REPRESENTATION THEORY AND NUMBER THEORY

Contents

Date: Fall 2011.

These notes are taken from Dick Gross' lectures at Columbia University on representation theory and number theory.

1. Tuesday September 20

Number theorists would like to understand extensions of $\mathbb{Q}$, but we have few ways of constructing extensions. Until very recently it wasn't known how to give nonabelian extensions $k/\mathbb{Q}$ or $\mathbb{F}(X)/\mathbb{F}(t)$ with discriminant 2^a or 3^b. The Langlands conjectures give a way of doing this.

1.1. **The local Langlands conjectures.** We consider k a local field. (Examples are $\mathbb{Q}_v$, $\mathbb{F}((t))$). If $k \neq \mathbb{R}$ or $\mathbb{C}$ then $A \subset k$ is the ring of integers has an element with $A/\pi A = \mathbb{F}$ finite. Let k^s be the separable closure of k. Then $\mathrm{Gal}(k^s/k)$ is a profinite group. Local class theory says that

$$Gal(k^s/k)^{ab} = \text{ the profinite completion of } k^\times.$$

The local Langlands conjectures are supposed to generalize this.

Set up: G is a reductive group over k. (eg. $GL_n, \mathrm{SL}_2, \mathrm{Sp}_{2n}, \ldots$) $\widehat{G}$ is the so-called dual group. (eg. $\mathrm{GL}_n(\mathbb{C}), \mathrm{PGL}_3(\mathbb{C}) = \mathrm{SO}(3), \mathrm{SO}_{2n+1}(\mathbb{C}), \ldots$) The initial form of the conjecture is that irreducible complex representations of $G(k)$ should correspond to

$$\{\varphi : \mathrm{Gal}(k^s/k) \to \widehat{G}(\mathbb{C}) \text{ up to conjugacy by } \widehat{G}(\mathbb{C})\}.$$

In the $G = \mathrm{GL}_1$ case this says that

$$\{\chi : k^\times \to \mathbb{C}^\times\} \leftrightarrow \{\rho : \mathrm{Gal}(k^s/k) \to \mathbb{C}^\times\}.$$

This is exactly what local class field theory tells us is the case. So, the general conjecture is supposed to generalize local class field theory.

Problems:

(1) We want this theory to contain the theory of highest weights. In other words, if $k = \mathbb{R}$ or $\mathbb{C}$, we should be able to recover the description of the irreducible representations of $G(\mathbb{C})$ in terms of their highest weights, but $\mathrm{Gal}(\mathbb{C}/\mathbb{C})$ is trivial and so this is clearly not the case in our naive conjecture. (The solution will be to replace $\mathrm{Gal}(k^s/k)$ with the Weil group W_k.)
(2) The image of φ will be comprised of semisimple elements, and it will be necessary to account for nilpotents. So we will need to introduce a nilpotent element in $\widehat{\mathfrak{g}}$, or equivalently, $\mathrm{SL}_2(\mathbb{C}) \to \widehat{G}$.

(3) We will need to replace $\widehat{G}$ by ${}^L G$ which contains $\widehat{G} = ({}^L G)^0$ as a normal subgroup.
(4) Unlike the abelian case, the correspondence is generally finite-to-one instead of one-to-one. This has to do with the notion of L-packets.

Even though we have these problems, it turns out that the naive notion already treats a lot of interesting examples. So we will work with this idea for the rest of the lecture.

1.2. **Some examples.** A continuous *parameter* $\varphi : \mathrm{Gal}(k^s/k) \to \widehat{G}(\mathbb{C})$ contains the following information.

- A finite extension K/k through which φ factors.
- Thus a finite subgroup $H \subset \widehat{G}(\mathbb{C})$ that is the image of φ. (Note that in the case $G = \mathrm{SL}_2, \widehat{G} = \mathrm{PGL}_2(\mathbb{C}) = \mathrm{SO}(3)$, the possible finite subgroups have been classified. They are cyclic, dihedral, A_4, S_4 and A_5. Remark: A_5 can't be the image φ because it is not solvable, but all of the other possibilities do arise.)
- We need a given isomorphism D (the decomposition group which has filtration $D \supset D_1 \supset D_2 \supset \cdots$) with H up to conjugacy by $N_{\widehat{G}(\mathbb{C})}(H)$.

1.3. **Unramified representations/parameters.** In terms of the filtration mentioned before, we now consider the case when $D_0 = 1$. This means that K/k has degree n is unramified, or in other words, $\mathrm{Gal}(K/k) = \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ where $q = \#A/\pi A$ and $n = [K : k]$. A generator of $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is given by $F : \alpha \mapsto \alpha^q$.

So $\varphi(F) = s \in \widehat{G}(\mathbb{C})$ must satisfy $s^n = 1$ and so it must be semisimple. The semisimple elements are parametrized by $\widehat{T}/W$, but we must also determine which have order n. We do this as follows. We will assume that G is split.

Our goal is to associate to $s \in \widehat{G}(\mathbb{C})$ a representation π_s of $G(k)$. To do this we consider

$$\mathrm{X}_\bullet(\widehat{T}) = \mathrm{Hom}_{\mathbb{C}}(\mathbb{G}_m, \widehat{T}) = \mathrm{X}^\bullet(T) = \mathrm{Hom}_k(T, \mathbb{G}_m).$$

(This equality is a consequence of how $\widehat{T}$ is defined.) First, we claim that s gives a character $\chi_s : T(k)/T(A) \to \mathbb{C}^\times$. To see this note that

$$T(k)/T(A) = \mathrm{X}_\bullet \otimes k^\times / \mathrm{X}_\bullet \otimes A^\times \simeq \mathrm{X}_\bullet(T).$$

Every semisimple element s (up to conjugacy) must be contained in $\widehat{T} = \mathrm{X}_\bullet(\widehat{T}) \otimes \mathbb{C}^\times = \mathrm{X}^\bullet(T) \otimes \mathbb{C}$, so we can think of s as being a character of T which we denote by

$$\chi_s : T \to \mathbb{C}^\times.$$

Choosing a Borel B such that $T(k) \subset B(k) \subset G(k)$, we can define

$$\pi_s = \mathrm{Ind}_B^G \chi_s \delta_B^{1/2}$$

where δ_B is the modular character and its presence makes the definition of π_s independent of the choice of B.

It is not true that π_s will be irreducible. When it is reducible the irreducible subquotients give an example of an L-packet.

Example 1.3.1. $G = \mathrm{SL}_2$. Then $\widehat{G} = \mathrm{PGL}_2(\mathbb{C})$ and an element in $\widehat{T}$ can be written as $s = \begin{pmatrix} t & \\ & 1 \end{pmatrix}$. That it have order n means that $t = \zeta_n$ is an n-th root of unity. The centralizer of s in $\widehat{G}$, $C_{\widehat{G}}(s)$ is the normalizer of the orbit of s. (Since we are doing things up to conjugacy, it is reasonable that this should be of interest.) If $n \geq 3$

then $C(s) = \widehat{T}$, but if $n = 2$ we have $s = \begin{pmatrix} -1 & \\ & 1 \end{pmatrix}$ is conjugate to $\begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$ but these do not differ by an element of $\widehat{T}$. Indeed,

$$C(s) = N(\widehat{T}) = O_2$$

which is not connected. The group of connected components $A_\varphi = C(s)/C(s)^0$ is $\mathbb{Z}/2$ in this case, and this accounts for the fact that π_s has two subquotients when $s = \begin{pmatrix} -1 & \\ & 1 \end{pmatrix}$.

The group A_ϕ is important. Somehow[1], there is a $\rho : A_\phi \to \mathrm{GL}_n(\mathbb{C})$.

1.4. **Other examples.** If C_φ is finite, φ is called a *discrete* parameter. These correspond to discrete series representations. Unramified parameters are never discrete because $\Im(\varphi) = \langle s \rangle$ has dimension zero, so $\dim C(s) \geq \mathrm{rank}(\widehat{G}) \geq 1$. So, C_φ is infinite.

Where the unramified parameters correspond to $D_0 = 1$ in the filtration $D \supset D_0 \supset D_1 \supset \cdots$, the next simplest case of parameters are those for which $D_1 = 1$. These are called *tamely ramified* parameters. In this case φ factors through $\mathrm{Gal}(k^{tame}/k)$. If k is p-adic then $\mathrm{Gal}(k^{un}/k) = \widehat{Z}$ and the maximal tamely ramified extension has $\mathrm{Gal}(k^{tame}/k^{un}) = \prod_{\ell \neq p} \mathbb{Z}_\ell$. In the function field case, i.e. $k = \mathbb{F}_q((t))$, $k^{un} = \bar{\mathbb{F}}_q((t))$ and $k^{tame} = \bar{\mathbb{F}}((t^{1/n}))$ for all n coprime to p. In either case, the Galois group is (topologically) generated by two elements:

$$\mathrm{Gal}(k^{tame}/k) = \langle \tau, F \mid F\tau F^{-1} = \tau^q \rangle.$$

We conclude that to give a tamely ramified parameter, we need $\varphi : \mathrm{Gal}(k^{tame}/k) \to \widehat{G}$ which factors through a finite extension K/k. Then $\varphi(\tau) = s$ and $\varphi(F) = n$ must satisfy $nsn^{-1} = s^q$.

Question: are there any tamely ramified parameters that are discrete? Assume that $s \in \widehat{T}$ is *regular*, i.e. $C_{\widehat{G}}(s) = \widehat{T}$. Consider the natural projection of the normalizer of $\widehat{T}$ onto the Weil group:

$$N_{\widehat{G}}(\widehat{T}) \to N_{\widehat{G}}(\widehat{T})/\widehat{T} =: W(\widehat{T}, \widehat{G}) = W.$$

For $n = \varphi(F) \in N_{\widehat{G}}(\widehat{T})$, let w be its image in the Weyl group. Then $C(\varphi) = \widehat{T}^w$. It can happen that this is finite.

Example 1.4.1. Let $G = \mathrm{SL}_2$ as before. Then $\widehat{T} = \mathrm{SO}(2) \lhd N(\widehat{T}) = O_2(\mathbb{C})$ and $W = \mathbb{Z}/2$. Suppose that $s \in \widehat{T}$ is regular. (If the order of s is at least 3 this is automatic.) If $n \mapsto w$ is nontrivial then we must have

$$nsn^{-1} = s^q, \quad n^2 = 1 \qquad \implies \qquad s^{q+1} = 1, \quad n^2 = 1.$$

The relations on right give the dihedral group $D_{2(q+1)}$

Example 1.4.2. Now, further assume that $k = \mathbb{Q}_2$. Then

$$\langle s, n \mid s^3 = 1, n^2 = 1 \rangle = S_3 = \mathrm{Gal}(\mathbb{Q}_2(\zeta_3, \sqrt[3]{2})/\mathbb{Q}_2)$$

gives a tamely ramified parameter φ with $A_\varphi = \mathbb{Z}/2$. (Hence a discrete parameter.)

The Langlands correspondence says there should be 2 representations. Which are they? The group $\mathrm{SL}_2(\mathbb{Q}_p)$ has two maximal open compacts:

$$K = \mathrm{SL}_2(\mathbb{Z}_2), \qquad K' = \begin{pmatrix} 2 & \\ & 1 \end{pmatrix} K \begin{pmatrix} 1/2 & \\ & 1 \end{pmatrix}.$$

[1] I think he was trying to give some explanation of what's going on here in terms of topology. I didn't get what he was saying.

Reduction modulo 2 gives a map
$$K \to \mathrm{SL}_2(\mathbb{Z}/2) \simeq S_3 \to \{\pm 1\}$$
where the final map is the sign character of S_3. Call this composition ϵ. Similarly, one obtains $\epsilon' : K' \to \{\pm 1\}$. The two representations are
$$\pi = \mathrm{Ind}_K^{\mathrm{SL}_2(\mathbb{Q}_2)} \epsilon, \quad \text{and} \quad \pi' = \mathrm{Ind}_{K'}^{\mathrm{SL}_2(\mathbb{Q}_2)} \epsilon'.$$
These are the discrete series representations of the L-packet of our parameter.

1.5. **Wildly ramified representations of $\mathrm{SU}_3(E/k)$.** Let us assume that q is odd. Let $E = k(\sqrt{\pi})$. Then $\mathcal{O} = A + A\sqrt{\pi}$ is the ring of integers in E. Consider the standard Hermitian form
$$\varphi : E^3 \times E^3 \to E \qquad \varphi(z,w) = \sum_{i=1}^{3} z_i \bar{w}_i.$$
Then
$$\mathrm{SU}_3(E) = \{g \in \mathrm{GL}_3 \mid \varphi(gz, gw) = \varphi(z,w) \text{ for all } z, w \in E^3\}.$$
If we define K to be the stabalizer of the natural lattice $\mathcal{O}^3 \subset E^3$, it can be checked that
$$K = \{g : \mathcal{O}^3 \to \mathcal{O}^3 \mid \ {}^t\bar{g}g = 1, \det g = 1\}.$$
Reduction modulo $\sqrt{\pi}$ gives
$$K \to SO_3(\mathbb{F}_q)$$
whereas reduction modulo π gives
$$1 \to V \to K \pmod{\pi^2} \to \mathrm{SO}_3(q) \to 1. \tag{1.5.1}$$
If $g \in V$ then we can write $g = 1 + \pi A$ where ${}^tA = A$, $\operatorname{tr} A = 0$. So V is a 5-dimensional $F = \mathcal{O}/\sqrt{\pi}\mathcal{O}$ vector space.

At this point I didn't understand what was going on. He said something about a form $\Delta : V \to \mathbb{F}$, and that a stable orbit of $\mathrm{SO}_3(q)$ is one for which $\Delta \neq 0$. If you take $\chi : \mathbb{F} \to \mathbb{C}^\times$ a nontrivial character then the identification $V \simeq V^*$ gives a map $\ell : V \to \mathbb{F}$ which is a stable orbit for $\mathrm{SO}_3(q)$. So the composition of these maps gives a character
$$\chi_\ell : \ker(K \to \mathrm{SO}_3(q)) \to \mathbb{C}^\times$$
which is trivial on $K/\pi K$. The kerner, U, is a pro-unipotent parahoric of K. We also get an elliptic curve[2]
$$y^2 = x^3 + I_2 x + I_3.$$
The representation associated to this parameter is $\mathrm{Ind}_U^G \chi_\ell$. (There is something miraculous about this, but I didn't catch what is so remarkable.)

Remark. The exact sequence (1.5.1) is analogous to
$$0 \longrightarrow \mathfrak{sl}_2(\mathbb{Z}_p/p\mathbb{Z}_p) \longrightarrow \mathrm{SL}_2(\mathbb{Z}_p/p^2\mathbb{Z}_p) \longrightarrow \mathrm{SL}_2(\mathbb{Z}_p/p\mathbb{Z}_p) \longrightarrow 1$$
$$X \longmapsto 1 + pX$$
It is easy to verify that this actually gives an exact sequence of groups.

[2] I don't know how this is, or why it's important.

2. Tuesday September 27

If we want to understand $\varphi : \mathrm{Gal}(k^s/k) \to \widehat{G}(\mathbb{C})$ there is a lot of stuff to know. The LHS requires us to understand the work of Artin, Weil, Deligne, Serre, and others. The RHS goes through the work of Chevalley, Borel, Grothendieck and so on. "To really appreciate it you have to understand both sides."

2.1. **Review of algebraic number theory: global theory.** Let k be a number field, i.e. $[k : \mathbb{Q}] = n < \infty$. The integral closure of $\mathbb{Z}$ in k is $A \simeq \mathbb{Z}^n$, hence a lattice in k. There is a non-degenerate pairing

$$\langle \cdot, \cdot \rangle : k \times k \to \mathbb{Q} \qquad \langle x, y\rangle = \mathrm{tr}(xy),$$

and therefore we can consider the dual lattice

$$A^* = \{x \in k \mid \langle x, y\rangle \in \mathbb{Z} \text{ for all } y \in A\}.$$

Then $A \subset A^*$ is of finite index, and $|d| = [A^* : A]$ where for any $\{x_i\}$ a $\mathbb{Z}$-basis of A,

$$d = \det\left[\mathrm{tr}(x_i x_j)\right]$$

is the discriminant of k.

For example, if $k = \mathbb{Q}(i)$ then $A = \mathbb{Z} + \mathbb{Z}i$. Taking the basis $\{1, i\}$ we find that $\mathrm{tr}\,1 = 2, \mathrm{tr}\,i = 0, \mathrm{tr}\,i^2 = -2$, so

$$d = \left|\left(\begin{smallmatrix} 2 & 0 \\ 0 & -2 \end{smallmatrix}\right)\right| = -4.$$

In this case, $A^* = \frac{1}{2}A$.

In the modern language, we consider $k \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. In the 19th century, they thought of this in terms of the *signature pairing*, which would be $(r_1 + r_2, r_2)$.

Let $I \subset k$ by an A-submodule. This is a lattice. An ideal $I \subset A$ is an example of such an object. Given two submodules I, J, we can consider their product

$$IJ = \{\sum_{i=1}^{N} \alpha_i \beta_i \mid \alpha_i \in I, \beta_i \in J\}.$$

Typically, it is hard to describe what this is, but since A is a Dedekind domain, every ideal can be written as a product of prime ideals:

$$I = \prod P_i^{m_i},$$

and this factorization extends to the fractional ideals. In short, the fractional ideals form a group freely generated by the primes and fitting in the following exact sequence.

$$1 \to A^\times \to k^\times \to \mathcal{I} = \bigoplus_{\text{primes } P} \mathbb{Z}P \to Cl(A) \to 0.$$

The map $k^\times \to \mathcal{I}$ is given by $\alpha \mapsto \alpha A$ gives the *principal ideals* (which are the only ideals that are easy to describe.)

The two big theorems in this subject are that $\#Cl(k) < \infty$ and $A^\times$ is finitely generated of rank $r_1 + r_2 - 1$. A lot of what makes this work is that A is a Dedekind domain, but not all.

Analogously, we could consider $A = \mathbb{C}[x, y]/(y^2 = f)x)$ with $f(x)$ a polynomial with distinct roots. In this case $A^\times = \mathbb{C}$ and $Cl(A)$ which equals the Jacobian of the hyperelliptic curve given by $y^2 = f(x)$ are not finite. However, if we replace

$\mathbb{C}$ by the finite field $\mathbb{F}_q$ then everything we said about number fields above goes through in this, the function field, case. (This is Artin's thesis.)

If we consider a prime p of $\mathbb{Q}$, then write $pA = \prod P_i^{e_i}$, the finite field A/P_i has order p^{f_i}. Moreover, $\sum e_i f_i = n$, so $p^n = \#(A/pA)$.

Every ideal is invertible. Let $\mathcal{D}$ be the inverse of A^*. It is called the *different*. For an ideal I let $\mathbb{N}(I) = (A : I) \geq 1$. Then $\mathbb{N}\mathcal{D} = |d|$. We can extend the norm to all fractional ideals: $\mathbb{N} : \mathcal{I} \to \mathbb{Q}_+^\times$.

Let us assume that $k = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/f(x)$. Then $A \supset \mathbb{Z}[\alpha] = \mathbb{Z}[x]/f(x)$. Suppose that p does not divide the index of $\mathbb{Z}[\alpha]$ in A. Then $\mathbb{Z}[\alpha] \cap pA = p\mathbb{Z}[\alpha]$, so

$$A/pA \simeq \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \simeq \mathbb{Z}[x]/(p, f(x)) \simeq \mathbb{Z}/p[x]/\bar{f}[x].$$

Now, write $\bar{f}(x) = \prod_{i=1}^N g_i(x)^{e_i}$ for g_i irreducible. Then

$$A/pA \simeq \bigoplus_{i=1}^N \mathbb{Z}/p[x]/g_i(x)^{e_i}.$$

It follows that $P_i = pA + g_i(\alpha)A$ is prime and $pA = \prod P_i^{e_i}$.

