smooth.

Facts 22.2.

- V is admissible
- $V \cong V^{ab}$

Setup: let K be a nonarchimedean local field of characteristic p. Let $G = \mathrm{Gal}(K_s/K)$, and let W be the Weil group.

Let L be a finite extension of $\mathbb{Q}_\ell$.

$$\begin{tikzcd}
\left\{\begin{matrix}\text{finite-image}\\ K^\times \to \mathbb{C}^\times\end{matrix}\right\} \arrow[r, hook] \arrow[dd, leftrightarrow] & \{K^\times \to \mathbb{C}^\times\} \arrow[rr, hook] \arrow[dd, "\begin{matrix}rec_1\\ \text{(local CFT)}\end{matrix}"', "\cong"] & & \left\{\begin{matrix}\text{irred. adm.}\\ GL_n(K) \to GL(\underbrace{V}_{\mathbb{C}\text{-VS}})\end{matrix}\right\} \arrow[d, "rec_n"', "\sim"] & \\
 & & & \left\{\begin{matrix}n\text{-dim. Frob-ss}\\ \text{WD reps}/\mathbb{C}\end{matrix}\right\} \arrow[d, hook] & \\
\{G \to \mathbb{C}^\times\} \arrow[r, hook] \arrow[dr, hook] & \{W \to \mathbb{C}^\times\} \arrow[r, hook] & \left\{W \to GL(\underbrace{V}_{\mathbb{C}\text{-VS}})\right\} \arrow[r, hook, "r \mapsto (r{,}0)"'] & \{\text{WD reps}/\mathbb{C}\} \arrow[dr, hook] & \\
 & \{G \to GL(V)\} \arrow[u, hook] & & & \left\{\begin{matrix}\text{all WD reps}\\ \text{over all } E\end{matrix}\right\} \\
 & & & \{\text{WD reps}/\ L\} \arrow[ur, hook] \arrow[d] & \\
 & & \{\ell\text{-adic reps of } G\} \arrow[r] & \left\{\begin{matrix}\ell\text{-adic reps of } W \text{ over } L\\ \text{not necessarily open kernel}\end{matrix}\right\} & \\
 & \{\text{smooth proj. vars}/K\} \arrow[ur, "\ell\text{-adic cohomology}"] & & &
\end{tikzcd}$$

Now the plan is to attach L-factors to the following items in the chart:

(1) $\{K^\times \to \mathbb{C}^\times\}$
(2) $\{W \to \mathbb{C}^\times\}$
(3) $\{W \to GL(V)\}$
(4) $\{\text{WD reps}/\mathbb{C}\}$

(5) $\{$WD reps over all $E\}$.

If we do this, then you get L-factors on everything else by looking at what it maps to.

(1) Recall we've already done this:

$$L(\chi) = \begin{cases} (1-\chi(\varpi))^{-1} & \text{if } \chi \text{ is unramified (i.e. } \chi|_{\mathcal{O}_K^\times} = 1) \\ 1 & \text{if } \chi \text{ is ramified} \end{cases}$$

To get a meromorphic function of $s \in \mathbb{C}$, recall that adding a factor of $|\ \ |^s$ doesn't change whether it's ramified or not, so consider

$$L(\chi|\ \ |^s) = \begin{cases} (1-\chi(\varpi)q^{-s})^{-1} & \text{if } \chi \text{ is unramified} \\ 1 & \text{otherwise} \end{cases}$$

(2) (1-dimensional characters of the Weil group) is isomorphic to the above. Recall the uniformizer of K corresponds to the geometric Frobenius, so our L-factors are:

$$L(\chi) = \begin{cases} (1-\chi(\mathrm{Frob}))^{-1} & \text{if } \chi \text{ is unramified } (\chi|_I = 1) \\ 1 & \text{if } \chi \text{ is ramified} \end{cases}$$

(3) Now let's try to define L-factors on representations $W \to GL(V)$ where V is a finite-dimensional $\mathbb{C}$-VS.

Problem: Frobenius is only well-defined up to the inertia group. One idea is to average over all possibilities. But if the inertia group acts nontrivially, then it all cancels out. Instead, restrict to the subspace where the inertia group acts trivially. I.e. define:

$$L(V) = \det(1 - \mathrm{Frob}|_{V^I})^{-1}.$$

Now for some intuition that this (especially the determinant part) is the right thing to define:

Example 22.3. Suppose $\dim V = 1$. If V is unramified, $V^I = V$, so $L(V) = (1-r(\mathrm{Frob}))^{-1}$.

If V is ramified, then $V^I = 0$. Now we're taking the determinant of a 0×0 matrix, which is 1; i.e. $L(V) = 1$.

This shows that this is compatible with definition (2).

Example 22.4. If $V = \chi_1 \oplus \chi_2$ where each character is unramified, then $V^I = V$, and

$$\begin{aligned} L(V) &= \det\left(\mathbb{1} - \begin{bmatrix} \chi_1(\mathrm{Frob}) & 0 \\ 0 & \chi_2(\mathrm{Frob}) \end{bmatrix}\right)^{-1} \\ &= (1-\chi_1(\mathrm{Frob}))^{-1}(1-\chi_2(\mathrm{Frob}))^{-1} \\ &= L(\chi_1)L(\chi_2) \end{aligned}$$

So this is a motivation for using the determinant: it's multiplicative in the appropriate sense.

More generally,

Proposition 22.5. *If $0 \to V_1 \to V_2 \to V_3 \to 0$ is an exact sequence of representations of W, then $L(V_2) = L(V_1)L(V_3)$.*

Proof. Usually when you take group invariants, it's not an exact functor:

$$0 \to V_1^I \to V_2^I \to V_3^I \to H^1(I, V_1) \to \dots$$

But I claim that the H^1 term is zero. All of these things are complex vector spaces, so the H^1 term is a $\mathbb{C}$-vector space. But it's a profinite group, i.e. the limit of finite groups, so every element has finite order. The only complex vector space with this property is 0.

