Artin L-Functions and Arithmetic Equivalence (Evan Dummit, September 2013)

1 Intro

- This is a prep talk for Guillermo Mantilla-Soler's talk.
- There are approximately 3 parts of this talk:
  - First, I will talk about Artin L-functions (with some examples you should know) and in particular try to explain very vaguely what "local root numbers" are. This portion is adapted from Neukirch and Rohrlich.
  - Second, I will do a bit of geometry of numbers and talk about quadratic forms and lattices.
  - Finally, I will talk about arithmetic equivalence and try to give some of the broader context for Guillermo's results (adapted mostly from his preprints).
- Just to give the flavor of things, here is the theorem Guillermo will probably be talking about:
  - Theorem (Mantilla-Soler): Let K, L be two non-totally-real, tamely ramified number fields of the same discriminant and signature. Then the integral trace forms of K and L are isometric if and only if for all odd primes p dividing $\text{disc}(K)$ the p-local root numbers of ρ_K and ρ_L coincide.

2 Artin L-Functions and Root Numbers

- Let L/K be a Galois extension of number fields with Galois group G, and ρ be a complex representation of G, which we think of as $\rho : G \to GL(V)$.
- Let $\mathfrak{p}$ be a prime of K, $\mathfrak{P}|\mathfrak{p}$ a prime of L above $\mathfrak{p}$, with $k_L = \mathcal{O}_L/\mathfrak{P}$ and $k_K = \mathcal{O}_K/\mathfrak{p}$ the corresponding residue fields, and also let $G_\mathfrak{P}$ and $I_\mathfrak{P}$ be the decomposition and inertia groups of $\mathfrak{P}$ above $\mathfrak{p}$.
- By standard things, the group $G_\mathfrak{P}/I_\mathfrak{P} \cong G(k_L/k_K)$ is generated by the Frobenius element $\text{Frob}_\mathfrak{P}$ (which in the group on the right is just the standard q-power Frobenius where $q = \text{Nm}(\mathfrak{p})$), so we can think of it as acting on the invariant space $V^{I_\mathfrak{P}}$.
- Definition: With L/K as above and ρ a complex representation of G, the corresponding Artin L-series is $\mathcal{L}(s;\, L/K,\, \rho) = \prod_{\mathfrak{p}\in\mathcal{O}_K} \left[\det(1 - \text{Frob}_\mathfrak{P} \cdot \text{Nm}(\mathfrak{p})^{-s})\right]^{-1}$.
  - Although the notation suggests the definition might depend on our choice of the prime $\mathfrak{P}$ lying over $\mathfrak{p}$, it actually doesn't: Galois acts transitively on the primes over $\mathfrak{p}$ – so choosing a different one will at most change $\text{Frob}_\mathfrak{P}$ by conjugation, which will not affect the determinant.
  - The series gives an analytic function for $\text{Re}(s) > 1$ in the usual way.
  - By the usual character theory, $\mathcal{L}(s;\, L/K,\, \rho)$ only depends on the character χ associated to ρ, so we will often write $\mathcal{L}(s;\, L/K,\, \chi)$ instead (when convenient).
- The general Artin L-series has some special cases which might be more familiar:
  - If we take ρ to be the trivial representation of G, it is easy to see that we end up with the Dedekind zeta function $\zeta_K(s) = \prod_{\mathfrak{p}\in\mathcal{O}_K} \left[1 - \text{Nm}(\mathfrak{p})^{-s}\right]^{-1} = \sum_{\mathfrak{p}\in\mathcal{O}_K} \frac{1}{\text{Nm}(\mathfrak{p})^s}$.
  - If we take $L = \mathbb{Q}(\zeta_m)$, $K = \mathbb{Q}$, so that $G \cong (\mathbb{Z}/m\mathbb{Z})^\times$: then a 1-dimensional representation ρ is the same as a Dirichlet character $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^*$. Class field theory then tells us what Frobenius does, and we see that Artin L-series here reduces to the Dirichlet L-series $L(s,\chi) = \prod_p (1 - \chi(p) \cdot p^{-s})^{-1} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$.
  - Now, both of these special cases have a nice representation as a sum (as well as being nice Euler products). One might ask whether the general Artin L-series also has a nice representation as a sum – unfortunately, it doesn't.
- The L-series behaves nicely in the ways one would expect:
  - If χ_1 and χ_2 are two characters, then $\mathcal{L}(s;\, L/K,\, \chi_1 + \chi_2) = \mathcal{L}(s;\, L/K,\, \chi_1) \cdot \mathcal{L}(s;\, L/K,\, \chi_2)$.

- If $L'/L/K$ is a tower with χ a character of $G(L/K)$, then $\mathcal{L}(s;\, L'/K,\, \chi) = \mathcal{L}(s;\, L/K,\, \chi)$.
- If $L/M/K$ is a tower and χ a character of $G(L/M)$ and χ_* the character induced on $G(L/K)$, then $\mathcal{L}(s;\, L/M,\, \chi) = \mathcal{L}(s;\, L/K,\, \chi_*)$.