It is a fact that $\mathrm{ord}_{P_i}(\mathcal{D}) \geq e_i - 1$ (with equality if and only if $p \mid e_i$.) This implies that only finitely many p have $e_i > 1$, i.e. only finitely many primes ramify.

Example 2.1.1. Let $k = \mathbb{Q}(\sqrt{a})$ with $a \in \mathbb{Z}$ squarefree. Then

$$d = \begin{cases} a & \text{if } a \equiv 1 \pmod 4 \\ 4a & \text{if } a \equiv 2, 3 \pmod 4, \end{cases}$$

$$A = \mathbb{Z} + \mathbb{Z}(\tfrac{d+\sqrt{d}}{2}), \qquad \mathcal{D} = \sqrt{d}A$$

and

$$pA = \begin{cases} P_1P_2 & \text{if } f_1 = f_2 = 1 & d \equiv \square \pmod p \\ P & \text{if } f = 2 & \left(\frac{d}{p}\right) = -1 \\ P^2 & \text{if } e = 2 & p \mid d. \end{cases}$$

Using the full statement of quadratic reciprocity, there is a Dirichlet character $\chi : (\mathbb{Z}/d\mathbb{Z})^\times \to \{\pm 1\}$ such that p is split if and only if $\chi(p) = 1$ and p is inert if and only if $\chi(p) = -1$.

2.2. **Galois theory.** Assume that $k/\mathbb{Q}$ is Galois with group G. Then G acts transitively on $P_i \mid pA$, hence each P_i has the same e_p, f_p. Let G_P be the stabalizer of one of them. Then G_P acts on A/p. We denote the kernel of this action by I_P. Hence

$$1 \to I_P \to G_P \to \mathrm{Aut}(A/P) \to 1.$$

Since A/P is a field it is cyclic of order f_p. The inertia group I_P acts trivially on the residue field and has order e_p. Let $Fr \in \mathrm{Aut}(A/P)$ denote the map $x \mapsto x^p$, and $F_p = Fr^{-1}$.

Since for almost all p $e_p = 1$, $G_P \simeq \mathbb{Z}/f \cdot F_p$. The conjugacy class $[F_p]$ is independent of the choice of P because the Galois group acts transitively.

Let k be the splitting field of $\mathbb{Q}(\alpha) = \mathbb{Q}[x]/f(x)$ with $\deg f = n$. Then since G permutes the roots of f, $G \hookrightarrow S_n$. We look at the decomposition

$$f(x) \pmod p = \prod_{i=1}^N g_i(x), \qquad \deg g_i = f_i.$$

Then the cycle decomposition of $[F_p]$ is of type $(f_1)(f_2)\cdots(f_N)$.

2.3. **Artin's theory.** Artin decided to study homomorphisms $G \to \mathrm{GL}(V)$ where V is a complex vector space. Since $\#G$ is finite, the image must consist of semisimple element. In particular the conjugacy class $[F_p]$ is well-defined and one of its invariants is the characteristic polynomial which is encoded in

$$L(V,s) = \prod_{p \nmid d} \det(1 - [F_p]p^{-s} \mid V).$$

The nice thing about this is that if $V = \mathbb{C}$ is the trivial representation, then

$$L(\mathbb{C},s) = \prod_{p \nmid d} (1 - p^{-s})^{-1}$$

which is nearly the Riemann zeta function $\zeta(s)$.

To handle the $p \mid d$, we can define the local factor $L_p(V,s) = \det(1 - [F_p]q^{-s} \mid V^{I_p})^{-1}$. This definition works equally well for $p \nmid d$ since in that case I_p acts trivially, but it has the advantage that $[F_p]$ has a well-defined action on V^{I_p} (even though, in general, it does not on V.) With this definition $L(\mathbb{C},s) = \zeta(s)$.

As we have seen, to a quadratic extension k of $\mathbb{Q}$ there is a character $\chi : G \to \{\pm 1\}$ such that $\chi(p) = 1$ if and only if p splits, and $\chi(p) = -1$ if and only if p is inert. If $p \mid d$, $V^{I_p} = 0$, so there is no contribution from these terms in the L-function. Then

$$\begin{aligned} L(\mathbb{C}_\chi, s) &= \prod_p \begin{cases} (1-p^{-s})^{-1} & \text{if } p \text{ splits} \\ (1-p^{-s})^{-1} & \text{if } p \text{ is inert} \end{cases} \\ &= \prod_{p \nmid d} (1 - \chi(p)p^{-s})^{-1} = \sum_{n \geq 1} \chi_d(n) n^{-s} \end{aligned}$$

is a Dirichlet L-function.

Artin conjectured that $L(V,s)$ has a meromorphic continuation to $\mathbb{C}$ with poles if and only if $V^G \neq 0$.

These notions can be generalized to finite extensions K of any global field k. Now for $\mathfrak{p}$ a prime ideal in $A \subset k$, we have $\mathfrak{p}A_L = \prod P_i^{e_i}$ with all but finitely many $e_i = 0$. We can define $F_\mathfrak{p} \in G = \mathrm{Gal}(K/k)$ as the generator $x \mapsto x^{1/q}$ in the automorphism group of $(A_L/P)/(A/\mathfrak{p})$. (Note that $q = \mathbb{N}(\mathfrak{p})$.)

The Riemann zeta function satisfies the functional equation

$$\Lambda(s) = \zeta(s)\pi^{-s/2}\Gamma(s/2) = \Lambda(1-s),$$

and more generally, Hecke proved that if

$$\zeta_k(s) = \prod_{\mathfrak{p}} (1 - \mathbb{N}\mathfrak{p}^{-s})^{-1} \sum_{I \subset A} \mathbb{N}(I)^{-s}$$

then

$$\Lambda(s) = \zeta_k(s)(\pi^{-s/2}\Gamma(s/2))^{r_1}(\pi^{-s}\Gamma(s))^{r_2} = |d|^{1/2-s}\,\Lambda(1-s).$$

Artin conjectured that setting

$$L_v(V,s) = \begin{cases} (\pi^{-s/2}\Gamma(s/2))^{\dim V^+}(\pi^{-\frac{s+1}{2}}\Gamma(\frac{s+1}{2}))^{\dim V^-} & \text{if } v \text{ is real,} \\ ((2\pi)^{-s}\Gamma(s))^{\dim V} & \text{if } v \text{ is complex,} \end{cases}$$

the function

$$\Lambda(V,s) = L(V,s) \prod_{v \mid \infty} L_v(V,s)$$

should satisfy a functional equation of the form

$$\Lambda(V,s) = w(V)A(v)^{1/2-s}\Lambda(V^*, 1-s)$$

where V^* is the dual representation to V, $A(V) \geq 1$ is an integer and $w(V)w(V^*) = 1$. Brauer proved this.

Remark. There is a uniform way (given in Tate's thesis) of defining the local L-factors. The idea is to choose a nice function that is its own Fourier transform (for example, $e^{-\pi x^2}$ in the real case, and $char(\mathbb{Z}_p)$ in the case of $\mathbb{Q}_p$) and then integrate this.

The conductor

$$A(V) = |d|^{\dim V} \underbrace{\mathbb{N}(f(V))}_{\prod_p p^{\mathrm{ord}_p(f(V))}} .$$

The so-called *conductor of the representation* $f(V)$ satisfies $\mathrm{ord}_p(f(V)) \geq 1$ if and only if $I_{\mathfrak{p}}$ acts non-trivially on V which is equivalent to saying that $L(V,s)$ has degree strictly less than $\dim V$. In fact, $\mathrm{ord}_p(f(V)) \geq \dim(V/V^{I_p})$.

2.4. **Review of algebraic number theory: local theory.** If k is a global field, p a prime ideal of A, then for every prime p (or more generally, every valuation v) we can consider the *local field* k_p which is the completion of k with respect to the valuation given by p. This gives an injection $k \hookrightarrow k_p$ such that

$$A \hookrightarrow A_v = \{\alpha \in k_v \mid |\alpha|_p \leq 1\},$$

$$p \hookrightarrow p_v = \{\alpha \in k_v \mid |\alpha|_p < 1\}.$$

Then $A/p^n \simeq A_p/p^n$ which implies that $A_p = \varprojlim A/p^n$.

We now assume that k is local, with integers A and uniformizer p. (Since A is a DVR, hence a PID, we can chose p that generates the maximal ideal in k.) Let K be a finite extension of k. Write B and π for the integers and uniformizer, so $pB = \pi^e B$. Let $f = [B/\pi B : A/pA]$.

The Galois group G of K/k corresponds to G_p (the p decomposition group(?)) in the global Galois group. We want to define a sequence of groups

$$G \rhd G_0 \rhd G_1 \rhd \cdots \rhd G_n = 1$$

where G_0 corresponds to I_p. That is G_0 acts trvially on $B/\pi B$, so $G/G_0 \simeq \mathbb{Z}/f \cdot F$. Then G_1 corresponds to the (tame?) ramification and acts trivially on $B/\pi^2 B$. The gives the *lower ramification filtration.*

One can see that

$$\sigma \in G_i \iff \mathrm{ord}(\sigma b - b) \geq i+1 \text{ for all } b \in B.$$

If $\sigma \in G_0$ this description simplifies to $\sigma \in G_i$ if and only if $\mathrm{ord}(\sigma\pi - \pi) \geq i+1$.

Let $U_B = B^\times$ and $U_B^i = 1 + \pi^i B$. Then there is an injection

$$G_0/G_i \hookrightarrow U_B/U_B^i \simeq (B/\pi B)^\times.$$

Since $(B/\pi B)^\times$ is cyclic of order $q^f - 1$ (q is the order of A/pA), this implies in particular that G/G_0 has order prime to p.

For $i \geq$ we have

$$G_i/G_{i+1} \to U_B^i/U_B^{i+1} \qquad \sigma \mapsto \frac{\sigma\pi}{\pi} \simeq B/\pi B.$$

Note that $B/\pi B$ is a vector space over A/pA, so this implies that G_i/G_{i+1} is an elementary abelian p-group. The (wild inertia?) group P in the global case corresponds to G_1 and is therefore the Sylow p subgroup of I. So we have, for example,

$$G_0 \simeq G_1 \rtimes G_0/G_1.$$

Given a representation $G \to \mathrm{GL}(V)$ (which can be thought of as the restriction of a global representation to G_p), we may define

$$L_p(V,s) = \det(1 - Fq^{-s} \mid V^I)^{-1}.$$

Then

$$A(V) = \mathrm{ord}_p(f(V)) = \sum_{i \geq 0} \dim(V/V^{G_i}) \frac{\#G_i}{\#G_0}.$$

We will see next time that this is an integer.

3. October 4, 2011

3.1. **Why did Artin introduce his L-functions?** Recall: Given $(p) \subset \mathbb{Z} \subset \mathbb{Q}$, and a number field k of degree n extension of $\mathbb{Q}$ we can consider $pA = \prod P_i^{e_i}$ in the ring of integers A of k.

When k is a Galois extension, Artin considered representations $G = \mathrm{Gal}(k/\mathbb{Q}) \to \mathrm{GL}(V)$ for complex vector spaces V. In this case, all $e_i = e$ are the same, and $e \neq 1$ if and only if $p \mid d_k$. If $p \nmid d_k$, choose P to be any one of the primes P_i above p. Then the stabilizer of P in $G = \mathrm{Gal}(k/\mathbb{Q})$, G_P is a cyclic subgroup of order $f_p = f$ generated by F_P. (In general, if $I_P \lhd G_P$ is the inertia subgroup then $\langle F_P \rangle = G_P/I_P$.) The conjugacy class $[F_P]$ is independent of P, so we can define

$$L(V,s) = \prod_p \det(1 - F_P p^{-s} \mid V^{I_P})^{-1}$$

which converges if $\mathrm{Re}(s) > 1$.

Let Reg_G be the regular representation of G. On the one hand, F_p acts on G giving n/f orbits of size f. Let us assume that $p \nmid d_k$. Then each n-th root of unity is an eigenvalue of the action of F_p on Reg_G with multiplicity n/f. Hence

$$\prod_{p \nmid d_k} ((1 - p^{-f_p})^{n/f})^{-1} = \prod_{p \nmid d} \prod_{P \mid pA} (1 - \mathbb{N}P^{-s})^{-1}.$$

This works at the ramified places too, and so we get that $L(Reg_G, s) = \zeta_k(s)$, the zeta function of the field k.

On the other hand, it is easy to verify that $L(V \oplus W, s) = L(V,s)L(W,s)$. Since $Reg_G = \bigoplus (\dim V) V$ where the sum is taken over all irreducible V, we conclude that

$$L(Reg_G, s) = \prod_{V \text{ irred.}} L(V,s)^{\dim V}. \tag{3.1.1}$$

Putting these two interpretations together, we see that $\zeta(s)$ divides $\zeta_k(s)$. (The Reimann zeta function appears in the decomposition (3.1.1) in the form of the trivial representation.) Artin's conjecture then implies that $\zeta_k(s)/\zeta(s)$ is holomorphic. (This has been proved.)

If L over $\mathbb{Q}$ is *not* Galois, we let k be the Galois closure with G as above, and $H = \mathrm{Gal}(k/L)$. As outlined above, one can prove that $L(\mathrm{Ind}_H^G 1, s) = \zeta_L(s)$. (Note that $Reg_G = \mathrm{Ind}_1^G 1$, so this generalizes the above construction.) The basic trick is to realize that G_P orbits on G/H correspond to H orbits on $G_p\backslash G$. One sees that

$$L(\mathrm{Ind}_H^G 1, s) = \prod_{V \text{ irred.}} L(V,s)^{\dim V^H}.$$

This kind of factoring is the basis for much work in number theory today. For example, we have $|d_k| = \prod_v f(V)^{\dim V}$ and $|d_L| = \prod_v f(V)^{\dim V^H}$.

The class number formula gives the first term of the Taylor expansion of $\zeta_k(s)$ around $s = 0$:

$$\zeta_k(s) \sim s^{r_1+r_2+1}\left(\frac{-hR}{w}\right) + O(s^{r_1+r_2})$$

where h is the class number of k, R is the regulator, and w is the number of roots on unity in A. Similarly, one would like to get a good expression for each of the $L(V,s)$ which is the point of Stark's conjecture. (It says that $L(V,s) \sim s^{\dim V^{G_\infty} - \dim V^G}$ times some expression in terms of Stark units....)

Let us return to the situation of $L/\mathbb{Q}$ non-Galois and k the Galois closure. Let $n = [L : \mathbb{Q}]$. If G acts 2-transitively on n letters then $\mathrm{Ind}_H^G \mathbb{C} = \mathbb{C} \oplus V_{n-1}$ (V_{n-1} is a representation of dimension $n-1$) so

$$\zeta_L(s) = \zeta(s)L(V_{n-1}, s), \qquad \text{and} \qquad |d_L| = f(V_{n-1}).$$

[I DON'T QUITE GET WHAT'S GOING ON HERE. I GUESS THAT IT'S JUST GROUP THEORY.]

Recall that after multiplying $L(V,s)$ by the appropriate infinite factor $L_\infty(V,s)$ we have

$$\Lambda(V,s) = L(V,s)L_\infty(V,s) = \varepsilon(V,s)\Lambda(V^*, 1-s).$$

Here we are denoting $\varepsilon(V,s) = w(V)f(V)^{1/2-s}$ where $f(V) = \prod p^{a(V)}$ and $a(v) \geq 0$ depends on the action of interia: $a(V) > 0$ if and only if $V\mid_{I_P}$ is nontrivial. Recall that we have the series

$$G_P = D \rhd \underbrace{D_0}_{\text{inertia}} \rhd \underbrace{D_1}_{\text{wild inertia}} \rhd \cdots$$

where D_i acts trivially on $A/P^{i+1}A$. Then

$$a(V) = \sum_{i\geq 0} \dim(V/V^{D_i})\#\frac{D_i}{D_0} = \dim(V/V^I) + \underbrace{\sum_{i\geq 1} \dim(V/V^{D_i})\#\frac{D_i}{D_0}}_{b(V)}.$$

Then integer $a(V)$ is called the *Artin conductor* and $b(V)$ is the *Swan conductor*.

Theorem 3.1.1 (Artin)**.** *There exists a complex representation Art of D_0 such that $a(V) = \dim_{D_0}(V, Art)$. (Hence $a(V)$ is an integer.) The character of Art is given (for σ nontrivial) by $\chi(\sigma) = -i(\sigma)$ where $i(\sigma) = 1$ if $\sigma \in D_0 \setminus D_1$, $i(\sigma) = 2$ if $\sigma \in D_1 \setminus D_2$, and so on. $\chi(e) = -\sum_{\sigma\neq e}\chi(\sigma)$.*

It is easy to see that χ is a function on conjugacy classes, but Artin showed that it is integer valued, hence a character. Even though the character of *Art* is easy to describe the representation is not. It is not defined over $\mathbb{Q}$ or $\mathbb{R}$ (or $\mathbb{Q}_p$) but it is defined over $\mathbb{Q}_\ell$ if ℓ doesn't divide the residue characteristic.

3.2. **Some calculations.** Let $f(x) = x^4 - 2x + 2$ which has discriminant $2^4 \cdot 101$. Consider

$$\begin{tikzcd}
k \arrow[dd, dash, "G"] \arrow[dr, dash, "H"] & \\
& L = \mathbb{Q}_2[x]/f(x) \arrow[dl, dash] \\
\mathbb{Q}_2 &
\end{tikzcd}$$

where k is the splitting field of $f(x)$. Note that $[L : \mathbb{Q}_2] = 4$. Since $\mathrm{ord}_2(\mathrm{Disc}(f)) = 4$ we must have $4 \mid e$. Moreover, since 101 is not a square in $\mathbb{Q}_2$, $2 \mid f$. (By some analysis) it can be shown that G is either S_4 or D_8. Since (it can also be argued) $f = 2$, G is S_4 if $e = 12$ and $I = A_4$ and G is D_8 if $e = 4$ and $I = (2, 2)$.

We claim that

$$S_4 = D \rhd A_4 = I \rhd (2,2) = D_1 \rhd D_2 = ?. \tag{3.2.1}$$

To prove this consider $\mathrm{Ind}_H^G \mathbb{C}$. [I suppose G acts 2-transitively, so] we have the decomposition $\mathrm{Ind}_H^G \mathbb{C} = \mathbb{C} \oplus V_3$ and $a(V_3) = |d_L| = 4$. Suppose that

$$D = D_8 \rhd D_0 = D_1 = (2,2) \rhd D_2 \cdots .$$

Then, we calculate that

$$a(V) = 3 + 3 + \cdots .$$

But this contradicts $a(V) = 4$, so it is not possible.

On the other hand, assume that (3.2.1) holds. Then

$$a(V) = 3 + 3\frac{1}{3} + \cdots .$$

So, D_2 acts trivially on V. Since V is a faithful representation, this implies that $D_2 = 1$.

Another example: $f(x) = x^4 - 4x + 2$ for which $\mathrm{Disc}(f) = 2^8(-19)$. Here $e = 4$, $f = 2$, and by an analysis analogous to the above, it can be shown that you get the same D, D_0, D_1 as above *but* $D_2 \neq 1$. It turns out that $D_2 = D_3 = D_4 = D_5 = K_4$ and $D_6 = 1$.

