Introduction to Algebraic Number Theory
Lecture 27

Andrei Jorza

10 ζ-functions and L-functions

(10.9) The Chebotarëv density theorem (continued).

Proof of the Chebotarev density theorem when $K = \mathbb{Q}$. The Kronecker-Weber theorem states that if $K/\mathbb{Q}$ is abelian Galois then $K \subset \mathbb{Q}(\zeta_n)$ for some n. We already proved Chebotarev for $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ and so by the previous proposition Chebotarev is true for all $K/\mathbb{Q}$ Galois. □

Remark 1. To prove Chebotarev in general one may either use cyclotomic extensions, as Chebotarëv originally did, or use class field theory, namely:

1. a description of all abelian extensions of K,
2. an identification of $\mathrm{Frob}_{\mathfrak{p}}$ with elements of K for each such abelian extension,
3. a generalization of the nonvanishing at $s = 1$ of L-functions.

(10.10) Applications of Chebotarëv.

Example 1. Let L/K be a Galois extension of number fields and $\mathfrak{p}$ a prime ideal of K. Then $\mathfrak{p}$ splits completely in L if and only if the conjugacy class $\mathrm{Frob}_{\mathfrak{p}} = 1$. Thus the density of prime ideals which split completely in L is $1/[L : K]$.

Example 2. Let $a \in \mathbb{Z}$ be an integer. Then $\left(\frac{a}{p}\right) = 1$ if and only if $X^2 - a$ splits $\pmod p$ if and only if p splits completely in $\mathbb{Q}(\sqrt{a})$. When a is a perfect square then the density of p with $\left(\frac{a}{p}\right) = 1$ is 1 and when a is not a perfect square then it is $1/2$.

Example 3 (Dedekind's theorem, from homework 6)**.** Let L/K be a Galois extension of number fields. Let $f \in \mathcal{O}_K[X]$ be an irreducible monic polynomial which is separable $\pmod{\mathfrak{p}}$ for a prime ideal $\mathfrak{p}$ of K. Write $f(x) \equiv \prod_{i=1}^{r} f_i(X) \pmod{\mathfrak{p}}$ where f_i are irreducible polynomials of degree n_i in $k_{\mathfrak{p}}$. View $\mathrm{Gal}(L/K)$ as a subgroup of S_n the group of permutations of the n distinct roots of f. Then the conjugacy class $\mathrm{Frob}_{\mathfrak{p}}$ consists of elements whose image in S_n are products of r cycles of lengths $n_1, \ldots, n_r$ (up to reordering of the cycles).

Example 4 (Applications of Dedekind)**.** Consider $f(X) = X^3 - 2$ with splitting field $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ with Galois group S_3 over $\mathbb{Q}$. There are three conjugacy classes: 1, 3 transpositions and 2 three-cycles. By Dedekind's theorem Frob_p is 1 (resp. transpositions, resp. three-cycles) if and only if $X^3 - 2 \pmod p$ is a product of linear factors (resp. a linear times an irreducible quadratic, resp. one irreducible cubic). Thus the density of primes p such that $X^3 - 2 \pmod p$ is a product of linear factors is $1/6$, a linear times an irreducible quadratic is $3/6 = 1/2$ and an irreducible polynomial is $2/6 = 1/3$.

Example 5. Let $f \in \mathbb{Z}[X]$ be an irreducible monic polynomial with Galois group S_n. Write $n = m_1 n_1 + \cdots m_k n_k$ where $n_1 > n_2 > \ldots > n_k > 0$ and $m_i \geq 1$. The density of primes p such that $f(X) \pmod p$ splits as a product of m_1 polynomials of degree n_1 times m_2 polynomials of degree n_2 etc is

$$\frac{1}{\prod n_i^{m_i} \prod m_i!}$$

Example 6. The density of primes p such that when $1/p = 0.a_1 \dots a_k(b_1 \dots b_\ell)$ is written in decimal notation the period $b_1 \dots b_\ell$ has an odd number of digits is $1/3$.

11 Special values of the ζ-function and of L-functions

(11.1) Conductors of characters.

A character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ also gives a composite character $\chi : (\mathbb{Z}/Nd\mathbb{Z})^\times \to (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ for any d. Thus a character $\chi \mod N$ is also a character $\mod Nd$ and so given χ there is an ambiguity on what group it is a character of. In particular, given $\chi \mod N$ there might exists $d \mid N$ such that χ comes from a character $\mod d$. For example the trivial character always comes from a character $\mod 1$.

Definition 7. The conductor f_χ of a character χ is the smallest integer such that χ is a character $\mod f_\chi$.

For example the character mod 8 taking 1 and 5 to 1 and 3 and 7 to -1 in fact comes from the character mod 4 taking k to $(-1)^{(k-1)/2}$ and so has conductor 4.

(11.2) Bernoulli numbers.

The Bernoulli numbers B_n are the coefficients

$$\frac{t}{e^t - 1} = \sum B_n \frac{t^n}{n!}$$

If χ is a character then $B_{n,\chi}$ is defined by

$$\sum_{a=1}^{f_\chi} \frac{te^{at}}{e^{f_\chi t} - 1} = \sum_{n \geq 0} B_{n,\chi} \frac{t^n}{n!}$$

with

$$B_{1,\chi} = \frac{1}{f_\chi} \sum_{a=1}^{f_\chi} \chi(a) a$$

In fact one can show that the definition of $B_{n,\chi}$ doesn't change if one replaces f_χ in the definition by any multiple of it.

(11.3) The ζ-function.

From homework 5 we take

$$\zeta(2n) = \frac{(-1)^{n+1} B_{2n} (2\pi)^{2n}}{2(2n)!}$$

$$\zeta(1-2n) = -\frac{B_{2n}}{2n}$$

(11.4) L-functions at negative integers.

Remark that if χ is a character modulo its conductor f_χ then we can also treat it as a character modulo $f_\chi d$ but the L-functions are not the same. Because of this we'll write $L(\chi, s)$ when χ is taken modulo its conductor and otherwise write $L(\chi \mod f_\chi d, s)$:

$$L(\chi, s) = \prod_{p \mid d, p \nmid f_\chi} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} L(\chi \mod f_\chi d, s)$$

Theorem 8. *If χ is a character modulo its conductor and $n \geq 1$ then*

$$L(\chi, 1-n) = -\frac{B_{n,\chi}}{n}$$

Proof. This is a long but not difficult computation in complex analysis. □