So we have a SES $0 \to V_1^I \to V_2^I \to V_3^I \to 0$. If you choose a basis for V_1^I and V_3^I and choose the induced basis for V_2^I, the matrix $\mathrm{Frob}|_{V_2^I}$ looks like $\begin{pmatrix} \mathrm{Frob}|_{V_1^I} & * \\ 0 & \mathrm{Frob}_{V_3^I} \end{pmatrix}$ so $\det(\mathrm{Frob}_{V_2^I}) = \det(\mathrm{Frob}|_{V_1^I}) \det(\mathrm{Frob}|_{V_3^I})$. □

Proposition 22.6. *Let $L \supset K$ be a finite separable extension. Note that G_L is a finite-index subgroup of G_K, so W_L is a finite-index subgroup of W_K. Let V_L be a representation of W_L over $\mathbb{C}$. Let $V_K := \mathrm{Ind}_{W_L}^{W_K}(V_L)$ (this is a representation of W_K).*

Then $L(V_K) = L(V_L)$.

Recall: we have exact sequences

$$\begin{tikzcd}
1 \arrow[r] & I_K \arrow[r] & W_K \arrow[r] & \mathrm{Frob}_K \arrow[r] & 1 \\
1 \arrow[r] & I_L \arrow[r] \arrow[u, hook] & W_L \arrow[r] \arrow[u, hook] & \mathrm{Frob}_L^{\mathbb{Z}} \arrow[r] \arrow[u, hook] & 1
\end{tikzcd}$$

Frob_L maps to $(\mathrm{Frob}_K)^f$ (where f is residue field degree).

Proof.

$$\begin{aligned}
V_K^{I_K} &= (\mathrm{Hom}_{W_L}(W_K, V_L))^{I_K} && \text{where } I_K \text{ acts on } W_K \\
&= \mathrm{Hom}_{W_L}(\underbrace{W_K/I_K}_{\mathrm{Frob}_K^{\mathbb{Z}}}, V_L) \\
&= \mathrm{Hom}_{W_L}(\mathrm{Frob}_K^{\mathbb{Z}}, V_L^{I_L}) && \text{images have to land in the inertia-invariants} \\
&= \mathrm{Hom}_{W_L}(\mathrm{Frob}_K^{\mathbb{Z}}, V_L^{I_L}) && \text{since } I_L \text{ acts trivially on both} \\
&= \mathrm{Ind}_{\mathrm{Frob}_L^{\mathbb{Z}}}^{\mathrm{Frob}_K^{\mathbb{Z}}}(V_L^{I_L})
\end{aligned}$$

Idea: we're inducing from $f\mathbb{Z}$ up to $\mathbb{Z}$. A representation of $f\mathbb{Z}$ is easy to describe: you just have to say where the generator goes.

This reduces to a fun linear algebra problem:

Lemma 22.7. *Let $\langle F \rangle$ be an infinite cyclic group with generator F, and let $n \geq 1$. Let V be a finite-dimensional representation of $\langle F^n \rangle$ over $\mathbb{C}$. Then $\det(1 - F|_{\mathrm{Ind}_{\langle F^n \rangle}^{\langle F \rangle} V}) = \det(1 - F^n|_V)$.*

(We're using $n = f$.)

Proof of Lemma. Without loss of generality take $V = \mathbb{C}^m$. $F^n|_V$ is just a matrix in $GL_m(\mathbb{C})$. Both sides are polynomials in the entries of $F^n|_V$. Diagonalizable matrices are dense in the space of all matrices, so by continuity, we may assume that $F^m|_V$ is diagonalizable, i.e. V is a direct sum of 1-dimensional vector spaces. Without loss of generality $V = \mathbb{C}$, and $F^n|_V = a$ (some element of $\mathbb{C}$).

$$\mathrm{Ind}_{\langle F^n\rangle}^{\langle F\rangle}\mathbb{C} = \left\{h : \langle F\rangle \to \mathbb{C} \,:\, h(F^n \cdot F^i) = ah(F^i)\ \forall i \in \mathbb{Z}\right\}$$

I claim that this is $\cong \mathbb{C}$, because you just have to specify the first n powers of F; i.e. the isomorphism takes $h \mapsto (h(F^0), \dots, h(F^{n-1}))$. The F-action is a shift action:

$$A := \begin{bmatrix} 0 & & & a \\ 1 & \ddots & & \\ & \ddots & 0 & \\ & & 1 & 0 \end{bmatrix}$$

Now we need to calculate the determinant: $\det(1 - A) = 1 - a$.

□

Proposition 22.8. *Every irreducible $r : W \to GL(V)$ (where V is a finite-dimensional $\mathbb{C}$-vector space) is $\rho : |\ \ |^s$ for some finite-image $\rho : W \to GL(V)$ and some $s \in \mathbb{C}$.*

Proof. By the homework, there exists some $j \geq 1$ such that $r(\mathrm{Frob}^j) \in$ center of $r(W)$. By Schur's lemma, $r(\mathrm{Frob}^j) = c \cdot \mathbb{1}_V$ for some $c \in \mathbb{C}^\times$. Choose $s \in \mathbb{C}$ so that $|\mathrm{Frob}^j|^s c$. Let $\rho = r|\ \ |^{-s}$. Then $\rho(\mathrm{Frob}^j) = 1$, so $\rho(I) = r(I)$ is finite. I and Frob generate all of the Weil group; $\left\langle I, \mathrm{Frob}^j\right\rangle$ has finite index in W. So $\rho(W)$ is finite. □

Now let's get back to defining L-factors. The point about Weil-Deligne representations is that they encode things about ℓ-adic representations. Over L, suppose the ℓ-adic representation ρ corresponds to the WD representation (r, N). Recall the correspondence, defined on $\mathrm{Frob}^n\sigma$, is $\rho(\mathrm{Frob}^n\sigma) = r(\mathrm{Frob}^n\sigma)\exp(t_{\zeta,\ell}(\sigma)N)$. In order for something to be fixed by the inertia group is if it's fixed by $\exp(\mathrm{const} \cdot N)$, i.e. it has to be in the kernel of N. It should also be fixed by r. That is,

$$V^{\rho(I)} = (\ker N)^{r(I)}.$$

Now we can define the L-factor for a Weil-Deligne representation (r, N) over $\mathbb{C}$:

$$L((r, N)) = \det(1 - \mathrm{Frob}|^I_{\ker N})^{-1}$$
$$L((r, N), s) = \det(1 - q^{-s}\mathrm{Frob}|_{(\ker N)^I})^{-1}$$

Replacing (r, N) by (r^{ss}, N) does not change these.