The determinate of G on V_3 is the sign representation, so $V_3' = V_3 \otimes \mathrm{sgn}$ is an orthogonal representation of S_4 with trivial determinate. This gives a parameter

$$\mathrm{Gal}(k/\mathbb{Q}_2) \to \mathrm{SO}_3(\mathbb{C}) = \mathrm{SO}(V_3)$$

with $b(V) = 1$. We can say which representation of $\mathrm{SL}_2(\mathbb{Q}_p)$ this corresponds to. Consider

$$\chi : I = \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}_p) \mid b \in 2\mathbb{Z}_p \} \to \{\pm 1\}, \qquad \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto (-1)^{b+c} \pmod 2.$$

This is a character, and the representation $\mathrm{Ind}_I^{\mathrm{SL}_2(\mathbb{Q}_2)} \chi$ is a supercuspidal representation with a complicated parameter. In fact, it's the unique parameter with $b(V) = 1$.

3.3. **What about function fields?** We now let $k = F(x)$ and $q = \#F$, g the genus of a curve X. (eg. $k = F(t)$, $g = 0$.) Then we consider an extension K of k. The analogue of the quantity $|d_K|^{\dim V}\,\mathbb{N}(f(V))$ from the number field case is

$$q^{(2g-2)\dim V + \deg a(V)}, \qquad \deg a(V) = \sum_P a_P(V)P.$$

We have

$$\zeta_{F(t)}(s) = \underbrace{(1-q^{-s})^{-1}}_{\text{contribution from } \infty} \prod (1-q^{-(\deg f)x})^{-1}$$

where the product is taken over all irreducible monic polynomials $f(x)$. Using the fact that $F[t]$ is a UFD, we get

$$\begin{aligned}\zeta_{F(t)}(s) =& (1-q^{-s})^{-1}\sum_{n\geq 0}\underbrace{(\#\text{monic polyns of degree } d)}_{q^n} q^{-ns}\\ =& (1-q^{-s})^{-1}(1-q^{1-s})^{-1}.\end{aligned}$$

(In the number field case we don't have such huge cancellation like what occurs here where q shows up in every term.)

In the case of genus g one has

$$\zeta_{F(X)}(s) = \frac{P_{2g}(q^{-s})}{(1-q^{-s})(1-q^{1-s})}$$

where P_{2g} is polynomial of degree $2g$, and in the greatest generality $L(V,s)$ is a rational function in q^{-s} of degree $(2g-2)\dim V + \deg a(V)$.

Let k be a finite extension of $F(X)$ with Galois group J, and consider $F'(X)$ the field obtained by adjoining the constants of k to $F(X)$. If $V^J = 0$ then $L(V,s)$ is a polynomial of degree $(2g-2)\dim V + \deg a(V)$, so if the genus is 0, $\deg a(V) \geq 2\dim V$. If equality holds $L(V,s) = 1$. (So a nontrivial representation can lead to a trivial L-function!)

We finish with an example. Let $k = F(t)$ and $K = F(\sqrt{t})$ with the characteristic of F not 2. These are both genus 0 curves. We take V to be the nontrivial quadratic character of $G = J$. Then

$$L(V,s) = \frac{\zeta_K(s)}{\zeta_k(s)} = 1$$

so $a(V) = 2\dim V$. We aim to explain how this is possible. First, it implies that the inertia group is nontrivial for $t = 0, \infty$ (tame) and $a(V) = (0) + (\infty)$.

In the "normal" situation of function fields over $\mathbb{C}$, if G acts on $\mathbb{P}^1$, then $G \hookrightarrow \mathrm{PGL}_2(\mathbb{C})$ [as a very small subgroup], but in characteristic p, for $F = \mathbb{F}_q$ we have $G = \mathrm{PGL}_2(q)$.

We can describe the orbits of $\mathrm{PGL}_2(q)$ on $\mathbb{P}^1(\overline{F})$.

- $\mathrm{PGL}_2(q)$ acts on $\mathbb{P}^1(\mathbb{F}_q)$ with stabilizer $B = \{\left(\begin{smallmatrix} * & * \\ & * \end{smallmatrix}\right)\}$.
- $\mathrm{PGL}_2(q)$ acts on $\mathbb{P}^1(\mathbb{F}_{q^2}) \setminus \mathbb{P}^1(\mathbb{F}_q)$ with stabilizer T_{q+1}.
- $\mathrm{PGL}_2(q)$ acts on anything else freely, since $\frac{a\tau+b}{c\tau+d} = \tau$ implies that τ lives in a quadratic extension of $\mathbb{F}_q$. In particular (this can be checked just by counting), $\mathbb{P}^1(\mathbb{F}_{q^2}) \setminus \mathbb{P}^1(\mathbb{F}_q)$ consists of a single $\mathrm{PGL}_2(q)$ orbit.

Then we can define a map $\mathbb{P}^1 \to \mathbb{P}^1$ be designating the first orbit above map to ∞, the second to 0 and the last to 1. The corresponding lower ramification series are as follows.

For the prime at infinity:

$$G_0^\infty = B \rhd G_1^\infty = U \rhd \cdots$$

because $U = \{\left(\begin{smallmatrix} 1 & * \\ & 1 \end{smallmatrix}\right)\}$ is the p-Sylow subgroup of B. It will follow from the claim below that $G_2^\infty = 1$.

For the prime at 0:

$$G_0^{t=0} = N(T) \rhd T = G_1^{t=0} \rhd G_2^{t=0} = 1.$$

Claim: The L-function attached to any nontrivial representation of $\mathrm{PGL}_2(q)$ is 1. Moreover, the Artin conductor is

$$a(V) = \dim V/V^T + \dim V/V^B + \frac{1}{q-1}\dim V/V^U = 2\dim V.$$

(In particular, the higher terms are zero so $G_2 = 1$.)

This can be checked case by case, since the irreducible representations of G well understood. There are the discrete series representations which have dimension $q+1$, the representations of dimension q, Steinberg of dimension $q-1$ and the characters (of dimension 1). In the first case, the representations are formed by inducing characters on T and they aren't obtained by inducing from characters on B, so $\dim V^T = 1$ and $\dim V^B = 0$. It is true that[3] that $\dim V^U = 2$. Then

$$\dim V/V^T + \dim V/V^B + \frac{1}{q-1}\dim V/V^U = q + (q+1) + \frac{1}{q-1}(q+1-2) = 2(q+1) = 2\dim V.$$

The other cases can likewise be checked.

4. Tuesday October 11

4.1. Special values of Artin L-functions.

Euler discovered that

$$\zeta(2) = 1 + \frac{1}{4} + \frac{1}{9} + \cdots = \frac{\pi^2}{6},$$

$$\zeta(4) = 1 + \frac{1}{16} + \frac{1}{81} + \cdots = \frac{\pi^4}{90},$$

and that $\zeta(2n) = \pi^{2n} r$ where $r \in \mathbb{Q}$.

Using the functional equation

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \pi^{(s-1)/2}\Gamma(\frac{1-s}{2})\zeta(1-s)$$

these results imply that

$$\zeta(-1) = \frac{1}{2}, \quad \zeta(-3) = \frac{1}{240}, \quad \zeta(-5) = \frac{-1}{252}, \quad \cdots \quad \zeta(-11) = \frac{691}{32760}, \quad \cdots$$

Actually, Euler argued that these were the correct values for $\zeta(1-2n)$ and from this deduced the functional equation. (We will see his proof later.)

Note that for $d \gg 0$ even $\zeta(d) = 1 + \frac{1}{2^d} + \frac{1}{3^d} + \cdots \approx 1$, so $\zeta(1-d) \approx \frac{2(d-1)!}{(2\pi i)^d} \in \mathbb{R}$ is very large. On the other hand if $d \geq 3$ is odd, then $\zeta(1-d) = 0$. Euler proved that $2^d(2^d-1)\zeta(1-d) \in \mathbb{Z}$. (We will see his proof later.)

[3] I don't know why this is.

4.1.1. *Number field case.* The value of $\zeta_K(0)$ can be studied by looking at the class number formula:

$$\zeta(s) \sim s^{r_1+r_2-1}\left(\frac{-hR}{w}\right) + s^{r_1+r_2} + \cdots .$$

For example, if $k = \mathbb{Q}$ then $r_1 = 1$, $r_2 = 0$, $h = R = 1$ and $w = 2$, so $\zeta(0) = \frac{-1}{2}$.

If $k = \mathbb{Q}(\sqrt{d})$ and $d > 0$, then $r_1 = 2$ and $r_2 = 0$ so $\zeta_k(0) = 0$. If $d < 0$, $r_1 = 0$ and $r_2 = 1$ so $\zeta_k(0) = \frac{-h(d)}{w(d)}$. (The regulator is trivial (apparently) in this case.) Since $\zeta_k(s) = \zeta(s)L(\chi_d, s)$ this implies that

$$L(\chi_d, 0) = \begin{cases} \frac{2\mathfrak{h}(d)}{w(d)} & \text{if } d < 0 \\ 0 & \text{if } d > 0. \end{cases}$$

Usually, $w(d) = 2$. [I think this is true except for $d = -1, -3$.] In that case $L(\chi_d, 0) = h(d)$.

Conjecture 4.1.1. $c\frac{|d|^{1/2}}{\log|d|} < h(d) < 2\,|d|^{1/2}\log|d|$.

If you want to tr prove this conjecture using the functional equation you have to understand $\sum_{n\geq 1}\frac{\chi(n)}{n}$ which is a conditionally convergent series. If this is close to 1, the conjecture would follow. But, if there is a Siegel zero then this series can't be controlled.

Let K/k be an extension of number fields with $G = \mathrm{Gal}(K/k) \to \mathrm{GL}(V)$. We can write

$$\Lambda(V, s) = \prod_{\text{all places } v} L_v(V, s) = \varepsilon(V, s)\Lambda(V^*, 1-s).$$

In the domain of convergence ($\mathrm{Re}(s) > 1$) $L_v(V, s) \neq 0$ so $\Lambda(V, s) \neq 0$. Therefore, the functional equation implies that $\Lambda(V, s)$ is nonzero if $s < 0$ and has a pole at $s = 0, 1$ of order $\dim V^G$. Artin conjectured that

- $\Lambda(V, s)$ is regular at all $s \neq 0, 1$,
- $\Lambda(V, s)$ vanishes only for $\mathrm{Re}(s) = \frac{1}{2}$.

We remark that just proving that $\Lambda(V, s) \neq 0$ for $\mathrm{Re}(s) = 1$ (or $\mathrm{Re}(s) = 0$) is very hard.

4.1.2. *Function field case.* Now let k be a function field. For function fields there are not infinite primes. So if V is the trivial representation we have

$$\Lambda(V, s) = \zeta_k(s) = \frac{P_{2g}(q^{-s})}{(1-q^{-s})(1-q^{1-s})}$$

so there are obviously poles at $s = 0, 1$.

Note that $s \mapsto \frac{2\pi i}{\log q}$ fixes Λ so one should consider as domain of $\zeta_k(s)$ the Riemann surface obtained by looking at $0 \leq \mathrm{Im}(s) < \frac{2\pi i}{\log q}$. Then the fact that the zeros of $P_{2g}(q^{-s})$ lie on strip $\mathrm{Re}(s) = \frac{1}{2}$ is equivalent to saying that its roots have absolute value $q^{1/2}$.

4.2. **How not to prove the Riemann hypothesis.** Let $k = \mathbb{Q}(\sqrt{d})$ for some $d < 0$ and $h(d) > 1$. Then for $\mathrm{Re}(s) > 0$ we can write

$$\begin{aligned} 2\pi^{-s}\Gamma(s)\zeta_k(s) =& 2\pi^{-s}\Gamma(s)\sum_{I\subset A}\frac{1}{(NI)^s} \\ =& 2\pi^{-s}\Gamma(s)\sum_{c\in h(d)}\underbrace{\left(\sum_{I\subset A, Cl(I)=c}\frac{1}{(NI)^s}\right)}_{\zeta_c(s)} \end{aligned}$$

The so-called *Epstein ζ-functions*, $\zeta_c(s)$, were studied by Dirichlet who showed that they satisfy

$$\zeta_c(s) = \sum_{(n,m)\neq(0,0)}\frac{1}{(am^2+bmn+cn^2)^s}$$

where $I \leftrightarrow ax^2 + bxy + cy^2$.

There is a functional equation

$$(2\pi)^{-s}\Gamma(s)\zeta_c(s) = (2\pi)^{s-1}\Gamma(1-s)\zeta_{c^{-1}}(s)$$

but this is not helpful because the Epstein ζ-functions do not satisfy the Riemann hypothesis, (they have zeros in $\mathrm{Re}(s) > 1$ and the don't have Euler products.)

4.3. **Back to special values.** So $\Lambda(V,s)$ has poles at $s = 0, 1$ of order $\dim V^G$. Let S be a nonempty finite set of places containing all $v \mid \infty$. Then set

$$L_S(V,s) = \prod_{v\notin S}L_v(V,s) = \Lambda(V,s)\cdot\underbrace{\prod_{v\in S}L_v(V,s)^{-1}}_{\text{This has a zero at } s=0 \text{ of order } \dim V^{G_v}}.$$

Since

$$L_v(V,s)^{-1} = \begin{cases} \det(1-F_p(Np)^{-s}|V^{I_p}) & \text{if } v \text{ is finite} \\ (2\pi)^s\Gamma(s)^{-1} & \text{if } v \text{ is complex} \\ (\quad\cdots\quad)^{-1} & \text{if } v \text{ is real,} \end{cases}$$

this implies that $L_S(V,s)$ is regular at $s = 0$.

For example, if k is the function field of a curve then

$$L_v(V,s) = \frac{P_{2g}(q^{-s})}{(1-q^{-s})(1-q^{1-s})}(1-q^{-ds})$$

where d is the degree of v. This clearly is regular at $s = 0$.

The following theorem is due to Weil for function fields and Siegel-Brauer for number fields.

Theorem 4.3.1. *For all $d \geq 1$, the values of $L_S(V, 1-d)$ are algebraic numbers and for all automorphisms σ of $\mathbb{C}$, $L_S(V,1-d)^\sigma = L_S(V^\sigma, 1-d)$. In particular, if V is defined over $\mathbb{Q}$ then $L_S(V, 1-d) \in \mathbb{Q}$.*

Siegel's proof of this is really ingenious. We already know $\zeta(1-d)$ is rational for odd d, so let us assume d is even. Then let

$$E = \frac{1}{2}\zeta(1-d) + \sum_{n\geq 0}\underbrace{\left(\sum_{a|n}a^{d-1}\right)}_{\in\mathbb{Z}}q^n$$

be the weight d Eisenstein series. Since the nonconstant Fourier coefficients are integers,

$$2(E - E^\sigma) = \zeta(1-d) - \zeta(1-d)^\sigma. \tag{4.3.1}$$

If f is a weight d modular form then f^σ is also a weight d modular form. (This is because the space of such forms has a basis whose Fourier coefficients are rational.) Using a weight argument this implies that (4.3.1) is 0.

Remark: Almost all $L(V, 1-d)$ are zero. Indeed, if $d \geq 2$ and k has a complex place then, since

$$\underbrace{((2\pi)^{-s}\Gamma(s))^{\dim V} L(V,s)}_{\neq 0 \text{ at } s=d} = \underbrace{((2\pi)^{s-1}\Gamma(1-s))^{\dim V}}_{\text{has a pole } s=d} L(V, 1-s),$$

$L(V, 1-d) = 0$. A similar argument can be used to prove the following.

Theorem 4.3.2. *If k a number field, $d \geq 2$ and $L_S(V, 1-d) \neq 0$, then*

(a) *k is totally real, and*
(b) *for all real places v, $V = V^+$ if d is odd, and $V = V^-$ if d is even.*

Note that (b) implies that if d is even that $\zeta_k(1-d) \neq 0$, and if d is odd then $L(\chi_d, 1-d) \neq 0$.

To get the integral values, we need to kill the pole at $s = 1$. To do this let T be a nonempty finite set of places disjoint from S. Define

$$L_{S,T}(V,s) = \underbrace{L_S(V,s)}_{\text{pole of order } \dim V^G \text{ at } s=1} \prod_{v \in T} \underbrace{(\det(1 - F_p(Np)^{1-s} | V^{I_p})}_{\text{zero of order } \dim V^{G_p} \text{ at } s=1}.$$

Now this is regular at both $s = 1$ and $s = 0$.

For example, consider $k = \mathbb{Q}$, $V = \mathbb{C}$, $S = \{\infty\}$ and $T = \{2\}$. Then

$$\begin{aligned} L_{S,T}(V,s) =& \zeta(s)(1-2^{1-s}) \\ =& \sum_{n \geq 1} \frac{1}{n^s} - 2\sum_{n\geq 1} \frac{1}{(2n)^s} \\ =& \sum_{n\geq 1} \frac{(-1)^{n+1}}{n^s} = \zeta^*(s). \end{aligned}$$

So $\zeta^*(1) = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots = \log 2$.

Even though $\zeta^*(0) = 1 - 1 + 1 - 1 + \cdots$ doesn't converge, Euler realized that formally

$$\zeta^*(0) = (1 - x + x^2 - x^3 + \cdots)|_{x=1} = \left.\frac{1}{1+x}\right|_{x=1} = \frac{1}{2}.$$

Similarly, $\zeta^*(-1) = 1 - 2 + 3 - 4 + \cdots$ doesn't converge, but

$$\begin{aligned} \zeta^*(-1) =& (1 - 2x + 3x^2 - 4x^3 + \cdots)|_{x=1} \\ =& \left.\left(\frac{d}{dx}(x - x^2 + x^3 - x^4 + \cdots)\right)\right|_{x=1} \\ =& \left.\frac{d}{dx}\left(\frac{x}{1+x}\right)\right|_{x=1} \\ =& \left.\frac{1}{(1+x)^2}\right|_{x=1} = \frac{1}{4} \end{aligned}$$

In this fashion Euler proved that $\zeta^*(1-d) \in \mathbb{Z}[\frac{1}{2^d}]$, and from this he was able to discover the functional equation.

Theorem 4.3.3 (Weil)**.** *For a function field k, if V is defined over $\mathbb{Q}$ then $L_{S,T}(V, 1-d) \in \mathbb{Z}$ for all $d \geq 1$. (If V is defined over a cyclotomic field $\mathbb{Q}(\zeta_n)$ then the L-value is in $\mathbb{Z}[\zeta_n]$.)*

This is clear for our example of the ζ-function of a curve: for $S = \{v\}$ and $T = \{w\}$, and $d = \deg v$ and $d' = \deg w$, we have

$$\frac{P_{2g}(q^{-s})}{(1-q^{-s})(1-q^{1-s})}(1-q^{-ds})(1-q^{d'(1-s)}) \tag{4.3.2}$$

which when evaluated at $s = 1-d$ will obviously be an integer.

The analogue in the case of k a number field was proven by Deligne-Ribet and Cassau-Nojves. When V is defined over $\mathbb{Q}$ it says that $L_{S,T}(V, 1-d) \in \mathbb{Z}[\frac{1}{p}]$ where p is the characteristic of $v \in T$. In particular, if T contains two primes of different characteristic then $L_{S,T}(V, 1-d) \in \mathbb{Z}$.

Returning to the function field case, for $X = \mathbb{P}^1$ and $S = \{\infty\}$, $T = \{0\}$ of degree 1, (4.3.2) gives $L_{S,T}(\mathbb{C}, s) = 1$. Hence $\zeta_{S,T}(1-d) = 1$.

