

Lecture 17

In the final lectures, we shall give a basic treatment of Artin L functions to introduce the reader to the ideas behind Stark's Conjectures. For a very thorough treatment of these ideas, see Tate *Les conjectures de Stark sur les fonctions L d'Artin en $s=0$: notes d'un cours Orsay [de] John Tate*, Birkhäuser, Progress in Mathematics.

Let $\mathbb{Q} \subseteq k$ be a Galois extension of degree n with Galois group G which is necessarily finite of order n . Let A denote the ring of algebraic integers in k . G acts on A , so for every prime number p , G acts on A/pA . Therefore, G permutes the prime ideals P of A of characteristic p .

Proposition 81. *G permutes the primes P of characteristic p transitively.*

Proof. Fix a prime ideal P of A of characteristic p . Let $I = \prod_{P_i \neq P} P_i$ where the product is taken over all prime ideals P_i of characteristic p such that $P_i \neq P$. Since each prime ideal of characteristic p is maximal, we see that $P + I = A$. Fix $\alpha \in P$ and $\beta \in I$ such that $\alpha + \beta = 1$. It follows that $\alpha \notin P_i$ for any i . For any $\sigma \in G$, $\sigma(\alpha) \in \sigma(P)$ and if $P_i \neq \sigma(P)$ then $\sigma(\alpha) \notin P_i$. Now, $p\mathbb{Z} = P \cap \mathbb{Z}$ and this ideal contains $a = \mathbb{N}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$. Thus, a is contained in exactly the primes P_i which are conjugate to P . Since $a \in p\mathbb{Z}$, we see that a lies in all the P_i , as desired. \square

Corollary 82. *In the prime factorization $pA = \prod_{i=1}^g P_i^{e_i}$, let $f_i = \deg(P_i) = (A/P_i : \mathbb{Z}/p\mathbb{Z})$. Then the e_i and f_i are independent of i and $n = efg$ where e and f denote the common value of e_i and f_i , respectively.*

Proof. The fact that the e_i and f_i are independent of i follows immediately from the fact that the P_i are all conjugate. The fact that $n = efg$ follows from the fact that the extension $\mathbb{Q} \subseteq k$ is Galois. \square

Corollary 83. *Let P be a fixed prime ideal of A dividing p . Let $G_P = \{\sigma \in G : \sigma(P) = P\}$ which is a subgroup of G of order ef . For an element τ of the coset space G/G_P , the ideal $P' = \tau(P)$ is a well-defined conjugate of P , and $G_{P'} = \tau G_P \tau^{-1}$ in G .*

Proof. This follows from the standard results regarding the transitive action of a group on a set. \square

With the notation of the corollary, we see that G_P acts on the finite field A/P since it stabilizes P . Let I_P denote the inertia subgroup, i.e., the kernel of this action. Then there is an exact sequence

$$1 \rightarrow I_P \rightarrow G_P \xrightarrow{\beta} \text{Aut}(A/P)$$

by definition of I_P . Since A/P is finite of order p^f , the Frobenius automorphism $F : A/P \rightarrow A/P$ given by $\alpha \mapsto \alpha^p$ is a generator of $\text{Aut}(A/P)$. Thus, $\text{Aut}(A/P)$ is cyclic of order f .

Theorem 84. *The map β is surjective. Consequently, I_P has order e . In particular, if p does not divide the discriminant d_k of k , then I_P has order 1.*

Proof. We shall only prove the result under the additional hypotheses of Corollary 32, i.e., when $k = \mathbb{Q}(\alpha)$ with $\alpha \in A$ and p does not divide the index $(A : \mathbb{Z}[\alpha])$. By Corollary 32

$$A/pA = \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] = (\mathbb{Z}[x]/h(x))/p(\mathbb{Z}[x]/h(x)) = (\mathbb{Z}/p\mathbb{Z})[x]/\tilde{h}(x)$$

where $\tilde{h}(x)$ denotes the reduction of $h(x)$ modulo p . The irreducible factorization of $\tilde{h}(x)$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ has the form

$$\tilde{h}(x) = \prod_{i=1}^g h_i(x)^e \quad (1)$$

where each $h_i(x)$ has degree f . Since every $\sigma(\alpha)$ satisfies $h(x)$, G permutes the zeroes of $h(x)$. G acts transitively on the zeroes: if α' is another root, then $k = \mathbb{Q}(\alpha')$ and the map $\alpha \mapsto \alpha'$ determines an element of G . Furthermore, G acts simply-transitively on the zeroes, that is, for each root α_i there exists a unique $\sigma \in G$ such that $\sigma(\alpha) = \alpha_i$. This follows from the fact that $h(x)$ has exactly n distinct zeroes where $n = (k : \mathbb{Q}) = \#(G)$, and G acts transitively on the zeroes.