In case (5) (all WD representations over all E), you can't get a meromorphic function of complex numbers: you have a matrix with E-entries. It's kind of a cop-out, but you can define zeta functions similarly by

$$Z((r,N),t) := \det(1 - t\mathrm{Frob}|_{(\ker N)^I})^{-1}.$$

This is an element in $E(t)$.

If $E \subset \mathbb{C}$, one can substitute $t = q^{-s}$ to get $L((r,N),s)$.

Lecture 23: May 7

Let $L \supset K$ be a finite separable extension of local fields. We defined V_L, a representation of the Weil group W_L over $\mathbb{C}$, and showed $L(\mathrm{Ind}_{W_L}^{W_K} V_L) = L(V_L)$. If K is a local field and V is a representation of W over $\mathbb{C}$, we defined $L(V) := \det(1 - \mathrm{Frob}|_{V^I})^{-1}$.

Virtual representations. Let G be a finite (or profinite) group. Maschke's theorem says that the category of finite-dimensional (continuous, if G is profinite) representations V of G over $\mathbb{C}$ is semisimple: every such V is $\bigoplus_{\substack{\text{irred.}\\ V_i}} V_i^{\oplus n_i}$ for some $n_i \in \mathbb{N}$ that are almost all zero.

Definition 23.1 (Definition #1 of virtual representations)**.** A *virtual representation* is a formal expression $\bigoplus_{\substack{\text{irred}\\ V_i}} V_i^{\oplus n_i}$ where $n_i \in \mathbb{Z}$ almost all zero. (Think of this as a formal difference of two actual representations.)

Let $R(G)$ be the set of all virtual representations. This is a commutative ring where $+$ is induced by $\oplus$ of representations, and $\oplus$ is induced by $\otimes$ (extended linearly).

Definition 23.2 (Definition #2 of virtual representations)**.** There is an embedding

$$\{\text{f.d. representations of } G/\mathbb{C}\} / \cong \hookrightarrow \{(\text{locally constant}) \text{ functions } G \to \mathbb{C}\}$$

sending $V \mapsto \chi_V$, where $\chi_V(g) := \mathrm{Tr}(g|_V)$. Note that the RHS is a commutative ring.

Let $R(G)$ be the additive group generated by the image.

Definition 23.3 (Definition #3 of virtual representations)**.** Let $R(G)$ be the Grothendieck group of the category of finite-dimensional representations of G over $\mathbb{C}$. That is, take the free abelian group with basis consisting of symbols $[V]$ for every finite-dimensional representation V, and then mod out by the relation $[V] = [V'] + [V'']$ for every short exact sequence $0 \to V' \to V \to V'' \to 0$.

Note that you only need a symbol for every irreducible representation, and if you only take those, you don't need any relations.

Definition #3 generalizes to finite-dimensional continuous representations of any topological group over any field E, even if Maschke's theorem doesn't apply. Even if a representation isn't the direct sum of irreducibles, you can still break it down to irreducibles using short exact sequences, so you still have $R(G) = \bigoplus_{\substack{\text{irred}\\ V}} \mathbb{Z}$ as an abelian group.

$R(G)$ has the following universal property: If A is an abelian group, giving a group homomorphism $f : R(G) \to A$ is the same as specifying $f(V)$ for each finite-dimensional representation V such that $f(V) = f(V') + f(V'')$ for every SES $0 \to V' \to V \to V'' \to 0$. (If f satisfies this property we say that f is *additive.*)

Example 23.4.

- $\dim : R(G) \to \mathbb{Z}$
- $\det : R(G) \to \mathrm{Hom}(G, \mathbb{C}^\times)$ (given a representation ρ, this assigns a function $G \overset{\rho}{\to} GL_n(\mathbb{C}) \overset{\det}{\to} \mathbb{C}^\times$)
- $(-,-) : R(G) \times R(G) \to \mathbb{Z}$ sending $V, W \mapsto \frac{1}{\#G} \sum \chi_V(g)\overline{\chi_W(g)}$. This only makes sense for finite groups; in the profinite case, replace $\frac{1}{\#G} \sum$ with $\int_G$ (using Haar measure). If V, W are irreducible, then (V, W) is 1 if $V \cong W$, and 0 otherwise.
- Given a closed subgroup $H \leq G$, get a restriction map $\mathrm{Res} : R(G) \to R(H)$.
- Given an open subgroup $H \leq G$, get an induced representation $\mathrm{Ind}_H^G : R(H) \to R(G)$ sending $V \mapsto V \otimes_{\mathbb{C}H} \mathbb{C}G$.

Theorem 23.5 (Frobenius reciprocity)**.** *Let $H \leq G$ be an open subgroup. If $V \in R(G)$ and $W \in R(H)$, then*

$$(\mathrm{Res} V, W)_H = (V, \mathrm{Ind}_H^G W)_G.$$

(I mean that the pairing on the left is the pairing in H, and the one on the right is the pairing in G.)

Theorem 23.6 (Brauer's theorem)**.** *Let $H \leq G$ be an open subgroup. The* monomial representations *(i.e. $\mathrm{Ind}_H^G \chi$ where $\chi : H \to \mathbb{C}^\times$ is 1-dimensional) generate $R(G)$ as an abelian groups.*

(Explicitly, $\mathrm{Ind}_H^G \chi$ looks like a permutation matrix, where instead of 1's in the matrix, there are arbitrary nonzero values.)