4.4. **Galois representations not over $\mathbb{C}$.** It turns out that the really interesting representations of $\mathrm{Gal}(k^s/k) = \varprojlim \mathrm{Gal}(K/k)$ are those which might not factor through a finite quotient. In order for this to be the case (and for the representation to be continuous), the representation must be "ℓ-adic."

For example, if n is not divisible by the characteristic of k we can consider the extension of k by μ_n: $\mathrm{Gal}(k(\mu_n)/k) \hookrightarrow (\mathbb{Z}/nZ)^\times$. Taking $n = \ell^m$ for $m = 1, 2, 3, \ldots$, we get a tower of fields:

$$k \subset k(\mu_n) \subset k(\mu_{n^2}) \subset \cdots,$$

and an action of $\mathrm{Gal}(k^s/k)$ on

$$\varprojlim \mu_{\ell^n}(k^s) = \mathbb{Z}_\ell \mathbb{G}_m \simeq \mathbb{Z}_\ell.$$

In other words, we get a continuous $\varphi : \mathrm{Gal}(k^s/k) \to \mathbb{Z}_\ell^\times$ which is usually infinite.

If ℓ is coprime to p, the residue characteristic of k, then one gets the same eigenvalue of Frobenius, independent of ℓ. This is because $Frob(\alpha) \equiv \alpha^q \pmod{p}$, which implies that on a root of unity $Frob(\zeta) = \zeta^q$.

5. Tuesday October 18

We now review the classification of reductive groups (which has a long history.) We begin by assuming that k is algebraically closed.

An affine algebraic group is a variety G with multiplication and inverse morphisms that give it the structure of a group. For example, $\mathrm{GL}(V)$ which when $\dim V = n$ is often denoted GL_n. Every element $g \in \mathrm{GL}(V)$ can be written as su, in canonical way, such that s is semisimple and u is unipotent. Every affine algebraic group can be embedded in $\mathrm{GL}(V)$ as a closed subgroup, and the decomposition $g = su$ is so canonical that if $g \in G$ then $s, u \in G$ as well.

5.1. **Reductive groups.** The category of affine algebraic groups is a little too large for us. We will restrict ourselves to *reductive groups* which are affine algebraic groups that are connected and for which the unipotent radical $R_u(G)$ (which is always a normal subgroup of G) is trivial. This is equivalent to saying that there exists a faithful semisimple representation $G \hookrightarrow \mathrm{GL}(V)$.

$\mathrm{GL}(V)$ is reductive. $G = \left(\begin{smallmatrix} a & b \\ & d \end{smallmatrix}\right) \subset \mathrm{GL}_2$ is not reductive: $R_u(G) = \left(\begin{smallmatrix} 1 & b \\ & 1 \end{smallmatrix}\right)$.

Additional examples of reductive groups: $\mathbb{G}_m = \mathrm{GL}_1$. If $\langle \cdot, \cdot \rangle : V \times V \to k$ is a alternating linear form then $\mathrm{Sp}(V, \langle \cdot, \cdot \rangle)$ is the subgroup of $\mathrm{GL}(V)$ which preserve the form. For $\dim V = 1$, $\mathrm{Sp}(V, \langle \cdot, \cdot \rangle) = \mathrm{SL}_2$. If the form is symmetric then the analagous group $O(V)$ is not reductive, but its connected component $\mathrm{SO}(V)$ is reductive.

5.2. **Tori.** A commutative reductive group is called a *torus*. One example of a torus is

$$T = \underbrace{\mathbb{G}_m \times \cdots \times \mathbb{G}_m}_{n\text{-times}} = (\mathbb{G}_m)^n.$$

In fact, up to isomorphism, all tori are of this type. Associated to a torus T is the character group $M = \mathrm{Hom}(T, \mathbb{G}_m)$ and $M^\vee = \mathrm{Hom}(\mathbb{G}_m, T)$. Both of these are free abelian groups, and there are in duality via $\mathrm{Hom}(\mathbb{G}_m, \mathbb{G}_m) \simeq \mathbb{Z}$. (If $\varphi \in \mathrm{Hom}(\mathbb{G}_m, \mathbb{G}_m)$ then $\varphi(\lambda) = \lambda^k$ for some $k \in \mathbb{Z}$.)

Every representation V of T is semisimple. This means that $V = \bigoplus_{\alpha M} m(\alpha)\chi_\alpha$ where $\chi_\alpha(t) = t^\alpha$. (We write M additively, so that $\chi_\alpha \chi_\beta = \chi_{\alpha+\beta}$.)

Theorem 5.2.1. *Let G be a reductive group. Then*

(a) *all maximal tori are conjugate, and*
(b) $Z_G(T) = T \lhd N_G(T)$.

From (b) we get $W(T, G)$ which is the quotient of $N_G(T)$ by T.

5.3. **Roots.** G acts on $Lie(G) = \mathfrak{g} = \ker(G(k[\epsilon]) \to G(k))$. (Here $k[\epsilon] = k[x]/(x^2)$.) $\dim \mathfrak{g} = \dim G$.

Restricting this action to a maximal torus T, we get a decomposition

$$\mathfrak{g} = Lie(T) \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{g}_\alpha$$

where $\Phi \subset M \setminus \{0\}$ and $\mathfrak{g}_\alpha = \{X \in \mathfrak{g} \mid tX = \alpha(t)X\}$. The elements in Φ are called roots. The set Φ is stable under $\alpha \mapsto -\alpha$ and $\dim \mathfrak{g}_\alpha = 1$.

The roots for $\mathrm{GL}(V)$: Writing $V = kv_1 \oplus kv_2 \oplus \cdots \oplus kv_n$ gives

$$T = \begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix},$$

$$M = \bigoplus \mathbb{Z} e_i, \qquad e_i(t) = \lambda_i,$$

$$M^\vee = \bigoplus \mathbb{Z} e_i^\vee, \qquad e_i^\vee(\lambda) = diag(1, \ldots, 1, \overbrace{\lambda}^{i\text{-th entry}}, 1, \ldots, 1).$$

The normalizer of T in G, $N_G(T)$ consists of all monomial matrices, i.e. those for which each row and column contains exactly one nonzero entry. Thus, $W(G, T) = N_G(T)/T = S_n$ consists of permutation matrices. The Lie algebra of $\mathrm{GL}(V)$ is

$\mathfrak{gl}(V) = \mathrm{End}(V)$. The action of T on $\mathfrak{g}$ is by conjugation, so if $E_{ij} \in \mathfrak{g}$ is the element with every entry zero except the entry in the i-th row and j-column is 1, it follows that $t \cdot E_{ij}(1) = \lambda_i/\lambda_j E_{ij}$. So $\mathfrak{g}_{e_i - e_j} = kE_{ij}$.

The roots of SL_2.

$$T = \begin{pmatrix} \lambda & \\ & \lambda^{-1} \end{pmatrix} \to \mathbb{G}_m \qquad \text{via } \lambda,$$

$$\mathfrak{g}_\alpha = kE = \begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix} 0, \qquad \mathfrak{g}_\alpha = kF = \begin{pmatrix} 0 & 0 \\ 0 & * \end{pmatrix} 0.$$

Thus, $t^\alpha = \lambda^2$ and $t^\beta = t^{-\alpha} = \lambda^{-2}$, and

$$M \simeq \mathbb{Z}, \qquad \Phi = \{2, -2\}, \qquad Lie(T) = kH = \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}.$$

Note that in characteristic 2 $Lie(T)$ is central, so we get

$$\begin{tikzcd} 0 \arrow[r] & kH \arrow[r] & \mathfrak{sl}_2 \arrow[r] \arrow[d] & kF \oplus kE \arrow[r] & 0 \\ & \text{2-diml} \arrow[r] & \mathfrak{pgl}_2 \arrow[r] & \text{1-diml} & \end{tikzcd}$$

[I don't know what he's saying here.]

Remark: $\mathfrak{g} \simeq \mathfrak{g}^*$ via $\langle A, B \rangle = \mathrm{tr}(AB)$.

5.4. **Coroots.**

Proposition 5.4.1. *Fix a maximal torus $T \hookrightarrow G$ and a root $\alpha \in \Phi$. Then there exists a morphism $\varphi : \mathrm{SL}_2 \to G$ unique up to conjugacy by T such that $\begin{pmatrix} \lambda & \\ & \lambda^{-1} \end{pmatrix} \to T$, $\begin{pmatrix} 1 & * \\ & 1 \end{pmatrix} \to U_\alpha$ with Lie algebra $\mathfrak{g}_\alpha$ and $\begin{pmatrix} 1 & \\ * & 1 \end{pmatrix} \to U_{-\alpha}$ with Lie algebra $\mathfrak{g}_{-\alpha}$. Furthermore, for $x \in k^\times$, the element $n(x) = \begin{pmatrix} & x \\ -1/x & \end{pmatrix} \in N_{\mathrm{SL}_2}\begin{pmatrix} \lambda & \\ & \lambda^{-1} \end{pmatrix}$ (with $n(x)^2 = \begin{pmatrix} -1 & \\ & -1 \end{pmatrix}$) satisfies $\varphi(n(x)) \in N_G(T)$, and $n(x)^2$ the image of $\begin{pmatrix} -1 & \\ & -1 \end{pmatrix}$ in T.*

Define $\alpha^\vee \in M^\vee$, the coroot associated to α, by $\alpha^\vee : \mathbb{G}_m \simeq \begin{pmatrix} \lambda & \\ & \lambda^{-1} \end{pmatrix} \to T$. By our identifications, $\langle \alpha, \alpha^\vee \rangle = 2$.

Note that $n_\alpha(x)^2 = \alpha^\vee(-1)$. Can define $H_\alpha = Lie(\alpha^\vee)(1)$ and $Lie(\alpha^\vee) : \mathbb{G}_a \to Lie(T)$. Then

$$[E_\alpha, F_\alpha] = H_\alpha, \qquad [H_\alpha, E_\alpha] = 2E_\alpha, \qquad [H_\alpha, F_\alpha] = -2F_\alpha.$$

How to construct $\mathrm{SL}_2 \to G$. Let T_α be the connected component of the kernel of $\alpha : T \to \mathbb{G}_m$. Then $\dim T_\alpha = \dim T - 1$, and $Z(T_\alpha)$ is reductive, and the derived subgroup $\mathcal{D}(Z(T_\alpha))$ is semisimple and isomorphic to either SL_2 or PGL_2.

For example, if $G = \mathrm{GL}(V)$ and $\alpha = e_1 - e_2$ then $\alpha(t) = \lambda_1/\lambda_2$ so

$$T_\alpha = \begin{pmatrix} \lambda & & & \\ & \lambda & & \\ & & \lambda_3 & & \\ & & & \ddots & \\ & & & & \lambda_n \end{pmatrix}, Z(T_\alpha) = \left(\begin{array}{c|ccc} \mathrm{GL}_2 & & & \\ \hline & \lambda_3 & & \\ & & \ddots & \\ & & & \lambda_n \end{array}\right), \mathcal{D}(Z(T_\alpha)) = \left(\begin{array}{c|ccc} \mathrm{SL}_2 & & & \\ \hline & 1 & & \\ & & \ddots & \\ & & & 1 \end{array}\right).$$

5.5. **(reduced) Root datum.**

A (reduced) root datum is a (M, Φ, M^v, Φ^v) where $M, M^\vee$ are finitely generated free abelian groups in duality, $0 \notin \Phi \subset M$, $0 \notin \Phi^\vee \subset M^\vee$ such that

(1) There is a bijection between Φ and $\Phi^\vee$ $\alpha \leftrightarrow \alpha^\vee$ such that $\langle \alpha, \alpha^\vee \rangle = 2$.
(2) If $\alpha \in \Phi$ then the only integral multiples $m\alpha \in \Phi$ are $m = \pm 1$.
(3) $s_\alpha(\Phi) = \Phi$ for all α (and similarly for $\Phi^\vee$.)

Here $s_\alpha : M \to M$ is the reflection $m \mapsto m - \langle m, \alpha^\vee \rangle \alpha$. By 1, it is a simple reflection such that $s_\alpha(\alpha) = -\alpha$ and s_α fixes the hyperplane perpendicular to $\alpha^\vee$. ($s_{\alpha^\vee} : M^\vee \to M^\vee$ is defined in the same way.)

This structure is very restrictive. For example, given two (linearly independent) roots α, β there are only four possibilities for $\mathbb{Z}\alpha + \mathbb{Z}\beta \cap \Phi$: A_1^2, A_2, B_2, G_2.

We illustrate this for $\mathrm{GL}(V)$. Let $T_{\alpha,\beta}$ be the intersection of T_α and T_β, hence it has codimension 2 in T. Let $\alpha = e_1 - e_2$ and $\beta = e_2 - e_3$. Then $T_{\alpha,\beta} = diag(\lambda, \lambda, \lambda, \lambda_4, \dots, \lambda_n)$ and

$$Z(T_{\alpha,\beta}) = \left(\begin{array}{c|ccc} \mathrm{GL}_3 & & & \\ \hline & \lambda_4 & & \\ & & \ddots & \\ & & & \lambda_n \end{array}\right), \mathcal{D}(Z(T_{\alpha,\beta})) = \left(\begin{array}{c|ccc} \mathrm{SL}_3 & & & \\ \hline & 1 & & \\ & & \ddots & \\ & & & 1 \end{array}\right).$$

This is an example of A_2. Notice that in this case $\langle \alpha, \beta^\vee \rangle = -1$.

Now take $\alpha = e_1 - e_2$ and $\beta = e_3 - e_4$. In this case $\mathcal{D}(Z(T_{\alpha,\beta}))$ has two SL_2 blocks. This is an example of A_1^2.

In general, $\langle \alpha, \beta^\vee \rangle \in \{0, \pm 1, \pm 2, \pm 3\}$.

Theorem 5.5.1. *The root datum $(M, \Phi, M^\vee, \Phi^\vee)$ of G determines the group up to isomorphism. For any choice of root datum there is a reductive group G over k giving rise to it.*

Note that this has nothing to do with the characteristic of k. (In SGA(III) Grothendieck proved that this can all be done scheme theoretically over $\mathbb{Z}$.)

Denoting the root datum attached to G by M_G and $T \subset G$ a maximal torus, there is a surjection

$$Isom_k((T, G), (T', G')) \to Isom(M_G, M_{G'})$$

but this is not an isomorphism. For example, if $G = G' = \mathrm{SL}_2$, $\mathrm{Aut}(M_G) = \mathbb{Z}/2$ but $\mathrm{Aut}((T, G)) = N_G(T)$. We would like to improve the above theorem by specifying the automorphisms of G. This is called a *pinning*. We will discuss it next time.

Some natural questions:

- When does the root datum correspond to a torus? It turns out that G is a torus if and only if $\Phi = \emptyset$. In this case $\mathrm{Aut}(G) = \mathrm{Aut}(M) \simeq \mathrm{GL}_n(\mathbb{Z})$.
- When is G semisimple? This happens if and only if $\mathbb{Z}\Phi \subset M$ has finite index. Moreover, the position of M in relation to $\mathbb{Z}\Phi \subset M \subset (\mathbb{Z}\phi^\vee)^*$ determines G within its isogeny class.

As an example, when G is rank 1, $\mathbb{Z}\Phi \subset (\mathbb{Z}\Phi^\vee)^*$ has degree two. $M = \mathbb{Z}\phi$ corresponds to $G = \mathrm{PGL}_2$, and $M = (\mathbb{Z}\Phi^\vee)^*$ corresponds to $G = \mathrm{SL}_2$.

More generally, if $M = \mathbb{Z}\Phi$ then G is adjoint, i.e. $Z(G) = 1$. (Care has to be taken by what $Z(G) = 1$ means because it must be interpreted in a scheme theoretic sense.)

Another question: When is the inclusion $\mathbb{Z}\Phi \hookrightarrow M$ (or $\mathbb{Z}\Phi^\vee \hookrightarrow M^\vee$) split? The answer is that it splits if $Z(G)$ is connected (or if $\mathcal{D}(Z(G))$ is simply connected).

We finish by remarking that if G has root datum $(M, \Phi, M^\vee, \Phi^\vee)$ the Langlands dual group is the group with root datum $(M^\vee, \Phi^\vee, M, \Phi)$.

6. Tuesday October 25

Last time we considered a maximal torus T of a reductive group G, and defined the roots $\Phi \subset \mathrm{Hom}(T, \mathbb{G}_m)$ and coroots $\Phi^\vee \subset M^\vee = \mathrm{Hom}(\mathbb{G}_m, T)$. The roots (and analogously the coroots) give automorphisms

$$s(\alpha, \alpha^\vee) : M \to M \qquad m \mapsto m - \langle m, \alpha^\vee \rangle \alpha$$

which preserve the set of roots. i.e. $s_\alpha(\Phi) = \Phi$ for all $\alpha \in \Phi$. We also identified elements $n_\alpha(x) \in N_G(T)$ which map to $s_\alpha = s(\alpha, \alpha^\vee)$ on M. The root datum $R = (M, \Phi, M^\vee, \Phi^\vee)$ determines G up to isomorphism.

Today we will play with root data, and begin to understand $\mathrm{Aut}(R)$.

Clearly, $\mathrm{Aut}(R) \hookrightarrow \mathrm{Aut}(M) \simeq \mathrm{GL}_n(\mathbb{Z})$. There is also a map $\mathrm{Aut}(R) \to \mathrm{Aut}(\Phi)$. We know that $W = \langle s_\alpha \rangle_{\alpha \in \Phi} \subset \mathrm{Aut}(R)$. This is the image of $n_\alpha(x)$ in $N_G(T)/T = W(T, G)$. In fact, $W \simeq W(G, T)$.

Example: $G = \mathrm{GL}_n$. As we have seen, $M = \oplus \mathbb{Z} e_i$. Then $\Phi = \{e_i - e_j \mid i \neq j\}$, and for $\alpha = e_i - e_j$, $s_\alpha(e_1 - e_2) = e_2 - e_1$, $s_\alpha(e_k) = e_k$ for $k = 3, \cdots, n$ and $s_\alpha(e_1 + e_2) = e_1 + e_2$. As an element of $\mathrm{Aut}(M)$,

$$s_\alpha = \left(\begin{array}{c|ccc} \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) & & & \\ \hline & 1 & & \\ & & \ddots & \\ & & & 1 \end{array}\right)$$

In general $s_{e_i - e_j} = (ij)$. So $W = \langle (ij) \rangle = S_n \simeq W(G, T)$. Note that the generators form a single conjugacy class in W. In this example, $-1 \in \mathrm{Aut}(R)$ but $-1 \notin W$. Exercise: show that $\mathrm{Aut}(R) = S_n \times \langle -1 \rangle$.

Example R of type G_2: $M = \mathbb{Z}[\zeta_3] \subset \mathbb{Q}(\sqrt{-3})$, $M^\vee = \frac{1}{\sqrt{-3}} M = \mathcal{D}^{-1}$. The pairing is given by $\langle x, y \rangle = \mathrm{tr}(x\bar{y})$. (So if $x \in M \cap M^\vee$, $\langle x, x \rangle = \mathrm{tr}(x\bar{x}) = 2Nm(x) \in 2\mathbb{Z}$.) $\Phi \subset M$ consists of the norm 1 and norm 3 elements, and $\Phi^\vee \subset M^\vee$ consists of norm $\frac{1}{3}$ and norm 1 elements. The element $1 = \alpha = \alpha^\vee$. In this case $W = \langle s_\alpha \rangle = D_{12} \rhd C_6$ and the generators form 2 conjugacy classes: one for the short roots and one for the long roots. Moreover $-1 \in \Phi$. In fact, $W = \mathrm{Aut}(R)$.