There are $n = efg$ distinct zeroes of $h(x)$ over $\overline{\mathbb{Q}}$. The fact that \mathbb{F}_p is perfect and the factorization 1 implies that there are exactly fg distinct zeroes of $\tilde{h}(x)$ over $\overline{\mathbb{F}_p}$, each of multiplicity e . By Corollary 32, the prime ideal P corresponds to one of the $h_i(x)$. Assume without loss of generality that P corresponds to $h_1(x)$. Let $\tilde{\alpha}_1$ denote the reduction modulo p of α to a zero of $h_1(x)$. For $\sigma \in G$, σ is an element of G_P if and only if $\sigma(\alpha)$ reduces to a zero of $h_1(x)$. Also, $\sigma \in I_P$ if and only if $\sigma(\alpha)$ is one of the e zeroes in characteristic 0 which reduces to $\tilde{\alpha}_1$. Since G acts simply transitively, this implies that $\#(I_P) \leq e$. $\#(I_P) \geq e$ because $\#(G_P) = ef$ and $\#(\text{Aut}(A/P)) = f$. Thus, $\#(I_P) = e$ and β must be surjective. If p does not divide d_k , then Corollary 32 implies that $e = 1$, proving the final claim. \square

Corollary 85. *There exists a coset $I_P F$ of I_P in G_P such that the action of any $\sigma \in I_P F$ on A/P is given by $\alpha \mapsto \alpha^p$.*

Proof. This follows from the fact that the Frobenius automorphism generates $\text{Aut}(A/P)$ and the sequence

$$1 \rightarrow I_P \rightarrow G_P \xrightarrow{\beta} \text{Aut}(A/P) \rightarrow 1$$

is exact. \square

Corollary 86. *If p does not divide d_k , so that $e = 1$ and $I_P = 1$, then the decomposition group G_P is cyclic, with a canonical generator F_P which satisfies the condition*

$$F_P(\alpha) \equiv \alpha^p \pmod{P}$$

Proof. Immediate. \square

If $P' = \tau(P)$ for some $\tau \in G$, then $G_{P'} = \tau G_P \tau^{-1}$ and $F_{P'} = \tau F_P \tau^{-1} \in G$. Thus, for all $p \nmid d_k$ we get a conjugacy class $F_P = \{F_{P'}\}$ in G .

Example. Let $\zeta = \zeta_m = e^{2\pi i/m}$ be a fixed primitive m th root of unity. The minimal polynomial of ζ is denoted $\phi_m(x)$ and divides $x^m - 1$. If $k = \mathbb{Q}(\zeta)$ then the extension

$\mathbb{Q} \subset k$ is Galois with Galois group $G \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$. (Note that if F is any field such that $\text{char}(F) \nmid m$ then we may consider the extension $F \subset F(\zeta_m)$ then the Galois group G embeds in $(\mathbb{Z}/m\mathbb{Z})^\times$ by mapping $\sigma \rightarrow a$ if $\sigma(\zeta_m) = \zeta_m^a$.) Gauss showed that over \mathbb{Q} the embedding $G \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$ is a surjection, i.e., that $\phi_m(x)$ is irreducible over \mathbb{Q} . (This is not true for an arbitrary field F .) We know that G is abelian, so for unramified p we get an element F_p which is F_P for any P dividing p . For $\alpha \in A$, the fact that $F_P(\alpha) \equiv \alpha^p \pmod{P}$ for every $P \mid p$ implies that $F_p(\alpha) \equiv \alpha^p \pmod{pA}$. If $p \nmid m$, then p is unramified in k , in fact, $p \nmid \text{disc}(\mathbb{Z}[\zeta_m])$. Via the map $G \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$, F_p is some class in $(\mathbb{Z}/m\mathbb{Z})^\times$. It is the class of a where $F_p(\zeta) = \zeta^a$. Since $F_p(\zeta) \equiv \zeta^p \pmod{pA}$ it follows that $a = p$ so that F_p is the class of p in $(\mathbb{Z}/m\mathbb{Z})^\times$.

