18.785: Analytic Number Theory, MIT, spring 2007 (K.S. Kedlaya)
Artin L-functions

This unit begins the fourth and final part of the course. In this part, we describe some other types of L-functions that are used for arithmetic purposes. This merely scratches the surface of what is now a rather vast theory of L-functions; §5 of Iwaniec-Kowalski gives a somewhat less narrow account.

Some of this discussion will only make sense if you have studied some algebraic number theory. The book I used to teach 18.786 last year is a reasonable place to start: it is Janusz, *Algebraic Number Fields*. I'm also presuming you are happy with representation theory of finite groups at the level of 18.702.

1 Frobenius elements of Galois groups

Let K be a finite Galois extension of $\mathbb{Q}$, and put $G = \mathrm{Gal}(K/\mathbb{Q})$. Let $\mathfrak{o}_K$ be the ring of integers of K; that is, $\alpha \in \mathfrak{o}_K$ if and only if α is a root of a monic polynomial with coefficients in $\mathbb{Z}$.

A prime p is said to be *ramified (in K)* if the ring $\mathfrak{o}_K/p\mathfrak{o}_K$ is not reduced (i.e., has nilpotent elements). For instance, if $K = \mathbb{Q}(i)$, then $\mathfrak{o}_K = \mathbb{Z}[i]$, and the only ramified prime is $p = 2$. In general, only finitely many primes are ramified; they are the ones dividing the discriminant of $K/\mathbb{Q}$.

On $\mathfrak{o}_K/p\mathfrak{o}_K$, one has both an action of G and a Frobenius map $x \mapsto x^p$.

Lemma 1. *There exists $g \in G$ such that $x^p = x^g$ has a nonzero solution $x \in \mathfrak{o}_K/p\mathfrak{o}_K$. Moreover, if p is unramified, then the set of such $g \in G$ forms a single conjugacy class.*

Any such g is called a *Frobenius element* for the prime p.

One can also define Frobenius elements for the infinite place: given an embedding of K into $\mathbb{C}$, complex conjugation on $\mathbb{C}$ induces an automorphism of K. Any such automorphism is called a *Frobenius element* for the infinite place, or more simply a *complex conjugation* on K.

2 Linear representations and L-functions

Let $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ be a linear representation, with character $\chi : G \to \mathbb{C}$; that is, $\chi(g) = \mathrm{Trace}\,\rho(g)$. We define the *(incomplete) Artin L-function* associated to ρ as the function

$$L(\rho, s) = \prod_p \det(1 - \rho(\mathrm{Frob}_p)p^{-s})^{-1},$$

where we only allow p to run over unramified primes, and Frob_p means any Frobenius element of p; it doesn't matter which one because they are all conjugate. (There is a correct way to put in the ramified primes: you only look at the determinant of the action of ρ on the

invariants under an inertia group corresponding to p. If you don't know what that means, never mind.)

For example, if we take $\rho : G \to \mathrm{GL}_1(\mathbb{C})$ to be the trivial representation, then $L(\rho, s)$ equals the Riemann zeta function with a few Euler factors missing. Note also that

$$L(\rho_1 \oplus \rho_2, s) = L(\rho_1, s)L(\rho_2, s).$$

Also, if K' is another Galois extension of $\mathbb{Q}$ contained in K, ρ factors through $\mathrm{Gal}(K'/\mathbb{Q})$, then the L-functions computed in terms of K and K' agree, in the sense that for each p which appears in both products (which is all but finitely many), the Euler factor is the same.

Note that

$$\left|1 - \det(1 - \rho(\mathrm{Frob}_p)p^{-s})^{-1}\right| = O(p^{-s}),$$

where the implied constant depends on the dimension of ρ. Consequently, the Euler product converges absolutely for $\mathrm{Re}(s) > 1$, uniformly for $\mathrm{Re}(s) \geq 1 + \epsilon$, and never vanishes in this region.

3 Artin's conjecture

The following is one of the deepest conjectures in modern number theory.

Conjecture 2 (Artin)**.** *The function $L(\rho, s)$ extends to a meromorphic function on all of $\mathbb{C}$, with no poles away from $s = 1$, and order of pole at $s = 1$ equal to the number of copies of the trivial representation contained in ρ (or equivalently, $1/|G| \sum_{g \in G} \chi(g)$).*

There are various stronger versions of this conjecture. For instance, there is also supposed to be a functional equation relating $L(\rho, s)$ with $L(\overline{\rho}, 1 - s)$. More comprehensively, there should be some sort of analogue for $L(\rho, s)$ of the function θ that we used for the proof of the functional equation of the Riemann zeta function. (Such a thing would be an example of a *modular form*.)