Artin L-series. Let K be a global field, and $G = \mathrm{Gal}(K_s/K)$. If v is a finite place of K, then we have:

- K_v = the completion at v
- $G_v = \mathrm{Gal}(K_{v,s}/K_v)$ (the image of this in G is the decomposition group)
- I_v = the inertia group
- Frob_v
- q_v = cardinality of the residue field

Let V be a (possibly virtual) finite-dimensional representation of G. Then you get a representation of G_v, namely $V_v := V|_{G_v}$. These are the same *as vector spaces.*

Let

$$L(V_v, s) := \det(1 - q_v^{-s} \mathrm{Frob}_v|_{V^{I_v}})^{-1}$$

be the local L-factor defined earlier for V_v. (If you want, you can think of this as $V_v^{I_v}$ instead; it doesn't matter.) It's like a characteristic polynomial...

Definition 23.7. The Artin L-series is

$$L(V,s) := \prod_{\substack{\text{finite} \\ v}} L(V_v, s)$$

You can expand out $L(V_v, s)$ as a Dirichlet series, and so $L(V,s)$ will also be a Dirichlet series (i.e. it looks like a ζ-function).

There's also a completed version where you put in Γ-factors for the archimedean places, but we haven't talked about those.

Examples 23.8.

- If $V = \mathbb{1}$ (the trivial representation), then $L(V,s) = \zeta_K(s)$: you're talking about a 1×1 matrix whose entry is 1.
- If $\dim V = 1$, then the completed Artin L-series is a Hecke L-function.

Proposition 23.9. *$L(V,s)$ converges (as a function of s) for $\operatorname{Re} s > 1$.*

Proof. Let $n = \dim V$. $\mathrm{Frob}_v|_{V^{I_v}}$ is a matrix of finite order, so its eigenvalues are all rots of unity. So

$$L_v(V,s) = \prod_{\leq n} (1 - q_v^{-s}\lambda)$$

where λ are eigenvalues, and there are $\leq n$ of them. Thus

$$\begin{aligned} \prod L_v(s) \text{ converges } &\Longleftarrow \sum q_v^{-s} \text{ converges} \\ &\Longleftarrow \zeta_K(s) \text{ converges} \\ &\Longleftarrow \operatorname{Re} s > 1 \end{aligned}$$

□

Corollary 23.10. *For $V \in R(G)$, one can define $L(V,s)$ as a nonvanishing holomorphic function on $\operatorname{Re} s > 1$.*

Proposition 23.11. *Let K'/K be a finite separable extension of global fields. Then we have an inclusion $G_{K'} \subset G_K$. Let V' be a finite-dimensional representation of $G_{K'}$; then*

$$V = \mathrm{Ind}_{K'/K} V' = \mathrm{Ind}_{G_{K'}}^{G_K} V'.$$

(Note that V) is a representation of G_K and V' is a representation of $G_{K'}$.

We will use the local version $L(\mathrm{Ind}_{W_L}^{W_K} V_L) = L(V_L)$ we proved last time in Proposition 22.6. This is more general than we need – it's about Weil groups, not Galois groups.

Sketch of proof. Let v be a finite place of K. Use the fact from group theory

$$(\mathrm{Ind}_{K'/K}V')_v \cong \bigoplus_{w|v} \mathrm{Ind}_{K'_w/K_v} V'_w.$$

($(-)_v$ means I'm restricting to the decomposition group.) Note that $\mathrm{Ind}_{K'w/K_v} V'_w$ is a representation of G_{K_v}, and $\mathrm{Ind}_{K'/K}V'$ is defined to be V. So if we take local L-factors on both sides, we get

$$L(V_v, s) = \prod_{w|v} L(\mathrm{Ind}_{K'_w/K_v} V'_w, s) \overset{\text{Prop. 22.6}}{=} \prod_{w|v} L(V'_w, s).$$

Multiply over all finite v of K to get $L(V, s) = L(V', s)$. □

Suppose K'/K is a finite Galois extension of global fields, with Galois group $\mathcal{G}$. Recall $\mathbb{C}\mathcal{G}$ is the regular representation of $\mathcal{G}$, but we can view it as a representation of G_K. This is $= \mathrm{Ind}_{K'/K}\mathbb{1}$. So

$$L(\mathbb{C}\mathcal{G}, s) = \zeta_{K'(s)}.$$

Also,

$$\prod_{\substack{\text{irred. reps.}\\ V \text{ of } G}} L(V, s)^{\dim V} = L(\mathbb{C}\mathcal{G}, s).$$

As an example of this, recall last term we proved

$$\zeta_{\mathbb{Q}(\zeta_n)}(s) = \prod_{\chi:(\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times} L(\chi, s).$$

The L-function corresponding to the trivial character is the Riemann ζ-function.

Now make a small generalization of this: let K'/K be a finite separable extension of global fields (not necessarily Galois). You can still talk about the induced representation $\mathrm{Ind}_{K'/K}\mathbb{1}$, but there's no more $\mathcal{G}$ for it to be $\mathbb{C}\mathcal{G}$. However, previously we could have viewed $\mathcal{G} = G_K/G_{K'}$ (corresponding to the tower diagram $K_s/K'/K$). We can still talk about $G_K/G_{K'}$ as a set of cosets, and it's still a G_K-set. So you can still form the permutation module $\mathbb{C}[G_K/G_{K'}]$ (vector space spanned by the cosets, with action of G_K). I claim that

$$L(\mathbb{C}[G_K/G_{K'}]) = \zeta_{K'}(s).$$

Theorem 23.12. *Every Artin L-series extends to a meromorphic function on $\mathbb{C}$ and there is a functional equation relating $L(V, s)$ to $L(V^*, 1 - s)$.*

Proof. By Brauer's theorem, it suffices to check monomial representations $V = \mathrm{Ind}_{K'/K}\chi$, where $\chi : G_{K'} \to \mathbb{C}^\times$. The L-series for V is the same as the L-series for χ, so it suffices to check just for χ. But now we're in a special case of Hecke L-series (well, uncompleted…). So we're done! □

There's a conjecture that most of these L-series are holomorphic. We already proved that in the Hecke case. Here, you're taking Hecke L-functions, inducing them up, and taking products *and quotients* of them. So it's kind of unusual that you should expect them to be holomorphic…

Lecture 24: May 12

Last time we were talking about Artin L-series. Let K be a global field, $G = \mathrm{Gal}(K_s/K)$, and V a finite-dimensional representation of G over $\mathbb{C}$. Recall we defined

$$L(V,s) = \prod_{v \nmid \infty} \det(\mathbb{1} - q_v^{-s}\mathrm{Frob}_v|_{V^{I_v}})^{-1}$$

where q_v is the size of the residue field and I_v is the inertia group of the local version of G.