The Dirichlet Density Theorem states that, as $s \rightarrow 1$,

$$\sum_{p \equiv a \pmod{m}} \frac{1}{p^s} \sim \frac{1}{\phi_m(s)} \log\left(\frac{1}{s-1}\right)$$

and it follows from the above discussion that we can state this theorem in terms of the Galois group G , as

$$\sum_{p \equiv a \pmod{m}} \frac{1}{p^s} = \sum_{\substack{p \text{ with} \\ F_p = a \in G}} \frac{1}{p^s}$$

We return to the general case where $\mathbb{Q} \subseteq k$ is any (finite) Galois extension. Fix a general conjugacy class $C \subseteq G$. Can we find an unramified prime p such that $F_p \in C$?

Theorem 87. (Chebotarev) *There are infinitely many primes $p \nmid d_k$ with $F_p \in C$ and as $s \rightarrow 1$*

$$\sum_{\substack{p \text{ with} \\ F_p \in C}} \frac{1}{p^s} \sim \frac{\#(C)}{\#(G)} \log\left(\frac{1}{s-1}\right)$$

Corollary 88. *There are infinitely many primes $p \nmid d_k$ with $F_p = 1$ in G for some (equivalently, for every) P dividing p , i.e., $p = P_1 \cdots P_n$ splits completely. These have density $1/\#(G)$.*

Next, we develop the higher analogs of the $L(\chi, s)$.

Definition. Let k be a finite Galois extension of \mathbb{Q} . We define the *Artin L-function* of k , as follows. Let G be the Galois group of k over \mathbb{Q} and let (V, ρ) be a finite-dimensional, complex representation of G . That is, V is a finite-dimensional, complex vector space and $\rho : G \rightarrow GL(V)$ is a homomorphism of groups. For a prime number $p \nmid d_k$, we have the conjugacy class F_p in G . For any element $F_P \in F_p$, the element $\rho(F_P)$ in $GL(V)$ has finite order. This implies that $\rho(F_P)$ is semisimple and determined up to conjugacy by its characteristic polynomial. Thus, for each such p the assignment

$$\det(1 - F_p t | V) = 1 - \text{Tr}(F_p | V)t + \cdots + (-1)^n \det(F_p | V)t^n$$

is well-defined, where $n = \dim(V) = \deg(\det(1 - F_p t | V))$.

We define $L(V, s)$ as a product over all primes p ,

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

where V^{I_P} denotes the subspace of V fixed by $\rho(I_P)$. The product converges absolutely and is nonzero in the region $\operatorname{Re}(s) > 1$.

Example. Let $V = \mathbb{C}$ and $\rho(\sigma) = 1$ for all $\sigma \in G$. (This is the *trivial representation* of G .) Then for every p

$$\det(1 - F_P p^{-s} | V^{I_P})^{-1} = (1 - p^{-s})^{-1}$$

as every $V^{I_P} = \mathbb{C}$. Thus, $L(\mathbb{C}, s) = \zeta(s)$.

Example. Let $k = \mathbb{Q}(\zeta)$ where $\zeta = \zeta_\ell$ is a primitive ℓ th root of unity. Then $G = (\mathbb{Z}/\ell\mathbb{Z})^\times$. If $\chi : G \rightarrow \mathbb{C}^\times$ is a character, then the fact that $GL_1(\mathbb{C}) = \mathbb{C}^\times$ implies that we may think of χ as a 1-dimensional representation. It follows that the L function of the representation is exactly the L function of the character, as defined before. In particular, we see that the L function of the representation has an analytic continuation to all of \mathbb{C} and satisfies a functional equation.

Artin Conjecture. With notation as above, $L(V, s)$ has a meromorphic continuation to all of \mathbb{C} with a pole of order $\dim(V^G)$ at $s = 1$ and no other poles.

Brauer proved that $L(V, s)$ has a meromorphic continuation to all of \mathbb{C} . There are a few facts which allow us to reduce to certain basic cases.

Fact 1. If $V = V_1 + V_2$ as a linear representation of G , then

$$L(V, s) = L(V_1, s)L(V_2, s)$$

To see this, note that $V^{I_P} = V_1^{I_P} + V_2^{I_P}$ since the representation on V takes the form

$$\sigma \mapsto \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$$

This form also shows that the characteristic polynomial of $F_P | V^{I_P}$ is the product of the characteristic polynomials of the $F_P | V_i^{I_P}$.