- One can generalize the definition further, by making the observation that a representation of $\mathrm{Gal}(L/K)$ is really the same thing as a continuous representation of $\mathrm{Gal}(\bar{K}/K)$ – or, by inducing appropriately, a continuous representation of $G_{\bar{\mathbb{Q}}}$ – so we can extend the definition to give a general Artin L-series attached to an arbitrary Galois representation. (I won't bother to write it down since the flavor is the same as what I already wrote.)
  - A typical example would be: if E is an elliptic curve over K, then the absolute Galois group of K acts on the l-Tate module $T_l(E)$ and gives us a nice l-adic Galois representation, whose Artin L-function we can then write down – in this case, it is closely related to the zeta function of the curve.

- Now, if this product has any business being called an L-series, it should have a functional equation.
  - As usual, we need to find the appropriate gamma functions (and such) to deal with the infinite places. The resulting "infinite part" $\mathcal{L}_\infty$ is basically the same as for other L-series, and we don't actually really care about the details here.
  - We also have to fix any "modularity" issues with the representation ρ, so we also need to find an integer $A(\rho)$ that solves those issues; the resulting $A(\rho)$ will only be divisible by the primes at which ρ is ramified.
  - We obtain a completed Artin L-series $\Lambda(s;\, L/K,\, \chi) = A(\rho)^{s/2} \cdot \mathcal{L}_\infty \cdot \mathcal{L}$, and it satisfies a functional equation $\Lambda(s;\, L/K,\, \chi) = W(\chi) \cdot \Lambda(1-s;\, L/K,\, \bar{\chi})$, where $W(\chi)$ is a constant of absolute value 1.

- This constant $W(\chi)$ (which may be familiar in the context of elliptic curves: it is the "sign of the functional equation") is itself the product of local factors $W(\chi_v)$ called local root numbers: these are what we are interested in.
  - The local root numbers are complex numbers of absolute value 1, and $W(\chi_v) = 1$ whenever v is unramified.
  - There are formulas of Deligne and others which give more explicit formulas for the local root numbers.

3 Quadratic Forms and Lattices

- Now I will discuss elementary things in the geometry of numbers.
- First, recall the basic equivalences from linear algebra regarding quadratic forms and bilinear forms:
  - If q is a quadratic form on a vector space V, then q can be uniquely written as $q(x) = x^T A x$ for a symmetric matrix A. (e.g., $x^2 + 2xy + 2y^2$ is associated to $A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$.)
  - If q is a quadratic form, then $\langle x, y \rangle = \dfrac{q(x+y) - q(x) - q(y)}{2}$ is a symmetric bilinear form with matrix A, and vice versa (given a bilinear form $\langle x, y \rangle$, the associated quadratic form is $\langle x, x \rangle$).
  - I will often implicitly equate all of these ways of thinking about quadratic forms.
  - A quadratic form is nondegenerate if none of the eigenvalues of its associated matrix are zero.

- Also recall that a lattice in $\mathbb{R}^n$ is a subgroup Λ generated by some ($\mathbb{R}$-linearly independent) basis vectors $v_1, \cdots, v_m$.
  - Observe that $\mathbb{R}$-linear independence implies that Λ is discrete, thus avoiding silliness like $\mathbb{Z} + \mathbb{Z}\sqrt{2}$.
  - Usually our lattices will have full rank (i.e., rank n), in which case the lattice has a fundamental domain whose volume will be equal to $|D|^{1/2}$ where $D = \det(\langle v_i, v_j \rangle)$ by standard linear algebra: if A is the change-of-basis matrix sending the v_i to the standard basis elements e_i, then $\mathrm{vol}(\Lambda) = |\det A|$, and $A = D\, D^T$.
  - The lattice carries a natural bilinear form (hence by the above, an associated quadratic form), namely the dot product inherited from $\mathbb{R}^n$. If the lattice has full rank then the associated quadratic form will be nondegenerate.

- Two lattices are isometric if there exists a volume-preserving map between them (i.e., an isometry). Equivalently, they are isometric if there exists an orthogonal matrix which conjugates their corresponding matrices to one another. (This should be familar in the specific example of elliptic curves over $\mathbb{C}$ as lattices in $\mathbb{C}$ up to isometry.)

- If $K/\mathbb{Q}$ is a number field of degree n, let $\sigma_1, \cdots, \sigma_r$ be the real embeddings of K and $\tau_1, \cdots, \tau_s, \bar{\tau}_1, \cdots, \bar{\tau}_s$ be the $2s$ complex embeddings of K.
  - We have a natural bilinear form associated to K (the rational trace form), namely $\langle \cdot, \cdot \rangle : K \times K \to \mathbb{Q}$ defined by $\langle x, y \rangle = \text{tr}_{\mathbb{Q}}(xy) = \sum_{\sigma} \sigma(xy)$.
  - We also have a natural map $j : K \to \mathbb{R}^n$ via $x \mapsto (\sigma_1(x), \cdots, \sigma_r(x), \text{Re}(\tau_1(x)), \cdots, \text{Re}(\tau_s(x)), \text{Im}(\tau_1(x)), \cdots, \text{Re}(\tau_s(x)))$. Since $n = r + 2s$ we see this is a map into $\mathbb{R}^n$.