Recall:

Theorem 24.1 (Brauer's theorem)**.** *Ever finite-dimensional representation of a (pro)finite group over $\mathbb{C}$ is a $\mathbb{Z}$-linear combination of representations induced from 1-dimensional representations on subgroups (these are called monomial representations).*

As a consequence of this,

Theorem 24.2. *Every Artin L-series is a ratio of products of Hecke L-series associated to idèle class characters of finite extensions of K. (The finite extensions correspond to subgroups of the Galois group.)*

Corollary 24.3. *$L(V,s)$ is meromorphic on $\mathbb{C}$.*

Conjecture 24.4 (Artin holomorphy conjecture)**.** For every irreducible representation V of G that is not the trivial representation of G_K, $L(V,s)$ is holomorphic on all of $\mathbb{C}$.

The point of the nontriviality condition is you have to exclude the Dedekind zeta function, which is not holomorphic. But the conjecture says that this is basically the only thing that can go wrong.

We proved the Artin holomorphy conjecture for $\dim V = 1$. Weil proved this when K is a global function field (this relates to the Weil conjectures).

Example 24.5. Let K'/K be a finite separable extension. Then $\mathrm{Ind}_{K'/K}\mathbb{C} = \mathbb{C}[G_K/G_{K'}]$ (permutation representation, with basis indexed by cosets). Think of those as functions on the set of cosets; you can embed $\mathbb{C} \subset$ this by taking the constant functions. I claim that $\mathrm{Ind}_{K'/K}\mathbb{C} = \mathbb{C}[G_K/G_{K'}] = \mathbb{C} \oplus V$ (where the copy of $\mathbb{C}$ on the left is the trivial representation of $G_{K'}$ and the $\mathbb{C}$ on the right is the trivial representation of G_K). Applying L-factors to $\mathrm{Ind}_{K'/K}\mathbb{C} = \mathbb{C} \oplus V$, we get $\zeta_{K'}(s) = \zeta_K(s)L(V,s)$.

Conjecture 24.6. Every zero of $\zeta_K(s)$ is also a zero of $\zeta_{K'}(s)$.

There are some things that are known about this.

Remark 24.7 (Aramata-Brauer)**.** If K'/K is also a Galois extension, then some positive integer multiple of χ_V (this is the V in $\mathbb{C} \oplus V$) is a *nonnegative* integer combination of monomial characters.

So you're multiplying together a bunch of Hecke L-series, and those are known to be holomorphic. So the Artin holomorphy conjecture holds.

A consequence of Theorem 24.2 is:

Theorem 24.8. *If the generalized Riemann hypothesis holds for all (completed) Dedekind zeta functions of number fields (i.e.* $\widehat{\zeta_K(s)}$ *has all its zeros on* $\operatorname{Re} s = \frac{1}{2}$ *– multiplying by Gamma factors cancels out the trivial zeros) then all zeros and poles of all completed Artin* L*-series are on* $\operatorname{Re} s = \frac{1}{2}$*.*

Of course, there aren't supposed to be any poles.

Proof of Chebotarev density theorem using Artin L-functions. There's actually a shortcut, where you can use some cheap group theory (groups are generated by cyclic subgroups, which are abelian) to prove this only using abelian L-series. But we won't do this.

Setup:

- K is a global field
- v is a nonarchimedean place of K
- K_v is the completion at v
- $\mathbb{F}_v$ is the residue field
- $q_v = \#\mathbb{F}_v$

Definition 24.9. If $P \subset \{\text{all } v\}$, define its *Dirichlet density* as

$$\delta(P) := \lim_{s \to 1^+} \frac{\sum_{v \in P} q_v^{-s}}{\log \frac{1}{s-1}}.$$

Think of the sum as related to the log of the Dedekind zeta function. At $s = 1$ it will diverge (like the harmonic series).

Remark 24.10. Changin P at finitely many places doesn't change δ. (Each individual term has a finite limit as $s \to 1$.) So we can just forget about finitely many places we don't like (e.g. ramified places).

To explain why this is a good definition:

Proposition 24.11. $\delta(\{\textit{all } v\}) = 1$.

Proof. Frob acts as a 1×1 matrix with a 1 inside. Recall $\zeta_K(s) = \prod_v (1 - q_v^{-s})^{-1}$ has a simple pole at $s = 1$. Define $f(s)$ by $\zeta_K(s) = \frac{1}{s-1} f(s)$; now f has a finite nonzero limit as $s \to 1^+$. Take the log of $\frac{1}{s-1} f(s) = \prod_v (1 - q_v^{-s})^{-1}$ to get

$$\begin{aligned} \log\left(\frac{1}{s-1}\right) + O(1) &= \sum_v (q_v^{-s} + O(q_v^{-2s})) \\ &= \sum_v q_v^{-s} + O(1) \end{aligned}$$

This proves the density is 1: divide the above equation by $\log\left(\frac{1}{s-1}\right)$, which goes to infinity. □

If K is a number field, there is also a *natural density*

$$\delta_{\text{natural}}(P) = \lim_{X \to \infty} \frac{\#\{v \in P \,:\, q_v \leq X\}}{\#\{\text{all } v \,:\, q_v \leq X\}}.$$

(fraction of primes that lie in your set). This only works well when K is a number field; if you're working with characteristic p, all the q_v's are powers of p, so the number jumps whenever you hit a power of p.

If $\delta_{\text{natural}}(P)$ exists, so does $\delta(P)$ and they are equal.

Let L/K be a finite Galois extension of global fields. Let $G = \mathrm{Gal}(L/K)$. Let v be a place of K; it might split into several places L.

Recall: if L/K is unramified above v, then we have $\mathrm{Frob}_w \in G$ for each $w \mid v$. Changing w just conjugates Frob_w by the element of the Galois group taking one w to the other. Thus $\mathrm{Frob}_v = \{\mathrm{Frob}_w \,:\, w \mid v\}$ is a conjugacy class in G.