Fact 2. $L(\mathbb{C}, s) = \zeta(s)$.

Fact 3. Let $V = \bigoplus_{g \in G} \mathbb{C}e_g$ denote the regular representation of G . Then

$$L(V, s) = \zeta_k(s)$$

To see this, note that for $p \nmid d_k$, the factor of $\zeta_k(s)$ corresponding to p can be written $((1 - p^{-fs})^{n/f})^{-1}$ where $f = \#(G_P)$ and $n = \#(G)$. As noted previously, F_P has order f in G : as a permutation of G , left multiplication by F_P has a cycle decomposition with n/f cycles, each of length f .

Fact 4. (Frobenius) The regular representation of G can be expressed in the form

$$V = \bigoplus_{\text{irred. } \nu} \dim(V) \nu$$

where the sum is taken over all irreducible representations of G . It follows from Facts 1 and 3 that

$$\zeta_k(s) = \prod_{\text{irred. } V} L(V, s)^{\dim(V)} = \zeta(s) \prod_{V \neq \mathbb{C}} L(V, s)^{\dim(V)}$$

This is known as the Artin factorization of $\zeta_k(s)$.

Example. The symmetric group S_3 has three irreducible representations: the trivial representation, the one-dimensional representation given by $\chi = \text{sgn}$, and a two-dimensional representation which we denote V . Frobenius' formula tells us that (in the representation ring) the regular representation is of the form $1 + \chi + 2V$. If k is a number field with Galois group $G = S_3$, then Fact 4 implies that $\zeta_k(s) = \zeta(s)L(\chi, s)L(V, s)^2$.

Theorem 89. (Brauer) $\zeta_k(s)/\zeta(s)$ is an entire function of s .

Lecture 18

Last lecture, we restricted our attention to the case of Galois extensions. Now, we wish to see what we can say in the general case.

Let k be a number field. Let K denote the Galois closure of k in $\overline{\mathbb{Q}}$, that is, K is the smallest subfield of $\overline{\mathbb{Q}}$ which contains all the conjugates of k . Then K is finite and Galois over \mathbb{Q} , say with Galois group G . Let H denote the subgroup of G which fixes k . The coset space G/H is a finite set which is in bijection with the set

$$\text{Hom}_{\mathbb{Q}}(k, \mathbb{C}) = \text{Hom}_{\mathbb{Q}}(k, \overline{\mathbb{Q}}) = \text{Hom}_{\mathbb{Q}}(k, K)$$

Note that the bijection depends on a fixed inclusion of k in K . This set has order $n = (k : \mathbb{Q})$. Also, there is an action of $\sigma \in G = \text{Aut}_{\mathbb{Q}}(K)$ on $\alpha \in \text{Hom}_{\mathbb{Q}}(k, K)$ given by $\sigma(\alpha) = \sigma \circ \alpha$.

If $k = \mathbb{Q}(\alpha)$, then the coset space G/H is in bijection with the n zeroes of $f_{\alpha}(x)$ in $\overline{\mathbb{Q}}$ by the assignment $\sigma \mapsto \sigma(\alpha)$. If we assume that $p \nmid \text{disc}(f)$, then distinct zeroes in characteristic zero pass to distinct zeroes modulo p , so this set is in bijection with the n zeroes of $f_{\alpha}(x) \pmod{p}$ in $\overline{\mathbb{F}}_p$. In this set of zeroes, F_P acts by $\alpha_i \mapsto \alpha_i^p$.

Assume that p is a prime number such that $p \nmid d_K$ so that p is unramified in K and $pA_K = P_1 \cdots P_g$. As in the discussion of Lecture 17, G permutes the P_i transitively, and if $P = P_1$, then the stabilizer of P is $G_P = \langle F_P \rangle \cong \mathbb{Z}/f\mathbb{Z}$. We claim (without proof) that the factors of p in k are in bijection with the elements in the (finite) double-coset space $G_P \backslash G/H$. We may think of $G_P \backslash G/H$ either as the set of G_P -orbits on G/H or as the H -orbits on $G_P \backslash G$. Under this correspondence, if a factor \mathfrak{p} of pA_k corresponds to the double coset $G_P gH$, then the degree of \mathfrak{p} is exactly the number of single G/H cosets in $G_P gH$.