There is, by the general classification, a group G_2 which corresponds to this datum, but there is no good way to describe it except in one way or another by generators and relations. (Either one describes it directly using a "Chevalley basis" or if it is described as the automorphism group of the octonians, then one needs to give generators and relations for the octonians.)

A Borel subgroup $B \subset G$ is a maximal connected solvable subgroup. It is well-defined up to conjugacy, and satisfies $N_G(B) = B$. Recall that the roots are defined via the action of T on

$$Lie(G) = Lie(T) \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{g}_\alpha.$$

The choice of Borel B gives

$$Lie(B) = Lie(T) \oplus \underbrace{\bigoplus_{\alpha \in \Phi^+(B,G)} \mathfrak{g}_\alpha}_{Lie(U)}$$

where $U \subset B$ is the nilradical of B (Borel subgroups are *not* reductive) and $\Phi^+ = \Phi^+(B, G) \subset \Phi$ satisfies $\Phi = \Phi^+ \cup (-\Phi^+)$. This determines a root basis $\Delta = \{\alpha_1, \ldots, \alpha_\ell\}$ which is a subset of Φ^+ for which every $\alpha \in \Phi^+$ can be written uniquely as $\alpha = \sum m_i \alpha_i$ for positive integers m_i.

In the case of GL_n, can take B to be the set of upper triangular matrices. Then $\Phi^+ = \{e_i - e_j \mid i < j\}$, $\Delta = \{e_1 - e_2, e_2 - e_3, \ldots, e_{n-1} - e_n\}$. The unipotent radical of B consists of the upper triangle unipotent elements. The simple roots correspond to

$$\begin{pmatrix} 1 & * & & 0 \\ & 1 & * & \\ & & \ddots & * \\ & & & 1 \end{pmatrix}, \qquad \text{and } U^{ab} = \bigoplus_{\alpha \in \Delta} \mathfrak{g}_\alpha$$

as a representation of T.

In the end, for fixed $T \subset B \subset G$ we get a *based root datum* $BR = (M, \Phi, \Delta, M^\vee, \Phi^\vee, \Delta^\vee)$. The set of Borel subgroups containing T are permuted simply transitively by $W(T, G)$. Both $\mathrm{Aut}(BR)$ and W are subgroups of $\mathrm{Aut}(R)$. In fact, the following is true.

Theorem 6.0.2. $\mathrm{Aut}(R) = W \rtimes \mathrm{Aut}(BR)$.

For GL_n, $\mathrm{Aut}(R) = S_n \rtimes \mathbb{Z}/2$, but (obviously) $-1 \in \mathrm{Aut}(R)$ is not an automorphism that preserves the basis Δ, so this is not the generator of the $\mathbb{Z}/2$ in this decomposition. Rather $\sigma : e_i \mapsto -e_{n+1-i}$ is the generator. (In matrix form this has -1 along the anti-diagonal and zeros elsewhere.) Exercise: what is the involution that this element induces on GL_n? (It can't be inverse transpose because it must preserve B, but it is something close.)

For G_2, $\mathrm{Aut}(BR)$ must be trivial because it has to preserve $\Delta = \{1, -\sqrt{3}+i\}$ but it can't permute them because they have different lengths. Hence $\mathrm{Aut}(R) = D_{12}$.

It is possible in complete generality to give a presentation

$$W = \langle s_\alpha \mid \alpha \in \Delta, s_\alpha^2 = 1, (s_{\alpha_i} s_{\alpha_j})^{m_{ij}} = 1 \rangle$$

for some integers m_{ij}. In the case of GL_n this looks like

$$S_n = \langle s_\alpha \mid \alpha \in \Delta, s_\alpha^2 = 1, (s_{\alpha_i} s_{\alpha_j})^2 = 1 \text{ if } j \neq i \pm 1, (s_{\alpha_i} s_{\alpha_j})^3 = 1 \text{ if } j = i \pm 1 \rangle,$$

and for G_2:

$$D_{12} = \langle s_\alpha, s_\beta \mid s_\alpha^2 = s_\beta^2 = 1, (s_\alpha s_\beta)^6 = 1 \rangle.$$

The exact sequence

$$1 \to T \to N_G(T) \to W \to 1$$

does not in general split. The map $N_G(T) \to W$ is given by $n_\alpha(x) \mapsto s_\alpha$. It can happen that $n_\alpha(x)$ has order 4. In the case of SL_2, this happens: $n_\alpha(x)^2 = \left(\begin{smallmatrix} 0 & x \\ -1/x & 0 \end{smallmatrix}\right)^2 = -1$. So s_α can not be lifted to an element of order 2 in $N_G(T) \setminus T$. However, $\mathrm{Aut}(BR)$ can be realized as automorphisms of G.

A *pinning* can be "visualized" as a butterfly with B and $-B$ the wings, and a choice of simple roots in G "pins" down the wing B. To describe this precisely, we start with fixed $T \subset B \subset G$ as before, and also for $\alpha \in \Delta$ we choose $X_\alpha \in \mathfrak{g}_\alpha$. The choice of X_α is equivalent to have maps $e_\alpha : \mathbb{G}_a \to U_\alpha \subset G$. Given e_α, we have $Lie(e_\alpha) : \mathbb{G}_a \to \mathfrak{g}_\alpha$, and we can set $X_\alpha = Lie(e_\alpha)(1)$. In the other direction, given X_α can define $e_\alpha(t) = \exp(tX_\alpha)$.

Making this choice of e_α pins down the group completely. The inner automorphism group of G is $Inn(G) = G/Z_G$, those inner automorphisms which preserve T give $Inn(G, T) = N_G(T)/Z_G$, those which also preserve T give $Inn(G, T, B) = T/Z_G$ and those which also preserve $\{X_\alpha\}$ are $Inn(G, T, B, \{X_\alpha\}) = Z_G/Z_G = 1$. To see this last equality, let $t \in T$ satisfy $tX_\alpha = X_\alpha$ for all α. Then $\alpha(t) = 1$ for all $\alpha \in \Delta$, hence $\alpha(t) = 1$ for all positive (hence negative) roots. Thus, t is in the subgroup of T dual to $M/\mathbb{Z}\Phi$. This implies that $t \in Z_G$.

So as subgroups of $\mathrm{Aut}(G)$, $\mathrm{Aut}(G,T,B,\{X_\alpha\})$ and $Inn(G)$ are disjoint. In fact, the following holds.

Theorem 6.0.3 (Chevalley)**.** *$\mathrm{Aut}(G) = Inn(G) \rtimes \Theta$ where Θ is the group of pinned automorphisms: $\Theta = \mathrm{Aut}(BR) = Out(R)$.*

(This is analogous to $\mathrm{Aut}(R) \simeq W \rtimes \Theta$.)

Exercise: Show that for GL_n the element $\sigma \in \mathrm{Aut}(BR)$ (from before) acts as an outer automorphism of GL_n.

The group Θ has been determined for all reductive groups. For the cases we have discussed we have the following.

G	$T = \mathbb{G}_m^n$	GL_n	G_2
Θ	$\mathrm{GL}_n(\mathbb{Z})$	$Z/2$	1

6.1. **Classification of reductive groups over an arbitrary field.** Let k be a field, and k^s the separable closure of k. The classification can be described in terms of $\mathrm{Gal}(k^s/k)$. Today we will discuss how it works for tori. We are looking for all T over k such that T is isomorphic to T_0 over $\bar{k}$. In fact this isomorphism can be accomplished over a finite separable extension.

Choose $f : T_0 \to T$ with is an isomorphism over k^s. For $\sigma \in \mathrm{Gal}(k^s/k)$ define $\sigma(f) = f \circ a_\sigma : T_0 \to T$ where $a_\sigma \in \mathrm{Aut}(T_0)(k^s) = \mathrm{Aut}(M) = \mathrm{GL}_n(\mathbb{Z}) = \mathrm{Aut}(T_0)(k)$. Can show that $a_{\sigma\tau} = a_\sigma \sigma(a_\tau)$. Because, in this case, σ acts trivially on $\mathrm{Aut}(T_0)(k^s)$, this reduces to $a_{\sigma\tau} = a_\sigma a_\tau$. In other words, we have a representation $a : \mathrm{Gal}(k^s/k) \to \mathrm{Aut}(M)$. If we replace f by $f' = fb$ then $a_{\sigma'} = b^{-1} a_\sigma b$. So a' is conjugate to a by an element $b \in \mathrm{GL}_n(\mathbb{Z})$.

To summarize, starting with T we get a homomorphism $a : \mathrm{Gal}(k^s/k) \to \mathrm{GL}_n(\mathbb{Z})$ that is defined up to conjugation, i.e. an integral representation of $\mathrm{Gal}(k^s/k)$ of rank n. This process can be reversed: given M, let $T(k) = ((k^s)^\times \otimes M^\vee)^{\mathrm{Gal}(k^s/k)}$.

For $n = 1$,

$$\{T \simeq \mathbb{G}_m \text{ over } k^s\} \leftrightarrow \{a : \mathrm{Gal}(k^s/k) \to \mathrm{GL}_1(\mathbb{Z})\} = \{\pm\}.$$

The case $a = 1$ corresponds to $T = \mathbb{G}_m$ over k. If a is non trivial then $\ker a$ fixes a separable quadratic extension E/k, and for σ a generator of $\mathrm{Gal}(E/k)$,

$$T = \{\alpha \in E \mid \alpha\alpha^\sigma = 1\}.$$

In the case that $k = \mathbb{R}$, there is a unique quadratic extension, so these two tori are $T = \mathbb{R}^\times$ and $T = S^1$.

For $n = 2$ and $k = \mathbb{R}$, : $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \to \mathrm{GL}_2(\mathbb{Z})$ corresponds to an order 2 element $a \in \mathrm{GL}_n(\mathbb{Z})$. The possibilities (up to conjugacy) are:

a	$\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$	$\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$	$1 - 1$	$-1 - 1$
$(\mathbb{R}^\times)^2$	$\mathbb{C}^\times$	$S^1 \times \mathbb{R}^\times$	$(S^1)^2$	

For $k = \mathbb{F}_q$, we seek continuous homomorphisms $\mathrm{Gal}(\bar{F}_q/F_q) \simeq \widehat{\mathbb{Z}} \to \mathrm{GL}_2(\mathbb{Z})$. This means that we seek elements of finite order in $\mathrm{GL}_2(\mathbb{Z})$. This will be the image of F. The possible orders are $1, 2, 3, 4, 6$. In all but the case of order 2, there is a single conjugacy class. For order 2, we have the same four cases as above (unless $2 \mid q$.) For general n, T is determined by the action of $F_q \in \mathrm{Aut}(M)$ and

$$\#T(q) = |\det(1 - F_q \mid M)|.$$

Note that for $k = \mathbb{Q}$ (or k in general, right?), all 1-dimensional tori can be realized as subgroups of SL_2.

7. Tuesday November 1

7.1. **The classification of forms.** We saw that if T is a torus then there are no roots, and so the root datum is just $R = (M, M^\vee)$ of dimension n, so $\mathrm{Aut}(R, \Delta) = \mathrm{Aut}(T) = \mathrm{GL}_n(\mathbb{Z})$.

In general, things are a little more complicated. Let k be a field with separable closure k^s, and assume that (R, T) is a based root datum. Then there exists a unique reductive split group $G_0 \supset B_0 \supset \mathbb{G}_m^n = T$. These are called Chevalley groups. Some examples: $\mathrm{GL}_n(V/k), \mathrm{SL}_n(V/k), \mathrm{Sp}_{2n}(V/k), \mathrm{SO}_n(V/k), \ldots$. In orthogonal case we need $W \subset V$ to be a maximal isotropic subspace over k.

If G has based root datum (R, Δ) then $G \simeq G_0$ over k^s. Choose $f : G_0 \to G$ to be an isomorphism. Every other isomorphism is of the form $f^\sigma = f \circ a_\sigma$ for $a_\sigma \in \mathrm{Aut}(G_0)(k^s)$. We have $a_{\sigma\tau} = a_\sigma \circ a_\tau$. The class c_G of this 1-cycle in $H^1(\mathrm{Gal}(k^s/k), \mathrm{Aut}(G_0)(k^s))$ determines the isomorphism class of G/k.

Where for tori $\mathrm{Aut}(T_0)(k^s) = \mathrm{Aut}(T_0)(k)$ (since the automorphism group is $\mathrm{GL}_n(\mathbb{Z})$), this is a whole other story. However, there is something similar. there is a (restriction?) map

$$H^1(\mathrm{Gal}(k^s/k), \mathrm{Aut}(G_0)(k^s)) \to H^1(\mathrm{Gal}(k^s/k), \mathrm{Out}(G_0)(k^s))$$

given by $c_G \mapsto d_G : \mathrm{Gal}(k^s/k) \to \mathrm{Out}(G_0)(k) = \mathrm{Aut}(R, \Delta)$. The cocycle d_G is a homomorphism since $\mathrm{Aut}(R, \Delta)$ is a trivial Galois module. In fact, every homomorphism d_G can be obtained this way. (This is because the sequence $G/Z \to \mathrm{Aut}(G) \to \mathrm{Aut}(R, \Delta)$ splits.

To summarize, $H^1(k, \mathrm{Aut}(G)) \to H^1(k, \mathrm{Out}(G)) \simeq \mathrm{Hom}(\mathrm{Gal}(k^s/k), \mathrm{Aut}(R, \Delta))$ is surjective. This gives, for each $q : \mathrm{Gal}(k^s/k) \to \mathrm{Aut}(R, \Delta)$, a group G_q which is characterized by the fact that it contains a Borel $B \subset T$, with T maximal but not necessarily split. These are called *quasi-split* groups. The fiber over q in $H^1(k, \mathrm{Aut}(G_0))$ can be identified with the image of $H^1(k, \mathrm{Aut}(G_0))$ in $H^1(k, G_q/Z_q)$. (Note that the image of G_q is G_q/Z_q.) The corresponding groups G are called *inner forms* of G_q.

Example 7.1.1. $G_0 = \mathrm{GL}_n$. Then T_0 can be taken to be the diagonal matrices $(\lambda_1, \ldots, \lambda_n)$ as usual, $\mathrm{Aut}(R, \Delta) = \mathbb{Z}/2$ with anit-diagonal matrix with entries -1 an element of $\mathrm{Aut}(M)$. Then G_q is determined by $q : \mathrm{Gal}(k^s/k) \to \mathbb{Z}/2$. If this is trivial, we get GL_n. If it is nontrivial q must fact through a quadratic extension E/k. If $n = 1$ we get $G_q = (E^\times)_{\mathbb{N}=1}$.

For general $n \geq 1$ (and q nontrivial), $G_q \simeq U_n(V)$ where V is an n-dimensional vector space over E with non-degenerate Hermitian form $\varphi : V \times V \to E$ satisfying $\varphi(w, v) = \varphi(v, w)^\sigma$ for the nontrivial element $\sigma \in \mathrm{Gal}(E/k)$. For $n = 2m$ or $n = 2m + 1$, this requires that there be an isotropic subspace $W \subset V$ of dimension m. Then there is a flag

$$\underbrace{0 \subset W_1 \subset W_2 \subset \cdots \subset W_m = W}_{\text{isotropic flag of } W} \oplus W_{m-1}^\perp \subset \cdots .$$

Then $B \subset U(V)$, the stabilizer of this flag, is a Borel with maximal torus $T(k) \simeq (E^\times)^m$ if $n = 2m$ and $T(k) \simeq (E^\times)^m \times (E^\times)_{\mathbb{N}=1}$ if $n = 2m + 1$.

Now we have to classify inner forms of each of these. For the GL_n, these correspond to element of $H^1(k, \mathrm{PGL}_n)$. Since $\mathrm{PGL}_n = \mathrm{Aut}(M_n)/k$ these correspond to isomorphism classes of central simple algebras A of rank n^2 and $G(k) = A^\times$.

Remark: $A^\times \simeq A_{\text{opp}}^\times$ so $G_A \simeq G_{A_{\text{opp}}}$. So even though A, A_{opp} may be different classes in $H^1(k, \mathrm{PGL}_n)$, the map to the same thing in $H^1(k, \mathrm{Aut}(G_0))$. This happens because/when $\mathrm{Aut}(G)(k) \to \mathrm{Out}(G)(k) = \mathbb{Z}/2$ is not surjective.

The inner forms of U_n correspond to $H^1(k, U_n/Z)$. By considering the restriction map

$$H^1(k, U_n/Z) \to H^1(E, U_n/Z) \simeq H^1(E, \mathrm{PGL}_n).$$

we, as above, get a central simple algebra A over E. Moreover, (for it to come from $H^1(k, U_n/Z)$) it must have a *anti-involution of the second kind*, i.e. an anti-involution τ which acts by conjugation on E. The unitary groups of other signatures will come from $A \simeq M_n(E)$, but $\tau(g) = h^{-1}gh$ for h non-Hermitian.

To do this kind of analysis in more generality, one has to know a lot about the field k. As Dick said, "fortunately, number theorists know a lot about the field."

For k finite of order q, there is a unique quadratic extension E/k of order q^2. In this situation the theorem of Wederburn implies that $H^1(k, \mathrm{PGL}_n) = H^1(k, U_n/Z) = 1$. This was generalized by Lang: $H^1(k, G_q/Z_q) = 1$ for G_q any connected algebraic group. So the classification over finite fields is quite nice:

$$H^1(k, \mathrm{Aut}(G_0)) = \mathrm{Hom}(\underbrace{\mathrm{Gal}(k^s/k)}_{\widehat{\mathbb{Z}}F}, \mathrm{Aut}(R, \Delta))/\sim = \{\text{finite order conj. classes in } \mathrm{Aut}(R, \Delta)\}.$$

Since $\mathrm{Aut}(R, \Delta)$ is known this is not hard. (For example, for GL_n, $\mathrm{Aut}(R, \Delta) = \mathbb{Z}/2$.)

For k local, Knaser proved that $H^1(k, G_{ad})$ is finite abelian for any group of adjoint type, i.e. $G_{ad} = G_q/Z_q$. He did this by considering the exact sequence

$$1 \to A \to G_q \to G_{ad} \to 1,$$

and then showing that in the corresponding long exact sequence of cohomology

$$H^1(k, G_{ad}) \simeq H^2(k, A_q).$$

(The latter group is a finite group scheme over k of multiplicative type.)

Tate duality gives

$$H^2(k, A_q) \times H^0(k, C(A_q)) \to H^2(k, \mathbb{G}_m) = \mathbb{Q}/\mathbb{Z}$$

where $C(A_q)$ is the Cartier dual of A_q. Since $C(A_q)) = \mathrm{Hom}(A_q, \mathbb{G}_m) = X(T^{sc})/\mathbb{Z}\Phi$, the calculation of H^0 is easy. Then

$$H^2(k, G_{ad}) = \mathrm{Hom}((X(T^{sc})/\mathbb{Z}\Phi)^{\mathrm{Gal}(k^s/k)}, \mathbb{Q}/\mathbb{Z}) = \pi_1(G_{ad})_{\mathrm{Gal}(k^s/k)}.$$

For GL_n, $H^1(k, \mathrm{PGL}_n) \simeq H^2(\mu_n) = H^0(\mathbb{Z}/n)^* \simeq (\mathbb{Z}/n)^\times$.