- Definition: The image of $\mathcal{O}_K$ under this map j yields a rank-n sublattice of $\mathbb{R}^n$, called the Minkowski lattice of K.
  - Up to some factors of 2 (resulting from the fact that we took real and imaginary parts), the fundamental domain of the Minkowski lattice has volume equal to $\sqrt{|D_K|}$, by the remark above, since the entries in the matrix are precisely those used in the definition of the discriminant. (Specifically, the volume is $2^{-s}\sqrt{|D_K|}$.)
  - Example: The Gaussian integers inside $\mathbb{C} = \mathbb{R}^2$ are the Minkowski lattice of $\mathbb{Q}(i)$. The discriminant of this number field is -4, and the volume of the fundamental domain is 1, and indeed $1 = 2^{-1} \cdot \sqrt{|-4|}$.

- Definition: The integral trace form is the restriction of the rational trace form to the ring of integers of K: thus, it is the map $\langle \cdot, \cdot \rangle : \mathcal{O}_K \times \mathcal{O}_L \to \mathbb{Z}$ with $\langle x, y \rangle = \text{tr}_{K/\mathbb{Q}}(xy)$.
  - The signature of the integral trace form is equal to the number of real embeddings of K.
  - The integral trace form carries strictly more information than the rational trace form.

4 Arithmetic Equivalence (and related things)

- Perlis in the 1970s proved that if two number fields have the same zeta function (such fields are called arithmetically equivalent), then their degrees, discriminants, and signatures are equal.
  - Arithmetically fields are not necessarily isomorphic: for example, there exists a pair of nonisomorphic fields of degree 8 which are arithmetically equivalent.
  - Indeed, Perlis gave a criterion for arithmetic equivalence: if K, L are number fields and N is the Galois closure of $KL/\mathbb{Q}$, then K and L are arithmetically equivalent iff $\text{Gal}(N/K)$ and $\text{Gal}(N/L)$ are "almost conjugate" subgroups of $\text{Gal}(N/\mathbb{Q})$.

- The context is as follows: If $K/\mathbb{Q}$ has degree n, then ζ_K is the L-function of the permutation representation ρ_K of $G_{\mathbb{Q}}$, so we can think of ρ_K as an element of $H^1(\mathbb{Q}, S_n)$. The inclusion $\iota : S_N \to O_n(\bar{\mathbb{Q}})$ induces a map of pointed sets $\iota^* : H^1(\mathbb{Q}, S_n) \to H^1(\mathbb{Q}, O_n)$ (where O_n is the group of orthogonal matrices).

- But the cohomology group $H^1(\mathbb{Q}, O_n)$ classifies isometry classes of nondegenerate rational quadratic forms of dimension n.
  - This is an example of Galois descent; here is a sketch of the argument from Serre's book on local fields book.
  - Let V be any $\mathbb{Q}$-vector space and $x \in [\otimes^p V] \otimes [\otimes^q V^*]$ be a fixed tensor of type (p, q)
  - Define the set "$E(K/\mathbb{Q})$" of $\mathbb{Q}$-isomorphism classes of pairs (V', x') that are K-isomorphic to (V, x) – that is, if they are isomorphic after tensoring with K.
  - Also define A_K to be the group of K-automorphisms of (V_K, x_K) obtained by tensoring with K.
  - Then it is a moderately exciting cocycle computation to construct a bijection between $E(K/k)$ and $H^1(\text{Gal}(K/\mathbb{Q}), A_K)$.
  - In our case, if we take x to be a nondegenerate rational quadratic form, then $E(K/\mathbb{Q})$ is the set of classes of quadratic forms that are K-isomorphic to it, and the group A_K is the group of orthogonal matrices with K-coefficients.

- So now we can ask: what quadratic form corresponds to $\iota^*(\rho_K)$?
  - The answer turns out to be: it is the rational trace form $\mathrm{tr}(xy)$. By invoking Chebotarev, we see that two arithmetically equivalent number fields will have the same rational trace form, up to some orthogonal matrix (i.e., up to isometry).
  - The converse to this result is not true: two number fields can have the same integral trace form, but not even the same discriminant.
- At this point, there are a variety of questions that one might ask: What hypotheses are needed to make "equal trace forms" imply "arithmetically equivalent"? And exactly what else does the integral trace form tell us?
  - These and related questions are what Guillermo will be talking about.
- <u>Theorem</u> (Mantilla-Soler): Let K, L be two non-totally-real, tamely ramified number fields of the same discriminant and signature. Then the integral trace forms of K and L are isometric if and only if for all odd primes p dividing $\mathrm{disc}(K)$ the p-local root numbers of ρ_K and ρ_L coincide.
  - The punchline is: a particular Stiefel-Whitney invariant gives a connection between the root numbers and the integral trace form. Then everything (seems to?) reduce down to using some formulas for the root numbers and some group cohomology arguments.