We rewrite the Euler factor of p in $\zeta_k(s)$. Assume that P_1, \dots, P_g are the factors of pA_k with degrees f_1, \dots, f_g , respectively. Then the Euler factor corresponding to p is

$$\prod_{i=1}^g (1 - p^{-f_i s})^{-1} = \det(1 - F_P p^{-s} | \mathbb{C}[G/H])^{-1}$$

as the Frobenius element F_p has a block form

$$\begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_g \end{pmatrix}$$

where A_i is the $f_i \times f_i$ square matrix

$$\begin{pmatrix} 0 & 0 & \cdots & 1 \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

We define the *induced representation* of G as

$$\text{Ind}_H^G(\mathbb{C}) = \mathbb{C}[G/H]$$

Then

$$\text{Ind}_H^G(\mathbb{C}) = \bigoplus_{\substack{\text{irred. reps.} \\ V \text{ of } G}} \dim(V^H)V$$

by Frobenius reciprocity, as

$$\text{Hom}_G(V, \text{Ind}_H^G(\mathbb{C})) = \text{Hom}_H(\text{Res}V, \mathbb{C})$$

It follows that

$$\zeta_k(s) = L(\text{Ind}_H^G(\mathbb{C}), s) = \prod_{\substack{\text{irred. reps.} \\ V \text{ of } G}} L(V, s)^{\dim(V^H)}$$

Problem. Can we find two non-isomorphic (i.e., not conjugate in $\overline{\mathbb{Q}}$) number fields k and k' with the same zeta function? This occurs if and only if every p decomposes identically in A_k and $A_{k'}$. Suppose that two such fields exist with the same Galois closure K . We must have $(k, \mathbb{Q}) = (k', \mathbb{Q})$ and they must have the same number of real places, complex places and roots of unity. By the class number formula, this implies that $hR = h'R'$. It is not necessarily true, however, that $h = h'$. We know that k and k' are isomorphic subfields of K if and only if the corresponding subgroups H and H' are conjugate in G . (Under these conditions, we say that H and H' are *globally conjugate*.) By our previous work, $\zeta_k(s) = \zeta_{k'}(s)$ if and only if $\text{Ind}_H^G(\mathbb{C}) \cong \text{Ind}_{H'}^G(\mathbb{C})$ as representations of G . This occurs if and only if, for every $\sigma \in G$, $\text{Tr}(\sigma : \text{Ind}_H^G(\mathbb{C})) = \text{Tr}(\sigma : \text{Ind}_{H'}^G(\mathbb{C}))$. If we write $\text{Ind}_H^G(\mathbb{C}) = \bigoplus_{G/H} \mathbb{C}e_{gH}$, then $\sigma(e_{gH}) = e_{\sigma gH}$ so that

$$\begin{aligned} \text{Tr}(\sigma : \text{Ind}_H^G(\mathbb{C})) &= (\text{the number of cosets } gH \text{ such that } \sigma gH = gH) \\ &= (\text{the number of cosets } gH \text{ such that } g^{-1}\sigma gH = H) \\ &= \#(\{g : g^{-1}\sigma g \in H\} / \{g \sim g' \Leftrightarrow gH = g'H\}) \\ &= \#(C_\sigma \cap H) / (\#(H) / \#(Z_\sigma(H))) \end{aligned}$$

Thus, $\zeta_k(s) = \zeta_{k'}(s)$ if and only if, for every conjugacy class C_σ in G , $\#(C_\sigma \cap H) = \#(C_\sigma \cap H')$. (Under these conditions, we say that H and H' are *locally conjugate*.)

We now give two examples of subgroups $H, H' \subset G$ which are locally conjugate but not globally conjugate.

Example. Let $G = S_6$ and consider the subgroups

$$\begin{aligned} H &= \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \\ H' &= \{e, (1\ 2)(3\ 4), (1\ 2)(5\ 6), (3\ 4)(5\ 6)\} \end{aligned}$$

The subgroups each have order 4, and they have the same cycle structure (2,2,1,1), and are therefore locally conjugate. (It is straightforward to verify this fact directly, as a conjugacy class is uniquely determined by the cycle structure of a representative.) However, H fixes the numbers 5 and 6, while H' fixes nothing, so H and H' are not globally conjugate.

Example. Let $G = \text{GL}_3(\mathbb{F}_2) = \text{GL}(V)$ where V is a three-dimensional vector space over \mathbb{F}_2 . Then G has order 168. If we let P denote the stabilizer of a line and P' the stabilizer of a plane, then P and P' each have index 7 in G . In fact, P and P' are locally conjugate, but they are not globally conjugate.