For k a global field, the Hasse principle gives

$$H^1(k, G_q/Z_q) \hookrightarrow \bigoplus_v H^1(k_v, G_q/Z_q).$$

(This is not a surjection.)

7.2. **The L-group.** If G/k is a reductive group with based root datum $(M, \Phi, \Delta, \ldots)$ we can define ${}^LG$ to be a complex algebraic group with connected component $\widehat{G}/\mathbb{C}$ whose root datum $(M^\vee, \Phi^\vee, \Delta^\vee, \ldots)$. The group G has a quasi-split inner form given by $q : \mathrm{Gal}(k^s/k) \to \mathrm{Aut}(R, \Delta)$. Let E be the (smallest) separable Galois extension of k through which q factors. (The maximal torus $T \subset B \subset G_q$ splits over E.) The component group of ${}^LG$ will be $\mathrm{Gal}(E/k)$.

Since $\mathrm{Aut}(R,\Delta) = \mathrm{Aut}(R^\vee, \Delta^\vee) = \mathrm{Aut}(\widehat{G}, \widehat{B}, \widehat{T}, \{\widehat{X}_\alpha\})$, for a fixed pinning, we get a map

$$\mathrm{Gal}(E/k) \hookrightarrow \mathrm{PinnAut}(\widehat{G}, \widehat{B}, \ldots) \subset \mathrm{Aut}(\widehat{G}).$$

With this map, we define

$$^L G = \widehat{G} \rtimes \mathrm{Gal}(E/k).$$

Note that this only remembers the quasi-split form of G.

A Langlands parameter is a homomorphism $\varphi : \mathrm{Gal}(k^s/k) \to {}^L G$ such that the composition of ϖ and the projection onto $\mathrm{Gal}(E/k)$ is the standard map $\mathrm{Gal}(k^s/k) \to \mathrm{Gal}(E/k)$. We consider $\varphi \sim \varphi'$ if they are conjugate by an element of $\widehat{G}$. The conjugacy class $C_\varphi \subset \widehat{G}$ [of the image] is an invariant of φ.

Example: Suppose $G = G_0$ is split (or G an inner form of G_0). Then $q = 1$, so ${}^L G = \widehat{G}$. For $G = \mathrm{GL}_n$, $\widehat{\mathrm{GL}_n} = \mathrm{GL}_n(\mathbb{C})$, so a Langlands parameter is an Artin representation.

Example: $G = \mathrm{SL}_2$. Then $[M : \mathbb{Z}\Phi] = 2$ and $[M^\vee : \mathbb{Z}\Phi^\vee] = 1$. Since $\widehat{G} = \mathrm{PGL}_2(\mathbb{C}) = \mathrm{SO}_3(\mathbb{C})$, a Langlands parameter of SL_2 is a 3-dimensional orthogonal representation of $\mathrm{Gal}(k^s/k)$ with determinant 1. The same phenomenon occurs for $G = \mathrm{Sp}_{2n}$ ($\widehat{G} = \mathrm{SO}_{2n+1}$).

Example: the L-group of a torus T over k. First, consider $\dim T = 1$. If $T \simeq \mathbb{G}_m$ then $\widehat{T} = \mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^\times$. If T is not split then it must be of the form $U_1(E/k)$ for separable quadratic extension E, and so ${}^L T = \mathbb{C}^\times \rtimes \mathrm{Gal}(E/k)$. If $\langle \sigma \rangle = \mathrm{Gal}(E/k)$, the action on $\mathbb{C}^\times$ is $\sigma z \sigma^{-1} = z^{-1}$.

In general an n-dimensional torus T corresponds to $q : \mathrm{Gal}(k^s/k) \to \mathrm{GL}(M) \simeq \mathrm{GL}(M^\vee)$, and $T(k) = (M^\vee \otimes (k^s)^\times)^{\mathrm{Gal}(k^s/k)}$. So $\widehat{T} \simeq (\mathbb{C}^\times)^n \simeq M \times \mathbb{C}^\times$. This is both the characters of T and the cocharacters of $\widehat{T}$, hence ${}^L T = M \otimes \mathbb{C}^\times \rtimes \mathrm{Gal}(E/k)$.

This formulation of ${}^L G$ as a semidirect product does have some problems. For example, for $G = \mathrm{PGL}_2/k$, and

$$\varphi : \mathrm{Gal}(k^s/k) \to \mathrm{SL}_2(\mathbb{C}) = \widehat{G} = {}^L G$$

suppose that φ factors through $N(\widehat{T})$. Then composing this with reduction modulo $\widehat{T}$ we have a map

$$\mathrm{Gal}(k^s/k) \to N(\widehat{T}) \to N(\widehat{T})/\widehat{T} \simeq \mathbb{Z}/2.$$

This gives an extension E/k for which one would like to say that this is a parameter of $U_1(E/k)$, but this is just not the case. (The problem is that $N(\widehat{T})$ is not isomorphic to $\widehat{T} \rtimes \mathbb{Z}/2$.)

As an exercise, give a classical description for a Langlands parameter of $G = U_n$. In this case, $\widehat{G} = \mathrm{GL}_n(\mathbb{C})$ and ${}^L G = \mathrm{GL}_n(\mathbb{C}) \rtimes \mathrm{Gal}(E/k)$.

In the case of GL_1,

$$\begin{tikzcd}
\mathrm{Gal}(k^s/k) \arrow[r] \arrow[dr] & {}^L G = \mathbb{C}^\times \rtimes \mathrm{Gal}(E/k) \arrow[r] & \mathbb{C}^\times \\
& \mathrm{Gal}(k^s/E) \arrow[ur, "\chi"] &
\end{tikzcd}$$

There is a map $Ver : \mathrm{Gal}(E^s/E)^{ab} \to \mathrm{Gal}(k^s/k)^{ab}$. The characters χ which arise are exactly those for which $Ver(\chi)$ is trivial.

8. November 18, 2011

Let k be a field, and G/k a reductive group with split form G_0. This gives an element $c_G \in H^1(k, \mathrm{Aut}(G_0))$. This group is hard to compute, but there is a map $H^1(k, \mathrm{Aut}(G_0)) \to H^1(k, \mathrm{Out}(G_0)) \simeq \mathrm{Hom}(\mathrm{Gal}(k^s/k), \mathrm{Aut}(R))$. In other words, there is an action of $\mathrm{Gal}(k^s/k)$ on

$$\mathrm{Aut}(BR) = \mathit{PinnedAut}(G_q \supset B \supset T, \{X_\alpha\}) = \mathit{PinnedAut}(\widehat{G} \supset \widehat{B} \supset \widehat{T}, \{X_\alpha^\vee\}).$$

Since this group sits in $\mathrm{Aut}(\widehat{G})$, we have an action of $\mathrm{Gal}(k^s/k)$ on $\widehat{G}$.

The composition $\mathrm{Gal}(k^s/k) \to \mathrm{Gal}(E/k) \to \mathrm{Aut}(BR)$ allows us to define ${}^LG = \widehat{G} \rtimes \mathrm{Gal}(E/k)$. (Note that it depends only on the image of c_G in $H^1(k, \mathrm{Out}(G_0))$, i.e. only on the quasi-split form of G.)

Now we can define a *Langlands parameter* to be a map $\varphi : \mathrm{Gal}(k^s/k) \to {}^LG$ which commutes with the natural projections of $\mathrm{Gal}(k^s/k)$ and ${}^LG$ onto $\mathrm{Gal}(E/k)$. We say that two parameters are equivalent, and write $\varphi \sim \varphi'$ if they are conjugate by an element of $\widehat{G}$.

Examples:

- $G = \mathrm{GL}_n$. Then ${}^LG = \mathrm{GL}_n(\mathbb{C}) = \mathrm{GL}(M)$, so a Langlands parameter is $\varphi : \mathrm{Gal}(k^s/k) \to \mathrm{GL}(M)$ up to conjugacy.
- If $G = U_n$ then ${}^LG = \mathrm{GL}(M) \rtimes \mathrm{Gal}(E/k)$. If n is odd (resp even) then this is the normalizer of GL_n in $O(W)$ (resp $\mathrm{Sp}(W)$) where W_{2n} is an orthogonal (resp symplectic) space over $\mathbb{C}$, and $W_{2n} = M \oplus M'$ with M a maximal isotropic subspace of dimension n. This gives $\mathrm{GL}(M) \hookrightarrow O(W)$ (resp $\mathrm{GL}(M) \hookrightarrow \mathrm{Sp}(W)$).

8.1. **Local parameters.**

Now assume that k is p-adic. (i.e. an extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$.) Let T/k be a torus. Then the root datum of T is just $(\mathrm{X}_\bullet(T), \mathrm{X}^\bullet(T))$ (there are no roots), and $\mathrm{Gal}(E/k)$ acts on $\mathrm{X}_\bullet(T)$. Then ${}^LT = \widehat{T} \rtimes \mathrm{Gal}(E/k) = (\mathrm{X}_\bullet(T) \otimes \mathbb{C}^\times) \rtimes \mathrm{Gal}(E/k)$. So a Langlands parameter for a torus T over k is

$$\varphi : \mathrm{Gal}(k^s/k) \to (\mathrm{X}_\bullet(T) \otimes \mathbb{C}^\times) \rtimes \mathrm{Gal}(E/k) \qquad \sigma \mapsto (c_\sigma, \bar{\sigma}),$$

which is a cocycle, to conjugation by $(d, 1)$:

$$\sigma \mapsto (d^{1-\sigma} \cdot c_\sigma, \bar{\sigma})$$

which is a coboundary. Hence Langlands parameters are given by $\alpha_\varphi \in H^1(k, \mathrm{X}_\bullet(T) \otimes \mathbb{C}^\times)$.

From the exact sequence

$$1 \longrightarrow \mathrm{X}_\bullet(T) \longrightarrow \mathrm{X}_\bullet(T) \otimes \mathbb{C} \xrightarrow{e^{2\pi i}} \mathrm{X}_\bullet(T) \otimes \mathbb{C}^\times \longrightarrow 1$$

and the fact that H^1 and H^2 of $\mathrm{X}_\bullet(T) \otimes \mathbb{C}$ is trivial, we get that α_φ can be thought of as an element of $H^2(k, \mathrm{X}_\bullet(T))$. Moreover, the pairing

$$\mathrm{X}_\bullet(T) \otimes T(k^s) \to (k^s)^\times$$

respects the Galois action. The cup product pairing in this case is

$$\underbrace{H^2(k, \mathrm{X}_\bullet(T))}_{discrete} \otimes \underbrace{H^0(k, T)}_{=T(k)} \to H^2(k, \mathbb{G}_m) = Br(k).$$

(Note that $T(k)$ is not compact.)

In the case that k is p-adic, local class field theory gives $Br(k) \simeq \mathbb{Q}/\mathbb{Z} \hookrightarrow S^1$, and by Tate there is a perfect pairing between $H^2(k, \mathrm{X}_\bullet(T))$ and the profinite completion

$\widehat{T(k)}$. We conclude that a Langlands parameter is an element of $H(T(k), S^1)$ of finite order.

In the case that $T = \mathbb{G}_m$, $T(k) = k^\times \simeq A^\times \times \pi^{\mathbb{Z}}$. $A^\times$ is compact, but obviously $\pi^{\mathbb{Z}}$ is not, so Langlands parameters of this type will not be able to give all homomorphisms $\chi \in \mathrm{Hom}(T(k), S^1)$. In order to get all homs, we need to replace $\mathrm{Gal}(k^s/k)$ by the Weil group.

$$\begin{tikzcd}
\mathrm{Gal}(k^s/k) \arrow[r] & \mathrm{Gal}(k^{un}/k) \simeq \widehat{\mathbb{Z}} \\
W(k) \arrow[u, hook] \arrow[r] & \mathbb{Z} \arrow[u]
\end{tikzcd}$$

(Note that $W(k)^{ab} = k^\times$, by local class field theory.) The group $W(k)$ has the same inertia as $Gal(k^s/k)$ but a representation of $W(k)$ can send $Frob$ to anything.

With this in mind, we give a new definition for a Langlands parameter: it is a homomorphism $\varphi : W(k) \to {}^LG$ for which the projections onto $\mathrm{Gal}(E/k)$ agree. When $G = T$ is a torus, these parametrize the irreducible complex representations of $T(k)$.

For archimedean fields, $W(\mathbb{C}) = \mathbb{C}^\times$ and $W(\mathbb{R}) = N_{\mathbb{H}^*}(\mathbb{C}^\times) = \mathbb{C}^\times \cup \mathbb{C}^* j$ where $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}ij$ is the Hamiltonian quaternion algebra with $jij = \bar{i}$ and $j^2 = -1$. So $W(\mathbb{R})$ sits in the (nonsplit!) exact sequence

$$1 \to \mathbb{C}^\times \to W(\mathbb{R}) \to \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \to 1.$$

The irreducible representations of $W(\mathbb{R})$ are of dimension 1 or 2. The 1-dimensional reps are the trivial character and the sign character of $\mathbb{R}^\times$ which is equal to the non trivial representation of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$. The 2-dimensional representations are given by half integers $\alpha \in \frac{1}{2}\mathbb{Z}$. Let

$$\chi_\alpha(z) = \frac{z^{2\alpha}}{(z \cdot \bar{z})^\alpha} \quad (\text{“=”} \left(\frac{z}{\bar{z}}\right)^\alpha).$$

Then $W_\alpha = \mathrm{Ind}_{\mathbb{C}^\times}^{W(\mathbb{R})} \chi_\alpha \simeq W_{-\alpha}$ is irreducible unless $\alpha = 0$ (in which case $W_0 \simeq 1 \otimes \mathrm{sgn}$.

If $\alpha \neq 0$ then $W_\alpha \simeq W_\alpha^*$. The pairing is symplectic if $\alpha \notin \mathbb{Z}$ and orthogonal if $\alpha \in \mathbb{Z}$. In the latter case the determinant of W_α is sgn.

Let $G = \mathrm{PGL}_2 = \mathrm{SO}_{2,1}$ over $\mathbb{R}$. The quasi-split form of G is SO_3, so each of these has L-group ${}^LG = \mathrm{SL}_2(\mathbb{C})$. So a Langlands parameter is a homomorphism $\varphi : W(\mathbb{R}) \to \mathrm{SL}_2(\mathbb{C})$ up to conjugation. Since $\mathrm{SL}_2(\mathbb{C}) = \mathrm{Sp}_2(\mathbb{C})$, this is a symplectic representation. By the above, these correspond to $\alpha = \pm\frac{1}{2}, \pm\frac{3}{2}, \pm\frac{5}{2}, \ldots$. These, in turn, correspond to the irreducible representations of SO_3 are of dimension $2|\alpha|$ and the discrete representations of PGL_2 of weight $2|\alpha| + 1$.

If $G = \mathrm{SO}_{2n+1}(\mathbb{R})$, ${}^LG = \mathrm{Sp}_{2n}(\mathbb{C})$. A parameter is then of the form $W_{\alpha_1} \oplus W_{\alpha_2} \oplus \cdots \oplus W_{\alpha_n}$. If all of the α_i distinct, we get the representation of $\mathrm{SO}_{2n+1}(\mathbb{R})$ of highest weight $\mu = (\alpha_1, \ldots, \alpha_n) - \rho$ where $\rho = (n - \frac{1}{2}, n - \frac{3}{2}, \ldots, \frac{1}{2})$.

8.2. **Unramified representations of p-adic groups.** For $G = \mathbb{G}_m$, $G(k) = k^\times \simeq A^\times \times \pi^{\mathbb{Z}}$. A character $\chi : k^\times \to \mathbb{C}^\times$ is *unramified* if it is trivial on $A^\times$. In this case χ is determined by $\chi(\pi)$. Recall that $W(k)^{ab} \simeq k^\times$. Under this isomorphism $I \to A^\times$. So a parameter of $W(k)$ is unramified if it is trivial on inertia.

If G is any reductive group over k, a parameter $\varphi : W(k) \to {}^L G \to \mathrm{Gal}(E/k)$ is *unramified* if it is trivial on I. Such parameter is determined by the image of F. Note that this forces E/k to be unramified. These correspond to the irreducible representations of $G(k)$ that "trivial on $G(A)$."

Let T be a torus over k split by an unramified extension E. (Then $\mathrm{Gal}(E/k) = \mathbb{Z}/n$.) Let $S \subset T$ be a maximal split subtorus, so that $\mathrm{X}^\bullet(S) \hookrightarrow \mathrm{X}^\bullet(T)^{\mathrm{Gal}(E/k)}$. $T(k)$ has a maximal compact subgroup (as does $S(k)$); call it $T(A)$ (respectively $S(A)$). It is a fact that

$$S(k)/S(A) \simeq T(k)/T(A) \simeq \mathrm{X}^\bullet(T).$$

So we would like to show that there is a correspondence

$$\left\{ \begin{array}{c} \text{unramified} \\ \text{parameters} \end{array} \right\} \leftrightarrow \{\chi : S(k)/S(A) \to \mathbb{C}^\times\}.$$

Recall that ${}^L T = \mathrm{X}_\bullet(T) \otimes \mathbb{C}^\times \rtimes \mathrm{Gal}(E/k)$. Let $F = (\hat{t}, F\mid_E) \in {}^L T$. Conjugating by an element $(u, 1)$:

$$(u,1)(\hat{t}, F\mid_E)(u,1)^{-1} = (\hat{t}\cdot u^{1-F}, F\mid_E).$$

Here $1 - F : \widehat{T} \to \widehat{T}$ with

$$1 \to (1-F)\widehat{T} \to \widehat{T} \to \widehat{S} \to 1$$

exact. We conclude that giving an unramified parameter is equivalent to giving an element of $\widehat{S} = \mathrm{X}_\bullet(S) \otimes \mathbb{C}^\times = \{\chi : S(k)/S(A) \to \mathbb{C}^\times\}$ as desired.

For general G/k quasi split, split by an unramified extension E, there is an injection $G(A) \hookrightarrow G(k)$ which gives a (hyperspecial) maximal compact subgroup. We say a representation $G(k) \to \mathrm{GL}(V_\mathbb{C})$ is unramified if $\dim(V_\mathbb{C}^{G(A)}) = 1$. (This is always ≤ 1 for irreducible representations.)

9. November 15, 2011

Today we will modify our definition of a Langlands parameter. Recall that an unramified local parameter is a map

$$\varphi : W(k) \to \mathbb{Z}F \to {}^L G = \widehat{G} \rtimes \mathrm{Gal}(E/k)$$

with E/k unramified. Assume that G is unramified (i.e. quasi-split and split by an unramified extension.)

9.1. **Reformulation of a Langlands parameter.** To see why we will have to modify our definition of a Langlands parameter, assume G is split. Let $A \subset k$ be the ring of integers. Since G actually has a model over $\mathbb{Z}$, we can consider G/A. Then $G(A) \subset G(k)$ is a (very special) maximal compact subgroup. We say that a representation V of $G(k)$ is *unramified* if $V^{G(A)} \neq 0$. (This generalizes the notion of unramifed representation of a torus T: $\chi : T(k)/T(A) \to \mathbb{C}^\times$. It is too much to ask that $G(A)$ act trivially, but this is saying that it acts trivially on the largest subspace possible.)

We will see that an unramified parameter $\varphi : W(k) \to \mathbb{Z}F \to \widehat{G}(\mathbb{C})$ should map F to a *semisimple* conjugacy class. This adjustment to our definition comes about because complex parameters of local Weil groups in $\mathrm{GL}_2(\mathbb{C})$ correspond to compatible families of ℓ-adic representations $\mathrm{Gal}(k^s/k) \to \mathrm{GL}_n(\mathbb{Q}_\ell)$ for $\ell \neq p$.

