MATH 776
APPLICATIONS: L-FUNCTIONS AND DENSITIES

ANDREW SNOWDEN

1. Dirichlet series

A **Dirichlet series** is a series of the form $\sum_{n \ge 1} \frac{a_n}{n^s}$ where the a_n are complex numbers. An **Euler product** is a product of the form $\prod_p f_p(p^{-s})^{-1}$, where the product is over prime numbers p and $f_p(T)$ is a polynomial (called the **Euler factor** at p) with constant term 1. One can formally expand an Euler product to obtain a Dirichlet series. A Dirichlet series admits an Euler product if and only if a_n is a multiplicative function of n (i.e., $a_{nm} = a_n a_m$ for $(n, m) = 1$) and $n \mapsto a_{p^n}$ satisfies a linear recursion for each prime p.

Example 1.1. The **Riemann zeta function** is $\zeta(s) = \sum_{n \ge 1} \frac{1}{n^s}$. It admits the Euler product $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$. $\square$

Example 1.2. Let K be a number field. The **Dedekind zeta function** of K is $\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathbf{N}(\mathfrak{a})^{-s}}$, where the sum is over all integral ideals $\mathfrak{a}$. Note that this is indeed a Dirichlet series, as it can be written in the form $\sum_{n \ge 1} \frac{a_n}{n^s}$ where a_n is the number of ideals of norm n. It admits the Euler product $\prod_{\mathfrak{p}} (1 - \mathbf{N}(\mathfrak{p})^{-s})^{-1}$, where the product is over all prime ideals. Note this this can be written as $\prod_p f_p(p^{-s})^{-1}$, where $f_p(T) = \prod_{\mathfrak{p} \mid p} (1 - T^{f(\mathfrak{p}|p)})$ and $f(\mathfrak{p}|p)$ denotes the degree of the residue field extension, and thus indeed fits our definition of Euler product. $\square$

Example 1.3. Recall that a **Dirichlet character** of modulus m is a group homomorphism $\chi \colon (\mathbf{Z}/m\mathbf{Z})^{\times} \to \mathbf{C}^{\times}$. The **Dirichlet L-series** associated to χ is $L(s, \chi) = \sum_{n \ge 1} \frac{\chi(n)}{n^s}$, where, by convention, we put $\chi(n) = 0$ if $(n, m) \ne 1$. This admits the Euler product $\prod_p (1 - \chi(p) p^{-s})^{-1}$, using the same convention. $\square$

Example 1.4. More generally, let $\mathfrak{m}$ be a modulus of a number field K. A **Dirichlet character** of K with modulus $\mathfrak{m}$ is a homomorphism $\chi \colon C_{\mathfrak{m}} \to \mathbf{C}^{\times}$, where $C_{\mathfrak{m}}$ denotes the ray class group. The **Dirichlet L-series** associated to χ is $L(s, \chi) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{\mathbf{N}(\mathfrak{a})^{-s}}$, where, as before, $\chi(\mathfrak{a})$ is defined to be 0 if $\mathfrak{a}$ is not prime to $\mathfrak{m}_f$. Again, this admits an Euler product $L(s, \chi) = \prod_{\mathfrak{p}} (1 - \chi(\mathfrak{p}) \mathbf{N}(\mathfrak{p})^{-s})^{-1}$. $\square$

Example 1.5. Let $\rho \colon G_K \to \mathbf{C}^{\times}$ be a continuous one-dimensional representation of the absolute Galois group of the number field K. The **Artin L-series** of ρ is $L(s, \rho) = \prod_{\mathfrak{p}} (1 - \rho(\mathrm{Frob}_{\mathfrak{p}}) \mathbf{N}(\mathfrak{p})^{-s})^{-1}$, using the convention that $\rho(\mathrm{Frob}_{\mathfrak{p}}) = 0$ if ρ is ramified at $\mathfrak{p}$ (i.e., inertia acts non-trivially). $\square$

Date: February 7, 2019.

Example 1.6. More generally, let $\rho\colon G_K \to \mathbf{GL}(V)$ be a continuos representation of G_K on a finite-dimensional complex vector space V. Then the **Artin L-series** of ρ is

$$L(s,\rho) = \prod_{\mathfrak{p}} \det(1 - \mathbf{N}(\mathfrak{p})^{-s}\mathrm{Frob}_{\mathfrak{p}} \mid V^{I_{\mathfrak{p}}})^{-1},$$

where $V^{I_{\mathfrak{p}}}$ denotes the space of vectors fixed by the inertia group $I_{\mathfrak{p}}$. Note that $V = V^{I_{\mathfrak{p}}}$ for all but finitely many $\mathfrak{p}$, and so the polynomial appearing in the Euler factor at $\mathfrak{p}$ is essentially the characteristic polynomial of $\mathrm{Frob}_{\mathfrak{p}}$. □

Thus we essentially have three types of L-series: Dedekind zeta functions, Dirichlet L-series, and Artin L-series. There are a few important relationships among them.