Here are some results about Artin's conjecture.

1. It holds for ρ trivial, by reducing to the Riemann zeta function.

2. It holds for ρ of dimension 1: by the Kronecker-Weber theorem, any such ρ is a Dirichlet character, and so we get a Dirichlet L-function.

3. It holds if ρ is induced by a permutation representation (e.g., the regular representation). In this case, this follows from the analytic properties of Dedekind ζ-functions. More generally, it holds if ρ is obtained by induction from a one-dimensional representation; see below.

4. If ρ has dimension 2, then either the image of ρ is solvable, in which case the conjecture is a theorem of Langlands and Tunnell, or the image is the icosahedral group A_5. In the latter case, the conjecture is known when ρ is *odd* (any complex conjugation has determinant -1) by recent results from the theory of modular forms (resolution of Serre's conjecture).

4 Induced representations

Let H be a subgroup of G and let $\sigma : H \to \mathrm{GL}_m(\mathbb{C})$ be a linear representation. Let V be the set of functions $f : G \to \mathbb{C}^m$ such that $h(f(g)) = f(hg)$ for all $h \in H$. This forms a representation of G notated $\mathrm{Ind}_H^G(\sigma)$. For instance, if σ is the trivial representation, then $\mathrm{Ind}_H^G(\sigma)$ is the linear representation given by the permutation representation of G on the cosets of H.

Theorem 3 (Artin)**.** *Every character of G is a $\mathbb{Q}$-linear combination of characters of induced representations from cyclic subgroups.*

Proof. By orthogonality of characters, it suffices to check that for each conjugacy class in G, one can construct a linear combination of induced representations whose character is nonvanishing except on that class. Let g be an element of the class, generating the cyclic subgroup H. Then there is a linear combination of one-dimensional representations of H whose character is nonzero only on g; inducing those to G gives the linear combination we seek. □

5 Chebotarev's density theorem

Here is a weaker form of Artin's conjecture that can be proved, but even this requires some heavy machinery.

Theorem 4. *For any ρ, the L-function $L(\rho, s)$ extends to a meromorphic function on a neighborhood of $\mathrm{Re}(s) \geq 1$. Moreover, on the line $\mathrm{Re}(s) = 1$, $L(\rho, s)$ is nonvanishing for $s \neq 1$, and for $s = 1$, the order of vanishing of $L(\rho, s)$ is $-1/|G| \sum_{g \in G} \chi(g)$. (In other words, there is a pole at $s = 1$ of order equal to the multiplicity of the trivial representation in ρ.)*

Sketch of proof. One first proves the claim for $\rho = \mathrm{Ind}_H^G \sigma$ for any abelian subgroup H of G and any one-dimensional representation $\sigma : H \to \mathrm{GL}_1(\mathbb{C})$. This requires class field theory in general, because one has to first write σ as a ray class character. See Janusz's book for details.

By Artin's theorem, for any given ρ, we deduce the claim for $\rho^{\oplus m}$. To deduce the claim for ρ, we may reduce to the case where ρ has no trivial subrepresentations; then $L(\rho, s)^m$ extends holomorphically to a neighborhood of $\mathrm{Re}(s) \geq 1$, without vanishing anywhere. Consequently, we can take the m-th root in a neighborhood of any s with $\mathrm{Re}(s) = 1$; by choosing the right root, we get a function that patches together with the function defined on $\mathrm{Re}(s) > 1$. □

By imitating the proof of Dirichlet's theorem, we deduce the following theorem of Chebotarev, which can be considered a nonabelian generalization of Dirichlet's theorem.

Theorem 5 (Chebotarev)**.** *For any conjugacy class C of G, the set of primes p for which $\mathrm{Frob}_p \in C$ has natural density $\#C/\#G$.*

It is also possible to prove this without using class field theory, as in Chebotarev's original work. (In fact, this result was one of the original impetuses for class field theory to be developed!) There is a nice explanation of this by Lenstra and Stevenhagen, available online at:

`http://www.math.leidenuniv.nl/~hwl/papers/cheb.pdf`

6 Exercises (optional)

Remember, there are no more problem sets, so don't bother turning these in.

1. Suppose that G is a group in which any two elements that generate the same cyclic subgroup are conjugate (e.g., S_n). Prove that every character of G is a $\mathbb{Q}$-linear combination of permutation representations. For such G, you don't need class field theory to prove Chebotarev as above, just the analytic properties of Dedekind zeta functions.

2. Let P be a polynomial with Galois group G. Use Chebotarev's theorem to compute the density of primes modulo which P factors into irreducibles of degrees $d_1, \ldots, d_k$. (This was proved by Frobenius, who then made a conjecture that became Chebotarev's theorem.)