For example, if $\ell \neq p$ then

$$T_\ell \mathbb{G}_m = V_\ell = \varprojlim \mu_{\ell^n}(k^s) = \varprojlim \mu_{\ell^n}(\mathbb{F}_q^s) \simeq \mathbb{Z}_\ell.$$

Moreover, F acts on V_ℓ by $\frac{1}{q}$ independent of ℓ. This corresponds to the parameter $\mathbb{Z}F \to \mathrm{GL}_1(\mathbb{C})$ given by $F \mapsto \frac{1}{q}$.

Similarly, if E/k is an elliptic curve, we define

$$T_\ell E - \varprojlim E[\ell^n](k^s) \simeq \mathbb{Z}_e ll^2.$$

This gives a representation $\mathrm{Gal}(k^s/k) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ for all $\ell \neq p$. If E has good reductions over $\mathbb{F}_q$ then this is an unramified representation and the characteristic polynomial of F^{-1} is $x^2 - ax + q$ where $\#E(\mathbb{F}_q) = q + 1 - a$. Hence F is semisimple.

It is also true that in the split case, unramified parameters correspond to semisimple conjugacy class in $\widehat{G}(\mathbb{C})$. In fact they are elements $s \in \widehat{T}(\mathbb{C})/W(T, G)$ which is sometimes called the Steinberg variety.

It turns out that our definition of Langlands parameter is still lacking. To see this we continue to study the ℓ-adic representation attached to an elliptic curve, but we now consider E with bad reduction. In this case, I acts nontrivially. The wild intertia group $I^{wild} \subset I$ must have finite image, but

$$I^{tame} = I/I^{wild} \simeq \prod_{\ell \neq p} \mathbb{Z}_\ell$$

can have infinite order. For example, $E : y^2 = x(x+1)(x-p)$ has multiplicative reduction and Tate proved that the image of I^{tame} is of finite index in $\left(\begin{smallmatrix} 1 & \mathbb{Z}_\ell \\ & 1 \end{smallmatrix}\right) \subset \mathrm{GL}_2(\mathbb{Z}_\ell)$.

The non-finiteness of the image of tame inertia can be accounted for by a unique element $N \in \mathfrak{gl}_n(\mathbb{C})$ such that $\varphi(\sigma t) = \exp(t_\ell(\sigma)N)$ on a subgroup of finite index in I^{tame}. This implies that a parameter $\varphi : W(k) \simeq I \rtimes \mathbb{Z}F$ must map F to a semisimple element and that there exists $N \in \widehat{\mathfrak{g}}$ such that $FNF^{-1} = q^{-1}N$.

To get our final definition of a parameter, we neet that it be a map $W(k) \times \mathrm{SL}_2(\mathbb{C}) \to {}^L G$ with the restriction to $W(k)$ as above and the restriction to $\mathrm{SL}_2(\mathbb{C})$ algebraic.

9.2. **Unramified representations of p-adic groups.** Let $G = \mathbf{G}(k) \supset \mathbf{G}(A) = K$ where $\mathbf{G}$ is an unramified reductive group. An admissible representation of G is a homomorphism $G \to \mathrm{GL}(V)$ where $Stab(v) \subset G$ is open for every $v \in V$ and $\mathrm{Res}_K(V) = \bigoplus m_i V_i$ where the V_i range over all irreducible representations of K and m_i are finite. (This is equivalent to saying that for all open compact subgroups J, V^J is finite dimensional.)

One problem with this definition is that $\mathrm{Res}_K(V^*) = \prod m_i V_i^*$ is not admissible if V is infinite dimensional (which is usually the case.) To remedy one considers the admissible dual $\bigoplus m_i V_i^*$.

A representation V is *unramified* if $\mathbb{C}$ =the trivial representation of K occurs.

For finite groups G, representations are synonymous with $\mathbb{C}[G]$-modules. The analogy in this case is as follows. Let

$$C_c^\infty(G) = \{f : G \to \mathbb{C} \mid f \text{ is locally constant and continuous}\},$$

and fix a Haar measure on G such that $\int_K dg = 1$. Then $C_c^\infty(G)$ acts on V by

$$f(v) = \int_G f(g)(gv)dg.$$

This contains a commutative subalgebra $\mathcal{H}_K \otimes \mathbb{C} = C_c^\infty(K\backslash G/K)$ which consists of the K-biinvariant functions. This has a basis of characteristic functions of double cosets[4] KgK, it acts on V and preserves V^K.

Theorem 9.2.1.
- *The map $V \to V^K$ of $\mathcal{H}_K \otimes \mathbb{C}$ gives a bijection betwen the irreducible representations of G with $V^K \neq 0$ and simple $\mathcal{H}_K \otimes \mathbb{C}$ modules.*
- *$\mathcal{H}_K$ is commutative, hence the simple modules are all 1-dimensional.*

The first fact holds for K replaced by any open compact J. The second fact implies that $\mathbb{C}$ occurs in V with multiplicity 1.

9.3. **The Satake isomorphism.** There is a Cartan decomposition $G = \cup_{t \in T(k)/T(A)} KtK$. Since $T(k) \simeq T(A) \times \mathrm{X}^\bullet(T)$ via $\lambda \in \mathrm{X}^\bullet(T) \mapsto \lambda(\pi)$, $T(k)/T(A) \simeq \mathrm{X}^\bullet(T)$. Thus, there is a map

$$\mathcal{H}_K \otimes \mathbb{C} \to (\mathcal{H}_T \otimes \mathbb{C})^W = \mathbb{C}[\mathrm{X}^\bullet(T)]^W = \mathbb{C}[\mathrm{X}_\bullet(\widehat{T})]^W.$$

This last group is isomorphic to $\mathcal{R}(\widehat{G}) \otimes \mathbb{C}$, the representation ring of $\widehat{G}$.

Both $\mathcal{H}_K$ and $\mathcal{R}(\widehat{G})$ are algebras over $\mathbb{Z}$, so one may ask whether there is a $\mathbb{Z}$-isomorphism between them. In fact

$$\mathcal{H}_K \otimes [q^{1/2}, q^{-1/2}] \simeq \mathcal{R}(\widehat{G}) \otimes [q^{1/2}, q^{-1/2}].$$

Example 9.3.1. Let $G = \mathrm{GL}_n(k) = \bigcup \mathrm{GL}_n(A)\,\mathrm{diag}(\pi^{m_1}, \dots, \pi^{m_n})\mathrm{GL}_n(A)$ with $m_1 \geq m_2 \geq \ldots \geq m_n$. This gives a basis of $\mathcal{H}_K$. Generators are

$$T_k = \mathrm{diag}(\overbrace{\pi, \dots, \pi}^{k \text{ times}}, 1, \dots, 1), \qquad T_n^{-1},$$

and

$$\mathcal{H}_K \otimes \mathbb{Z}[q^{-1}] = \mathbb{Z}[q^{-1}][T_1, T_2, \dots, T_n, T_n^{-1}].$$

9.4. **Global representations.** If k is a global field, the adeles $\mathbb{A}$ are a subset of $\prod k_v$ and contain $\bigoplus k_v$. Unlike $\bigoplus k_v$, $\mathbb{A}$ contains k, and unlike $\prod k_v$, $\mathbb{A}$ is locally compact.

$$\mathbb{A} = \prod\nolimits^* k_v = \bigcup_{S \text{ finite}} \left(\prod_{v \in S \supset S_\infty} k_v \times \prod_{v \notin S} A_v \right).$$

Hecke characters are characters $\chi : \mathbb{A}^\times / k^\times \to \mathbb{C}^\times$. Any character $\chi : \mathbb{A}^\times \to \mathbb{C}^\times$ can be written as $\chi = \prod_v \chi_v$ where $\chi_v : k_v \to \mathbb{C}^\times$ is unramified (hence trivial on A_v) for all but finitely many v, so it is easy to construct such characters. However, the assumption the $\chi\,|_k = 1$ poses strong restrictions.

This notion can be generalized to arbitrary groups, where we define an admissible representation π of $G(\mathbb{A}) = \prod^*_{G(A_v)} G(k_v)$ to be such that $\pi = \bigoplus' \pi_v$ where the π_v are admissible representations and all but finitely many are unramified. The generalization of a Hecke character is an admissible representation that is trivial on $G(k)$. The (almost correct) definition of an automorphic representation, is an admissible representation π such that there exists a nonzero linear form $f : \pi \to \mathbb{C}$ that is $G(k)$-invariant and if π_v is unramified and $\langle e_v \rangle = \pi_v^{K_v}$, $\langle e \rangle \in \pi$,

$$F(g) = f(ge) : G(k)\backslash G(\mathbb{A}) / \prod K_v \to \mathbb{C}$$

is fixed by $G(k)$.

[4] $\mathcal{H}_K = \bigotimes \mathbb{Z} char(KgK)$ where the sum is over all double cosets.

9.5. **The Steinberg representation.** We return to the case of k local. Assume $k \neq \mathbb{R}, \mathbb{C}$. There is an admissible representation $St : G(k) \to \mathrm{GL}(V)$ with parameter

$$\varphi : W(k) \times \mathrm{SL}_2(\mathbb{C}) \to {}^L G$$

where $N \in \widehat{G}$ is a generator of the regular nilpotent orbit. Can take $N = \sum \widehat{X}_i \in \mathfrak{g}$ where $\widehat{T} \subset \widehat{B} \subset \widehat{G}$ has pinning $\{\widehat{X}_i\}$. The element N is stable by $\mathrm{Gal}(E/k)$ and $C(\varphi) = \widehat{\mathbb{Z}}^{\mathrm{Gal}(E/k)}$. This is called the *Steinberg parameter.* Next time we will define the representation which corresponds to this.

10. November 29, 2011

Today we will discuss ramified representations of $G(k)$ for k local, and we will compare measures and define the "motive of a reductive group." Next time we will discuss a trace formula, and in the final lecture how this can be used to describe the dimension of certain spaces of automorphic forms.

Let k be a local field ($k \neq \mathbb{R}$ or $\mathbb{C}$) with ring of integers A, and $F_q = A/\pi$. Let G be a split reductive group over A. Then $G(A)$ is an open compact subgroup of the locally compact group $G(k)$. We say that $G(k) \to \mathrm{GL}(V_{\mathbb{C}})$ is unramified if $V_{\mathbb{C}}^{G(A)} \neq 0$. If $V_{\mathbb{C}}$ is irreducible then $\dim V_{\mathbb{C}}^{G(A)} \leq 1$. Then $V_{\mathbb{C}}^{G(A)}$ is a module for $\mathcal{H}(G(A)\backslash G(k)/G(A)) \simeq R(\widehat{G}) \otimes \mathbb{C}$. So we get a semisimple element $s \in \widehat{G}(\mathbb{C})$.

10.1. **The Steinberg representation.**

10.1.1. *Over a finite field.* Let G be a reductive group over $\mathbb{F}_q$. Then $G(q)$ is a finite group which contains $B(q)$ a Borel and $U(q)$ the unipotent radical of $B(q)$. In fact $U(q)$ is a Sylow p-subgroup of $G(q)$.

There exists an irreducible complex representation $\mathrm{St}(q)$ of $G(q)$ with dimension equal to $\#U(q)$ and $\mathrm{St}(q) \mid_{U(q)}$ is the regular representation of $U(q)$. $\mathrm{St}^{B(q)}$ is a 1-dimensional representation of the Hecke algebra $\mathcal{H}_{B(q)} = \mathbb{C}[B(q)\backslash G(q)/B(q)]$. There is a *Bruhat decomposition*: $G(q) = \cup_{w \in W} B(q)wB(q)$. Therefore, the dimension of $\mathcal{H}_{B(q)}$ is equal to $\#W$.

Theorem 10.1.1. *$\mathcal{H}_{B(q)} \simeq \mathbb{C}[W]$ as algebras.*

Recall that $\mathbb{C}[W]$ is generated by $\{s_\alpha \mid \alpha \in \Delta\}$ with $(s_\alpha s_\beta)^{m_{\alpha\beta}} = 1$ for some $m_{\alpha\beta} \in \{2, 3, 4, 6\}$ and $(s_\alpha - 1)(s_\alpha + 1) = 0$. On the other hand, $\mathcal{H}_{B(q)}$ is generated by $\{T_\alpha \mid \alpha \in \Delta\}$ and $(T_\alpha - q)(T_\alpha + 1) = 0$.

From this isomorphism we see that W has 2 distinguished characters:

- The trivial character. (This corresponds to $s_\alpha = 1$ for $\alpha \in \Delta$.)
- The sign character $\mathrm{sgn} = \det(W \mid M(T))$ (for which $s_\alpha = -1$.)

On the side of $\mathcal{H}_{B(q)}$ these characters correspond to $T_\alpha \mapsto q$ (the trivial representation), and $T_\alpha \mapsto -1$ (the Steinberg representation).

10.1.2. *The p-adic case.* Recall that there exists a canonical regular nilpotent element $N = \sum \widehat{X}_i \in \widehat{\mathfrak{g}}$ and therefore a map $\mathrm{SL}_2(\mathbb{C}) \to \widehat{G}$ which is fixed by $\mathrm{Gal}(E/k)$. This data then corresponds to a parameter $\varphi : W(k) \times \mathrm{SL}_2(\mathbb{C}) \to \widehat{G}(\mathbb{C})$, which is the Langlands parameter of the Steinberg representation.

In some sense the Steinberg representation for $G(k)$ corresponds to the sign character.

The Steinberg representation can best be constructed with a Hecke algebra (similar to the finite case.) There is a subgroup $I \subset G(A)$ which contains U as a normal subgroup. This is called the *Iwahori*.

In the case $G = \mathrm{GL}_2$,

$$\mathrm{GL}_2(\mathbb{Z}_p) \supset I = \begin{pmatrix} a & b \\ cp & d \end{pmatrix} \rhd \begin{pmatrix} 1+pa & b \\ pc & 1+pd \end{pmatrix} \rhd \begin{pmatrix} 1+pa & pb \\ pc & 1+pd \end{pmatrix}.$$

Note that the indices of these subgroups are $p-1$, $(p-1)^2$ and p.

The Steinberg representation is not unramified (i.e. $\mathrm{St}^{G(A)} = 0$) but St^I has dimension 1, hence it is a representation of $\mathcal{H}_I = \mathcal{H}(I\backslash G(k)/I)$, a noncommutative algebra. Letting $W_{aff} = N_G(T)(k)/T(A)$, there is a decomposition

$$1 \to T(k)/T(A) \to W_{aff} \to W \to 1.$$

(Recall that $T(k)/T(A) = \mathrm{X}^\bullet(T)$ by a choice of uniformizer π.) Similar to the Bruhat decomposition, $G(k) = \cup_{w \in W_{aff}} IwI$. As a $\mathbb{C}$ vector space representation of $\mathcal{H}_I$ is $\bigoplus_{w\in W_{aff}} \mathbb{C}w$.[5] Then $\mathcal{H}_I \simeq \mathbb{C}[W_{aff}]$ (as q-deformation.)

The elements $\alpha \in \Delta$ together with $-\beta$ where (for G simple) β is a highest root generate W_{aff}. Like in the finite case the Steinberg representation sends T_α to -1.

For any parahoric $P \supset I$, $\mathrm{St}^P = 0$.

10.2. **Depth zero supercuspidals.** We can consider $\mathrm{St}(q)$ as a representation of $G(A)$ by considering its action after reduction. It is a fact then that $\mathrm{Res}_{G(A)} \mathrm{St}$ contains $\mathrm{St}(q)$ with multiplicity 1. On the other hand, $\mathrm{Ind}_{G(A)} \mathrm{St}(q)$ is in general of infinite length so it is not a good way to construct St.

However, there are irreducible representations $V(q)$ of $G(q)$ such that $\mathrm{Ind}_{G(A)} V(q) = \pi$ is irreducible and $\mathrm{Res}_{G(A)} \pi$ contains $V(q)$ a cuspidal[6] representation of $G(q)$.

For example, the irreducible representations of $\mathrm{SL}_2(q)$ are

dim	1	q	$q+1$	$q-1$
rep	trivial	$\mathrm{St}(q)$	$\mathrm{Ind}_B \chi$	discrete series

The last ones are the cuspidal representations which come from characters of the nonsplit torus, but are harder to produce.

The discrete series representations can be realized in the ℓ-adic cohomology where they are indexed by characters of anisotropic tori $T(q) \subset G(q)$.

It is natural to ask what the Langlands parameters for these representations are. Reeder and DeBacker show that they are

$$\varphi : W(k) \to \widehat{G}(\mathbb{C})$$

that are trivial on I^{wild}. Hence, they factor through $I^{tame} \rtimes \langle F \rangle = W(k)/I^{wild}$. Moreover, $I^{tame} \to C \subset \widehat{T}$ a cyclic group of order prime to p with $Z(C) = \widehat{T}$ and $F \to N(\widehat{T})$ maps to an elliptic class in $N(\widehat{T})/\widehat{T} = W$.

[5] Sorry this sentence makes no sense. Possibly (?!) it should have said that $\mathrm{X}^\bullet(T)$ as a $\mathbb{C}$ vector space..., but I don't know.

[6] Gross called $V(q)$ a *supercuspidal* representation, but I have always understood the *super* part to come from the fact that it is some kind of p-adic version of what is called merely *cuspidal* in the finite field case.

10.3. **Wild representations.** All of the representations we have studied so far satisfy $\pi^{G(A)_1} \neq 0$ where $G(A)_1$ is the kernel of reduction mod p. Such representations are *tame*. Those for which $\pi^{G(A)_1} = 0$ are *wild*.

Let $U = U(I)$ be the unipotent radical of the Iwahori group I. It contains U^+. The Frattini quotient is $\phi(U) = U/[U,U]U^0$. It is an elementary abelian p-group, therefore a $\mathbb{Z}/p$ vector space. As representations of $T(q)$,

$$U(I)/U^+ = \bigoplus_{i \neq p} \mathbb{F}_q^+(\alpha_i).$$

By this we mean that $\mathbb{F}_q$ is taken as an additive group, $\alpha_0, \alpha_1, \dots, \alpha_\ell$ are affine simple roots.

We call a character $\chi : \sum_{i \neq p} \mathbb{F}_q^+(\alpha_i) \to \mathbb{C}^\times$ *generic* if it is nontrivial on each $\mathbb{F}_q(\alpha_i)$.

For $\mathrm{GL}_n(q)$, $\phi(U)$ consists of upper triangle unipotent matrices with nonzero terms only on the offdiagonal.

A character $\chi : U(I) \to \mathbb{C}^\times$ is *affine generic* if it is non trivial on each othe $\ell = 1$ lines. In this case, $\mathrm{Ind}_{U(I)}\,\chi$ is of finite length and contains a representation π_χ with trivial central character. These are called *simple supercuspidal representations*. They are wild.

For GL_2,

$$U(I) = \begin{pmatrix} 1+pa & b \\ pc & 1+pd \end{pmatrix}, \qquad U(I)^+ = \begin{pmatrix} 1+pa & pb \\ p^2c & 1+pd \end{pmatrix}.$$

In this case, $\chi : U(I) \to \mathbb{C}^\times$ is given by a character of a pro-p group. (This will be useful later.)

For $G(k) = \mathrm{SL}_2(\mathbb{Q}_2)$, $I = U = \left(\begin{smallmatrix} a & b \\ 2c & d \end{smallmatrix}\right)$ has a unique affine generic character: $\left(\begin{smallmatrix} a & b \\ 2c & d \end{smallmatrix}\right) \to (-1)^{b+c}$.