How are these conjugacy classes distributed?

Theorem 24.12. *Lt L, K, and G be as above. Let C be a fixed conjugacy class in G. Then*

$$\delta(\{\textit{unramified } v \,:\, \mathrm{Frob}_v = C\}) = \frac{\#C}{\#G}.$$

Definition 24.13. Let G be a finite group. $f : G \to \mathbb{C}$ is a *class function* if f is constant on each conjugacy class C in G. Then $f(C) = f(c)$ for any $c \in C$.

Example 24.14. If $\rho : G \to GL(V)$ is a finite-dimensional representation of G over $\mathbb{C}$, then its character $\chi_\rho(g) = \operatorname{Tr} \rho(g)$ is a class function.

Fact 24.15. *$\{\chi_\rho \,:\, \rho$ is an irreducible representation of G over $\mathbb{C}\}$ is a $\mathbb{C}$-basis for the set of class functions.*

Definition 24.16.

$$\delta(f) := \lim_{s\to 1^+} \frac{\sum_v f(\mathrm{Frob}_v) q_v^{-s}}{\log \frac{1}{s-1}}$$

If $f = \mathbb{1}_C$, then $\delta(f) = \delta(\{v : \mathrm{Frob}_v = C\})$ (the sum is just counting the v's that you care about in the Chebotarev density theorem).

Proof of Chebotarev density theorem. We'll prove more generally that for any class function f,

$$\delta(f) = \frac{1}{\#G}\sum_{g\in G} f(g).$$

It's a generalization of the Chebotarev density theorem, but it's actually equivalent; any such f is a formal $\mathbb{C}$-linear combination of the ones you care about. So there are two bases for the same space: irreducible characters, and f's that appear in the Chebotarev density theorem; the proof involves the first basis.

By linearity, without loss of generality f is a character χ of some irreducible ρ.

$$L(\rho, s) = \prod_{\text{unram. } v} \det(\mathbb{1} - q_v^{-s}\rho(\mathrm{Frob}_v))^{-1} \cdot e^{O(1)}$$

There's a multiplicative error term coming from the bad (i.e. ramified) Euler factors (it doesn't approach 0 or ∞ as $s \to 1^+$). Now factor the characteristic polynomial of $\rho(\mathrm{Frob})$ in terms of eigenvalues $\lambda_{v,i}$; say there are d of them (with multiplicity).

$$= \prod_{\text{unram. } v}\prod_{i=1}^{d}(1 - q_v^{-s}\lambda_{v,i})^{-1}$$

All the eigenvalues are roots of unity – this is because G is finite. Take the log and see what happens when $s \to 1$. Use the same estimate for $\log(1-x)^{-1}$ as earlier.

$$\log L(\rho, s) = \sum_v \sum_{i=1}^{d} (q_v^{-s}\lambda_{v,i} + O(q_v^{-2s})) + O(1)$$

If the L-function has order of vanishing m, it looks like $(s-1)^m \cdot$ (something bounded). Also use the fact that the sum of the eigenvalues is the trace, and the $O(q_v^{-2s})$'s are bounded.

$$(\mathrm{ord}_{s=1} L(\rho, s)) \cdot \log(s-1) + O(1) = \sum \chi(\mathrm{Frob}_v) q_v^{-s} + O(1)$$

Divide by $-\log(s-1)$ and take the limit

$$-\mathrm{ord}_{s=1} L(\rho, s) = \delta(\chi)$$

On the homework you compute the order of vanishing: it's -1 if $\rho \cong \mathbb{1}$ and zero otherwise. This is $-(\chi, 1) = -\frac{1}{\#G}\sum \chi(g)$. □

Lecture 25: May 14

"Where is the homeland of zeta values to which the true reasons of celestial phenomena of zeta values are attributed? How can we find a galaxy train to approach it?" – Kazuya Kato

Why study ζ-function and L-series? ζ-functions go back to Euler, but Dirichlet invented L-series to prove the theorem on primes in arithmetic progressions.

- Equidistribution theorems
  - ○ Dirichlet's theorem on primes in arithmetic progressions
  - ○ Chebotarev density theorem
  - ○ Behavior of an elliptic curve over $\mathbb{Q}$ mod p as p values
- Prime number theorem (number of primes up to X is asymptotically $\frac{\log X}{X}$)
- Special values at integers
  - ○ $\zeta(2) = \frac{\pi^2}{6}$, etc.
  - ○ Dirichlet analytic class number formula
  - ○ Birch and Swinnerton-Dyer conjecture $\operatorname{ord}_{s=1} L(E, s) = \operatorname{rank} E(\mathbb{Q})$
  - ○ Relations with algebraic K-theory

Local ε-factors.

Theorem 25.1 (Deligne)**.** *There exists a unique function $\varepsilon : \{(V, \psi, dx)\} \to \mathbb{C}^\times$ (where V is a finite-dimensional representation of W_K for some local field K, ψ is a nontrivial additive character of K, and dx is a Haar measure on K) such that:*

(1) (Additive) For every exact sequence $0 \to V' \to V \to V'' \to 0$,

$$\varepsilon(V, \psi, dx) = \varepsilon(V', \psi, dx)\varepsilon(V'', \psi, dx).$$

This lets us define $\varepsilon(V, \psi, dx)$ also for virtual representations $V \in R(W_K)$.

(2) $\varepsilon(V, \psi, a\, dx) = a^{\dim V}\varepsilon(V, \psi, dx)$ (where $a \in \mathbb{R}_{>0}$). In particular, if $\dim V = 0$ (which happens all the time for virtual representations), ε is independent of dx, and we may write $\varepsilon(V, \psi)$.

(3) ("Inductive in dimension zero") If $L \supset K$ is a finite separable extension of local fields, and $V_L \in R(W_L)$ is of dimension zero, then $\varepsilon(\operatorname{Ind}_{L/K} V_L, \psi) = \varepsilon(V_L, \psi \circ \operatorname{Tr}_{L/K})$.