We will like to solve the following problem. Let k be a global field, and S a finite set of places containing all archimedean primes and bad primes of G a reductive group over k. Let T be a finite set of primes disjoint from S. We want to count the number of automorphic representations $\pi = \otimes' \pi_v$ of $G(\mathbb{A})$ such that

- $\pi_\infty = \mathbb{C}$ when $v \mid \infty$ and $G(k_v)$ is compact,
- for $v \in S$, π_v is the Steinberg representation,
- for $v \in T$, π_v is a simple supercuspidal representation,
- for other v, π_v is unramified.

In fact, we will count π with multiplicity: i.e. we will give a formula for $\sum_\pi m(\pi)$ where $m(\pi) = \dim \mathrm{Hom}_{G(k)}(\pi, \mathbb{C})$ for π satisfying the above and $m(\pi) = 0$ otherwise.

10.4. **Haar measures on $G(k)$ or $G(\mathbb{A})$.** The set of left invariant measures on a locally compact topological group G (i.e. those for which $\mu(gE) = \mu(E)$ for all measurable E and $g \in G$) is a cone in $\mathbb{R}$. Given such a measure, $\mu(Eg) = \Delta(g)\mu(E)$ for a character

$$\Delta : G \to \mathbb{R}_+^\times$$

called the *modulus character*. If $\Delta = 1$, μ is called *bi-invariant* and G is called *unimodular*.

There are two situations in which one can conveniently normalize μ. If G is compact then it is customary to take $\int_G \mu = 1$. If G is discrete, then setting $\mu(e) = 1$ (hence $\mu(g) = 1$ for all $g \in G$) one obtains $\int_G f \; d\mu = \sum f(g)$.

If H is a subgroup of G such that $\mathrm{Res}(\Delta_G) = \Delta_H$ then there exists a G-left invariant measure $d\sigma$ on G/H:

$$\int_G f\ dg = \int_{G/H} \left(\int_H f(gh) dh \right) d\sigma.$$

Thus, giving any two of the measures dg, dh and $d\sigma$ determines the third.

Some nice examples:

- If $H \subset G$ is discrete and G/H is compact then putting together the discrete measure on H and the compact measure on G/H determines a measure on G. For example, for $G = \mathbb{R}$ and $H = \mathbb{Z}$ this gives the usual measure on $\mathbb{R}$ for which $[0, 1]$ has measure 1.
- If $H \subset G$ is open and compact and G/H is discrete, again we can combine the measures from above to get a measure on G. An example of this is $G = \mathbb{Q}_p$ and $H = \mathbb{Z}_p$. The resulting measure on G assigns measure 1 to $\mathbb{Z}_p$ (as usual.)

The problem with the adelic case is that both of these options are viable, but they give incompatible measures on G. A simple example of this phenomenon caan be seen when G is finite. Then G is both compact and discrete, $\mu_{dis} = \#G\mu_{cpt}$. (This is why for $G = \mathbb{Z}/n$, one often sees the measure $\sqrt{n}\mu_{cpt} = \frac{1}{\sqrt{n}}\mu_{dis}$ which is self dual used.)

Next time we will discuss how the size of $G(q)$ is determined by the so-called exponents of G. In the case of GL_n,

$$\#\mathrm{GL}_n(q) = q^{n^2}(1 - q^{-1})(1 - q^{-2}) \cdots (1 - q^{-n}).$$

The exponents of GL_n are $1, 2, \ldots, n$.

11. Tuesday December 6

11.1. **The motive of G/k.** Recall that if G_q is quasisplit then G_q contains a Borel B which contains a maximal (not necessarily split) torus T all defined over k. Let $\ell = \dim(Y)$. Then $Y = \mathrm{X}^\bullet(T) \otimes \mathbb{Q}$ is a representation of $\mathrm{Gal}(k^s/k)$ as well as a representation of $N_{G(k^s}(T)/T(k^s) = W$. Hence, $W \rtimes \mathrm{Gal}(k^s/k)$ acts on Y.

The symmetric polynomials in Y fixed by W, $S^\bullet(Y)^W$ is a polynomial ring in ℓ variables. Writing $S^\bullet(Y) = \mathbb{Q}^+ \cdot R_+$,

$$R_+/R_+^2 = \bigoplus_{d \geq 1} V_d$$

where V_d consists of primitive invariant polynomials of degree d. Each V_D is a representation of $\mathrm{Gal}(k^s/k)$ and $\sum \dim(V_d) = \dim Y = \ell$.

For GL_n, V_d is 1-dimensional for $d = 1, 2, \ldots, n$ and $V_d = 0$ for $d > n$. The Galois action is trivial. (The group is split!)

For $U_n(E/k)$, V_d is as in the case of GL_n and $\mathrm{Gal}(E/k)$ acts trivially on V_d for d even. However, for d odd $\mathrm{Gal}(E/k)$ acts non-trivially.

We can now give Steinberg's formula for the size of reductive groups over finite fields.

$$\#G(q) = q^{\dim G} \prod_{d \geq 1} \det(1 - Fq^{-d} \mid V_d).$$

Thus, by the above descriptions,

$$\#\mathrm{GL}_n(q) = q^{n^2}(1 - q^{-1})(1 - q^{-2}) \cdots (1 - q^{-n}),$$

$$\#U_n(q) = q^{n^2}(1-q^{-1})(1+q^{-2})(1-q^{-3})\cdots(1\pm q^{-n}).$$

Since F acts on $\mathbb{Q}(1)$ by q^{-1}, and $V_d(d) = V_d \otimes \mathbb{Q}(1)^{\otimes d}$, Steinberg's formula can be written as

$$\#G(q) = q^{\dim G}\det(1 - F \mid \bigoplus_{d\geq 1} V_d(d)).$$

We define the *motive of* G to be $M = V_d(d)$. If k is local or global we can consider the L-function of this motive. In nonarchimedean local case we define

$$\begin{aligned} L(M,s) &= \det(1 - Fq^{-s} \mid V_d(1-d)^I)^{-1} \\ &= \prod_{d\geq 1}\det(1 - Fq^{d-1-s} \mid V_d)^{-1}. \end{aligned}$$

Set $L(M) = L(M,0) = \prod_{d\geq 1} L(V_d, 1-d)$.

One can ask when $L(M,s)$ has a pole at $s=0$. Note that this is possible only if $d=1$, $V_1^I \neq 0$ and F has eigenvalue 1 which implies that $V_1^{\mathrm{Gal}(k^s/k)} \neq 0$. However, $V_1 = X(Z_G^0)$ so if $Z(G)$ is anisotropic (hence has no split part), $L(M) \neq \infty$. For global k things work out similarly.

11.2. **The mass formula.** Let k be a local field.

Proposition 11.2.1 (Serre)**.** *There is a unique invariant measure $d\nu$ on $G(k)$ such that for every discrete co-compact torsion free subgroup $\Gamma \subset G(k)$,*

$$\int_{\Gamma\backslash G} d\nu = \chi(H^\bullet(\Gamma, \mathbb{Q}))$$

Where χ is the Euler characteristic.

For example:

- If $G(k)$ is compact and $\Gamma = 1$ then $d\nu = \mu_{cpt}$, i.e. $\int_{G(k)} d\nu = 1$.
- If $G = \mathrm{GL}_1$ ($G(k) = k^\times$) and $\Gamma = \pi^{\mathbb{Z}} \hookrightarrow k^\times$, $H^i(\Gamma, \mathbb{Q})$ is 1 if $i = 0,1$ and it is 0 otherwise. So in this case $d\nu = 0$.

Proposition 11.2.2.
- *$d\mu \neq 0$ if and only if G has an anisotropic maximal torus T defined over k. Equivalently, $G(k)$ has a discrete series in $L^2(G, dg)$. If k is p-adic this is equivalent to $Z(G)^0$ being anistropic.*
- *If G is simply connected and k is p-adic then there exist maximal compact subgroups $P_i \subset I \subset G(k)$ for $i = 0,\ldots,\ell$ such that for $S \subset \{0,1,\ldots,\ell\}$, $S \neq \emptyset$, the groups $P_S = \bigcap_{s\in S} P_s$ are parahoric subgroups containing I. Then*

$$d\nu = \sum_S (-1)^{\#S-1}\frac{dg}{\int_{P_S} dg}.$$

Note that $dg/\int_{P_S} dg$ is independant of the choice of measure dg.

This proposition suggests that $L(M)d\nu$ might be well-behaved.

Let's consider the example of SL_2. Then $P_0 = \mathrm{SL}_2(A)$ and $P_1 = \left(\begin{smallmatrix} a & \pi^{-1}b \\ \pi c & d\end{smallmatrix}\right)$. Both of these have index $q+1$ in $I = \left(\begin{smallmatrix} a & b \\ c\pi & d\end{smallmatrix}\right)$. (Note that P_0 and P_1 are conjugate in GL_2, but not in SL_2.) Then

$$\int_{P_0} dg_A = \int_{P_1} dg_A = 1, \qquad \int_I dg_A = \frac{1}{q+1}.$$

Therefore, Serre's result gives

$$d\nu = 2dg_A - \frac{dg_A}{1/(q+1)} = (1-q)dg_A$$

which is negative.[7] In this case $M = \mathbb{Q}(-1)$ ($d = 2$.)

If G is unramified and simply connected then $dg_A = L(M)d\nu$. Note that dg_A is the "compact" measure giving $G(A)$ measure 1, and $d\nu$ is the "discrete" measure.

In the global case let us assume that $G/\mathbb{Q}$ is a simply connected group such that $G(\mathbb{R})$ is compact and G is split over $\mathbb{Q}_p$ for all p. Then $G(\mathbb{A})$ contains $G(\mathbb{Q})$ which is discrete and co-compact, and the group $K = G(\mathbb{R}) \times \prod_p G(\mathbb{Z}_p)$ which is compact and co-discrete.

Define $d\nu$ to be the measure such that $\int_{G(\mathbb{Q})\backslash G(\mathbb{A})} d\nu = 1$. (This is the Tamagawa measure.) Define $d\mu_K$ via $\int_K d\mu_K = 1$.

Proposition 11.2.3. *Let G be as above, $S = \{\infty\}$. Then*

$$dg_k = \frac{1}{2^{\dim M}} L_S(M, 0) \cdot d\nu.$$

Hence $\int_{G(\mathbb{Q})\backslash G(\mathbb{A})} dg_K = 2^{-\dim M} L(M, 0)$.

This proposition is equivalent to the mass formula which states that the finitely many K-orbits each have a finite stabilizer Γ_i and

$$\sum_{G(\mathbb{Q})\backslash G(\mathbb{A})/K} \frac{1}{\#\Gamma_i} = \int_{G(\mathbb{Q})\backslash G(\mathbb{A})} dg_K = \frac{1}{2^{\dim M}} L(M, 0).$$

As an example, let $G = \mathrm{Aut}(\mathbb{O})$. This is a group of type G_2 compact over $\mathbb{R}$ and split over $\mathbb{Q}_p$. Its motive is $M = \mathbb{Q}(-1) \oplus \mathbb{Q}(-5)$ (so $d = 2, 6$), from which we conclude that $L(M, s) = \zeta(s-1)\zeta(s-5)$ and

$$\frac{1}{4} L(M, 0) = \frac{1}{2^6 3^3 7} = \frac{1}{12096}.$$

One can find an orbit and see that its stabalizer is $G_2(2)$ which by Steinberg's formula has order 12096. Therefore, by comparing this with the mass formula, one sees that this is the only orbit. (There is no other known way to prove that this is the only orbit.) We conclude that $G(\mathbb{A}) = G(\mathbb{Q})K$.

Similar analysis for F_4 reveals that $d = 2, 6, 8, 12$ and leads to discovering that there are two orbits.

To generalize the proposition for G not necessarily unramified everywhere, let S be a finite set of places such that G is unramified outside of S. Now define $d\mu_S = d\nu_\infty \times \prod_{p \in S} d\nu_p \times \prod_{p \notin S} dg_A$. Then

$$d\mu_S = \frac{1}{2^{\dim M}} L_S(M, 0) \cdot d\nu.$$

This can also be generalized further. For example, to $G(\mathbb{R})$ non-compact.

[7] The sign of $d\nu$ is $(-1)^\ell$ for these groups. [I don't know what "these" refers to. Perhaps split, semisimple, unramified (?)]

11.3. **Trace formula.** Let k be a global field. Then $G(k) \hookrightarrow G(\mathbb{A})$ is discrete and co-compact, and $G(\mathbb{A})$ acts on $L^2(G(\mathbb{A})/G(k), \mathbb{C})$ with the left action. For $\varphi : G(\mathbb{A}) \to \mathbb{C}$ compactly supported and locally constant, we define

$$\varphi(f)x = \int_{G(\mathbb{A})} f(g^{-1}x)\varphi(g)dg.$$

The operator φdg is a compactly supported measure, so this a trace class, i.e. it has a trace $\operatorname{tr}(\varphi dg \mid L^2)$ which can be shown to equal

$$\sum_{\gamma \in G(\mathbb{Q})//G(\mathbb{Q})} O_\gamma(\varphi dg),$$

$$O_\gamma(\varphi dg) = \int_{G_\gamma(\mathbb{Q})\backslash G(\mathbb{A})} \varphi(g^{-1}\gamma g)dg = \int_{G_\gamma(\mathbb{A})\backslash G(\mathbb{A})} \varphi(g^{-1}\gamma g)dg/dg_\gamma \cdot \int_{G_\gamma(\mathbb{Q})\backslash G_\gamma(\mathbb{A})} dg_\gamma.$$

12. Tuesday December 13

Let G be a simply connected group over $\mathbb{Q}$ with $G(\mathbb{R})$ compact. Let S be a finite set such that G is unramified outside of S. $G(\mathbb{A})$ acts by right translation on $L^2(G(\mathbb{Q})\backslash G(\mathbb{A})) = \widehat{\bigoplus} m(\pi)\pi$ where π runs through unitary representations of $G(\mathbb{A})$. We want to see what possibilities of π appear.

Recall φdg on $G(\mathbb{A})$ with compact support gives an operator $v \mapsto \int_G \varphi(g)gv\, dg$ with a trace:

$$\operatorname{tr}(\varphi \mid L^2) = \sum m(\pi)\operatorname{tr}(\varphi \mid \pi).$$

For any given φ, this sum is finite.

To see this, write $\pi = \bigotimes \pi_v$ with π_v irreducible representations of $G(\mathbb{Q}_v)$. Suppose that $\varphi = \otimes \varphi_v$. It is necessary that $\varphi_v = char(G(\mathbb{Z}_p))$ for almost all primes p. Hence

$$\operatorname{tr}(\varphi \mid \pi) = \prod \operatorname{tr}(\varphi_p \mid \pi_v)$$

In the case that $\varphi_v = char(G(\mathbb{Z}_p))$, this operator is projection to the $G(\mathbb{Z}_p)$ fixed space of π_v, so $\operatorname{tr}(\varphi_p \mid \pi_p)$ is the dimension of the space of π_p fixed by $G(\mathbb{Z}_p)$.

Let us define a particular element $\varphi = \otimes\varphi_v$. For $p \notin S \cup \{\infty\}$ let $\varphi_p = char(G(\mathbb{Z}_p))$, for $v = \infty$ let $\varphi_v = 1 \cdot dg_\infty$, and for $p \in S$ let

$$\varphi_p = \sum_J (-1)^{\#J-1} char(P_J)dg_J$$

where $K_0, \dots, K_\ell \subset I$ are the maximal parahorics containing the Iwahori subgroup I and $P_J = \cap_{j \in J} P_j$ for $i \in J \subset \{0, \dots, \ell\}$ and dg_J gives volume 1 to P_J. Recall that $d\nu = \sum_J (-1)^{\#J-1} dg_J$, so $\varphi_p(1) = d\nu_p$ for $p \in S$.

Similar to the fact that $\operatorname{tr}(char(G(\mathbb{Z}_p))) = \dim \pi^{G(\mathbb{Z}_p)}$, we have

$$\begin{aligned}\operatorname{tr}\Big(\sum_J (-1)^{\#J-1} char(P_J)dg_J\Big) &= \sum (-1)^{\#J-1} \dim \pi^{P_J} \\ &= \begin{cases} (-1)^\ell & \text{if } \pi_p = St \\ 1 & \text{if } \pi_p \text{ is trivial} \\ \chi(H^\bullet(\pi_p)) & \text{if } \pi_p \text{ is unitary.} \end{cases}\end{aligned}$$

Casselman proved that the last case is actually 0.

This particular choice, which we denote, φ_S is called the *pseudo-coefficient*. By the above, if $\mathrm{tr}(\varphi_S \mid \pi) \neq 0$ then $\pi_\infty = \mathbb{C}$, $\pi_p = C$ or St for $p \in S$ and π_p is unramified for $p \notin S$. Therefore,

$$\mathrm{tr}(\varphi_S \mid L^2) = 1 + (-1)^{\ell_p} \sum_\pi m(\pi)$$

where π ranges over all such representations.

The trace formula says that for any φ,

$$\mathrm{tr}(\varphi \mid L^2) = \sum_\gamma \int_{G_\gamma(\mathbb{Q})\backslash G(\mathbb{A})} \varphi(g^{-1}\gamma g) dg$$

for γ ranging through all conjugacy classes in $G(\mathbb{Q})$. Note that when $\gamma = 1$, $G_\gamma = G$, and

$$\int_{G(\mathbb{Q})\backslash G(\mathbb{A})} \varphi_S = \int_{G(\mathbb{Q})\backslash G(\mathbb{A})} \prod_S \nu \prod_{v \notin S} dg_{A_v} = L_S(M_G)\frac{1}{2^{\dim M}}.$$

Claim: $\int_{G_\gamma(\mathbb{Q})\backslash G(\mathbb{A})} \cdots \neq 0$ then γ has finite order. This is because for the test function we have chosen, γ must be both discrete and compact (hence finite) in order for the integral to be nonzero.

Example 12.0.1. Let $G = \mathrm{SL}_2$ over $\mathbb{Q}$. The possible orders of γ are $m = 1, 2, 3, 4, 6$. For $m = 4$ must have that the characteristic polynomial must be $x^4 - 1$. The problem is that there are infinitely many classes with this characteristic polynomial. The way to get around this is to consider *stable classes*.

Let T be a finite set of primes disjoint from S. Recall that $\mathrm{Ind}_{U_p} \chi_p$ is of finite length where $U_p \lhd I_p$ and $\chi_p : U_p \to \mathbb{C}^\times$ is affine generic. If $Z_G(\mathbb{Q}_p) = 1$ then this is irreducible. Let us assume this so that $\pi_p = \mathrm{Ind}_{U_p} \chi_p$ is a simple supercuspidal representation.

Now we define $\varphi_{S,T}$ by replacing φ_p with

$$\varphi_p^* = \begin{cases} \bar{\chi}_p & \text{on } U_p \\ 0 & \text{otherwise} \end{cases}$$

for $p \in T$. By Frobenius reciprocity,

$$\mathrm{tr}(\varphi_p^* \mid \pi_p') = \begin{cases} 1 & \text{if } \pi_p' = \pi_p \\ 0 \text{ otherwise.} & \end{cases}$$

Note that

$$dg_{G(\mathbb{Z}_p)} = \frac{1}{[G(\mathbb{Z}_p) : U_p]} dg_{U_p}$$

and $[G(\mathbb{Z}_p) : U_p] = [G(p) : U(p)]$.