(4) ("Normalization") If V is a 1-dimensional representation (so V corresponds to a multiplicative character χ of $K^\times$), then $\varepsilon(V, \psi, dx) = \varepsilon(\chi, \psi, dx)$, where the RHS is as defined in the first half of the class.

The uniqueness is (relatively) easy: once you know how to do it for 1-dimensional characters, and you know how to induce (albeit for 0-dimensional representations), then you can use Brauer's theorem to get all the rest. But existence is hard: there might be many ways to write a representation as a combination of 1-dimensional characters.

Bonus: Hilbert's irreducibility theorem. Reference: Serre's *Lectures on the Mordell-Weil theorem.* (This uses some algebraic geometry, which I will try to avoid.)

Theorem 25.2. *Suppose $f(x, y) \in \mathbb{Q}(t)[x]$ is irreducible over the field $\mathbb{Q}(t)$. Then there exist infinitely many $t_0 \in \mathbb{Q}$ such that:*

(1) $f(x, t_0) \in \mathbb{Q}[x]$ has no zeros in $\mathbb{Q}$

(2) (Hilbert irreducibility theorem) $f(x, t_0)$ is irreducible over $\mathbb{Q}$
(3) $\mathrm{Gal}_{f(x,t_0)} = \mathrm{Gal}_f$, where Gal_f is the Galois group of the splitting field L of f over $\mathbb{Q}(t)$.

If λ is a prime in $\mathcal{O}_L$ over $\mathbb{Q}[t]$, then let $\mathbb{F}_\lambda$ denote the corresponding residue field (and note that the residue field corresponding to the prime $(t - t_0)$ is $\mathbb{Q}$). Then there's a SES

$$1 \to I_\lambda \to D_\lambda \to \underbrace{\mathrm{Gal}(\mathbb{F}_\lambda/\mathbb{Q})}_{\mathrm{Gal}_{f(x,t_0)}} \to 1$$

where we note that $D_\lambda \subset \mathrm{Gal}_f$. Also, I_λ is trivial for all but finitely many t_0, so you can view $\mathrm{Gal}_{f(x,t_0)}$ as a subgroup of Gal_f.

Example 25.3. $x^2 - t$ is irreducible over $\mathbb{Q}(t)$. The theorem says that there are infinitely many $t_0 \in \mathbb{Q}$ such that $x^2 - t_0$ is irreducible over $\mathbb{Q}$.

Lemma 25.4. *Every finite extension of $\mathbb{C}((t))$ is $\mathbb{C}((t^{1/n}))$ for some $n \geq 1$.*

Elements of $\mathbb{C}((t^{1/n}))$ are called Puiseux series.

Proof. Let L be such an extension. $L/\mathbb{C}((t))$ is totally ramified: there can't be any nontrivial residue field because then it would be an extension of the residue field of $\mathbb{C}((t))$, namely $\mathbb{C}$, which doesn't have any extensions. It's also totally *tamely* ramified: you can only have wild ramification in characteristic p. But we have a classification for these: $L = \mathbb{C}((t))(\pi^{1/n})$ for some $\pi = tu$ (where $u = u_0 + u_1 t + \cdots \in \mathbb{C}[[t]]^\times$ where $u_0 \neq 0$). By Hensel's lemma, u is an n^{th} power in $\mathbb{C}((t))^\times$. So $1 = \mathbb{C}((t))(t^{1/n}) = \mathbb{C}((t^{1/n}))$. □

We have $\mathbb{C}(t) \subset \mathbb{C}((\frac{1}{t}))$, Laurent series expansions at ∞. Take the closure of this: $\overline{\mathbb{C}(t)} \subset \overline{\mathbb{C}((\frac{1}{t}))}$, where the latter is the field of Puiseux series at ∞.

Example 25.5. $\sqrt{t^3 + t^2} = t^{3/2} + \frac{1}{2}t^{1/2} - \frac{1}{8}t^{-1/2} + \dots$

Just as Laurent series at ∞ converge for some "neighborhood of ∞", you can show that each Puiseux series at ∞ of an element of $\overline{\mathbb{C}}(t)$ converges for real $t \geq R$, for some large number R.

Proposition 25.6. *Let $\varphi \in \overline{\mathbb{C}((\frac{1}{t}))}\backslash\mathbb{C}[t]$, and suppose $\varphi(t)$ converges for $t \geq R$. Let $\Omega = \{t \geq R : t \in \mathbb{Z}$ and $\varphi(t) \in \mathbb{Z}\}$. Then there exists $\varepsilon > 0$ such that $\#(\Omega \cap [1, B])$ is $O(B^{1-\varepsilon})$.*

Example 25.7. If $\varphi(t) = t^{1/2} + 5t^{-1/2} + \dots$ then for large t, I claim that t and $t+1$ cannot both be in Ω: by the mean value theorem, $\varphi(t+1) - \varphi(t) \approx \varphi'(t) \approx \frac{1}{2}t^{-1/2} \ll 1$. Similarly, t and $t + c$ cannot both be in Ω, at least if $c \ll \mathrm{const} \cdot t^{1/2}$.

The general proof is along the same lines. But this example wouldn't work if the leading term was $t^{3/2}$. In the case, you have to take second derivatives (i.e. second differences).

To prove Proposition 25.6, we need a lemma:

Lemma 25.8. *Notation as in Proposition 25.6. Choose $n \geq 1$ such that $\varphi^{(n)} = c_u t^{-u} + \dots$ for some $u > 0$. Then there exists $\alpha > 0$ such that for all $t \gg 1$, $[t, t + t^{\alpha}]$ contains at most n elements of Ω.*

(In the example, we only needed 2 elements to get the contradiction; in the general case, we need more.)

Proof. Suppose $t_1, \dots, t_{n+1} \in \Omega \cap [t, t + t^{\alpha}]$ are distinct. In the mean value theorem, you compare your function to the linear function that passes through those two points. Here, let $P(x)$ be the degree n polynomial such that $P(t_i) = \varphi(t_i)$ for $i = 1, 2, \dots, n+1$. This is Lagrange interpolation; the formula for this is

$$P(x) = \sum_{i=1}^{n+1} \varphi(t_i) \cdot \frac{\prod_{j \neq i}(x - t_j)}{\prod_{j \neq i}(t_i - t_j)} =: p_n \frac{x^n}{n!} + \dots \in \mathbb{Q}[x].$$

(This should make sense; the quotient term is zero at every t_j except t_i, and has the value 1 there thanks to the denominator.)

You prove the mean value theorem by applying Rolle's theorem. Here, you apply it (to $P - \varphi$) n times. (If you start with $n+1$ zeros, you get n zeros on the derivative, etc.) So you get $\tau \in [t, t + t^{\alpha}]$ such that $P^{(n)}(\tau) = \varphi^{(n)}(\tau)$. I know this isn't identically zero, so it's $c_u t^{-u} + \dots$ for some nonzero c_u. I know $P^{(n)}(\tau)$ is just the coefficient p_n, a rational number with *denom*$(p_n) \leq$ the lcm of the denominators in the $P(x)$ formula, which is $\leq \left|\prod_{1 \leq i < j \leq n+1}(t_i - t_j)\right| \leq t^{\frac{n(n+1)}{2}\alpha}$. Choose α such that $\frac{n(n+1)}{2}\alpha < u$ to get a contradiction. □

Proof of Proposition 25.6. Divide by interval $[1, B]$ into $[1, B^{\delta}]$ and $[B^{\delta}, B]$, and subdivide the latter interval into intervals each of width $B^{\alpha\delta}$. I'll use the trivial bound for $[1, B^{\delta}]$, namely $\#(\Omega \cap [1, B^{\delta}]) \leq B^{\delta}$; for each of the little intervals use Lemma 25.8 to get an estimate $\Omega \cap$ interval $\leq n$, and there are $\frac{B}{B^{\alpha\delta}}$ of them. So the total is $O(B^{1-\varepsilon})$ for some $\varepsilon > 0$. □

Proof of Theorem 25.2(1). Let $f \in \mathbb{Q}(t)[x]$ be irreducible. Let $\varphi_1, \dots, \varphi_{\alpha}$ be its roots in the field of Puiseux series at ∞; they are algebraic over $\mathbb{Q}(t)$. You can think of these as curves in the t vs. x plane. Puiseux series, e.g. $x = \varphi_i(t)$, are the curves in the plane that asymptotically approach an x-value as $t \to \infty$. I claim that most of the time, when you plug in t_0, you don't get rational points above it.

Claim 25.9. *There are infinitely many $t_0 \in \mathbb{Z}_{\geq 1}$ such that none of the $\varphi_i(t_0)$ are in $\mathbb{Q}$.*

Proof of claim. Multiply the φ_i by a nonzero polynomial in $\mathbb{Z}[t]$ to assume that the φ_i are *integral* over $\mathbb{Z}[t]$. Then $\varphi_i(t_0)$ is integral over $\mathbb{Z}$ for any $t_0 \in \mathbb{Z}$ large enough, so $\varphi_i(t_0) \in \mathbb{Q}$ iff $\varphi_i(t_0) in \mathbb{Z}$. Proposition 25.6 says that the number of $t_0 \in [1, B]$ such that $\varphi_i(t_0) \in \mathbb{Z}$ is $O(B^{1-\varepsilon})$ for each i. Sum over i: there are only d of them, and each of them is only contributing $O(B^{1-\varepsilon})$ bad values. There are plenty of t_0 left over such that there are no bad values.

□

Proof of Theorem 25.2(2,3). It suffices to prove (3), as the Galois group acts transitively on the roots. Recall L is the splitting field of f; we have $L = \mathbb{Q}(t)(\varphi_1, \ldots, \varphi_\alpha)$. Write $G := \mathrm{Gal}_f$; this is a finite group. For each subgroup $H \lneq G$, choose ψ generating L^J over $\mathbb{Q}(t)$. Without loss of generality φ is integral over $\mathbb{Z}[t]$. Let $F(x)$ be its minimal polynomial over $\mathbb{Q}(t)$. It is irreducible (it's a minimal polynomial) of degree ≥ 2, because the extension $L^H/\mathbb{Q}(t)$ it generates is nontrivial.

For example, suppose $G = S_n$ and $H = A_n$, and we want to know when the specialized Galois group $\mathrm{Gal}_{f(t_0,x)}$ is contained in A_n. Let $\Delta = \operatorname{disc} f$. Define $\psi := \sqrt{\Delta} = \prod_{i<j}(\varphi_i - \varphi_j)$. Then $F(x) = x^2 - \Delta$. Then I specialize and ask whether $\mathrm{Gal}_{f(t_0,x)} \subset A_n$; this is true iff $x^2 - \Delta(t_0)$ has a root in $\mathbb{Q}$. The point is to relate statements about Galois groups to statements about auxiliary polynomials.

Lemma 25.10. *Excluding finitely many t_0's, if $\mathrm{Gal}_{f(x,t_0)} \subset H$, then $F(x, t_0)$ has a root in $\mathbb{Q}$.*

Proof of Lemma. Recall $D_\lambda \cong \mathrm{Gal}(\mathbb{F}_\lambda/\mathbb{Q}) = \mathrm{Gal}_{f(x,t_0)}$ because the inertia group is (almost always) trivial. So the condition $\mathrm{Gal}_{f(x,t_0)} \subset H$ means $D_\lambda \subset H$. If $h \in D_\lambda$, then $h(\varphi \pmod{\lambda}) = \varphi \pmod{\lambda}$ (because that's how φ was chosen: ${}^h\varphi = \varphi$ and ${}^h\lambda = \lambda$ since $h \in D_\lambda$). So $(\varphi \pmod{\lambda}) \in \mathbb{Q}$, and $\varphi \pmod{\lambda}$ is a root of $F(x, t_0)$. □

$F(x, t_0)$ has a root in $\mathbb{Q}$ happens only for $O(B^{1-\varepsilon})$ t_0's. Do this argument for every H, and add this up; it's still rare. □

Another Kato quote (talking about Bloch and Beilinson's work about relations to algebraic K-theory):

"It seems to me that the only known general method for discovering general elements is to open our mouths and wait for such elements to fall from the sky. I don't know how people with small mouths can catch such elements so often."