Proposition 1.7. *We have the following:*

(a) Let ρ and σ be two representations of G_K. Then $L(s,\rho\oplus\sigma) = L(s,\rho)L(s,\sigma)$.
(b) Let L/K be a finite extension and let ρ be a representation of G_L. Then $L(s,\rho) = L(s,\mathrm{Ind}_{G_L}^{G_K}(\rho))$.
(c) Let L/K be a finite Galois extension with group G, and let ρ be the regular representation of G. Then $L(s,\rho) = \zeta_L(s)$.
(d) Let L/K be a finite Galois extension with group G. Then $\zeta_L(s) = \prod_\rho L(s,\rho)^{d(\rho)}$ where the product is over the irreducible complex representations ρ of G and $d(\rho)$ denotes the degree (dimension) of ρ.

Proof. (a) This is obvious since the characteristic polynomial on a direct sum is the product of characteristic polynomials.

(b) Let $\mathfrak{p}$ be a prime of K and let $\mathfrak{q}_1,\ldots,\mathfrak{q}_r$ be the primes of L above it. By Mackey's theorem (which explains how induction and restriction interact), the restriction of the induced representation to the decomposition group $G_{\mathfrak{p}}$ decomposes as $\bigoplus_{i=1}^r \mathrm{Ind}_{G_{\mathfrak{q}_i}}^{G_{\mathfrak{p}}}(\rho|_{G_{\mathfrak{q}_i}})$. The result now easily follows.

(c) Let σ be the trivial representation of G_L. Then clearly $L(s,\sigma) = \zeta_L(s)$. As $\rho = \mathrm{Ind}_{G_L}^{G_K}(\sigma)$, the result follows from (b).

(d) This follows from (a) and (c) together with the result describing how the regular representation decomposes into irreducibles. □

The following proposition links Artin and Dirichlet L-series via class field theory. The use of class field theory here is very simple, but this is an extremely important bridge.

Proposition 1.8. *Let K be a number field and let $\mathfrak{m}$ be a modulus. Let $\chi\colon C_{\mathfrak{m}} \to \mathbf{C}^\times$ be a Dirichlet character. Let $\rho\colon G_K \to \mathbf{C}^\times$ be the one-dimensional obtained by the following composition:*

$$G_K \longrightarrow \mathrm{Gal}(K_{\mathfrak{m}}/K) \xrightarrow{\varphi} C_{\mathfrak{m}} \xrightarrow{\chi} \mathbf{C}^\times,$$

where $K_{\mathfrak{m}}$ is the ray class field and φ is the isomorphism induced by the global Artin map. Then $L(s,\chi) = L(s,\rho)$, up to finitely many Euler factors.

Proof. We have $\rho(\mathrm{Frob}_{\mathfrak{p}}) = \chi(\mathfrak{p})$ by definition (recall that $\varphi(\mathrm{Frob}_{\mathfrak{p}}) = \mathfrak{p}$), and so the Euler factors in $L(s,\chi)$ and $L(s,\rho)$ are the same at $\mathfrak{p}$ prime to $\mathfrak{m}$. (Note that $\mathfrak{p}$ could divide $\mathfrak{m}$ but χ could be unramified at $\mathfrak{p}$—e.g., take χ to be the trivial character—and at such $\mathfrak{p}$ the Euler factors differ.) □

Corollary 1.9. *Let H be a subgroup of $C_{\mathfrak{m}}$, and let $L = K_{\mathfrak{m}}^H$ be the corresponding abelian extension. Then*

$$\zeta_L(s) = \prod_{\chi\colon C_{\mathfrak{m}}/H \to \mathbf{C}^\times} L(s,\chi),$$

up to finitely many Euler factors, where the product on the right is over all Dirichlet characters of modulus $\mathfrak{m}$ that are trivial on H.

Proof. This follows by combining Propositions 1.7(d) and 1.8. □

2. Convergence of Dirichlet series

So far, we have been treating Dirichlet series as formal series. We now analyze their convergence behavior. We begin by recalling the behavior of the Riemann zeta function:

Proposition 2.1. *Let $\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}$ be the Riemann zeta function.*

(a) The Dirichlet series defining $\zeta(s)$ converges absolutely for $\Re(s) > 1$. The function $s \mapsto \zeta(s)$ is holomorphic in this half-plane.
(b) The series $(1-2^{1-s})^{-1}\sum_{n\geq 1}\frac{(-1)^{n+1}}{n^s}$ converges for $\Re(s) > 0$ and coincides with $\zeta(s)$ for $\Re(s) > 1$. Thus $\zeta(s)$ admits a meromorphic continuation to the half-plane $\Re(s) > 0$ that is holomorphic away from $s = 1$ and has a simple pole at $s = 1$ of residue 1.
(c) In fact, $\zeta(s)$ admits a meromorphic continuation to the entire complex plane that is holomorphic except at $s = 1$.

Proof. (a) This is basic analysis.

(b) The identity

$$(1-2^{1-s})^{-1}\sum_{n\geq 1}\frac{(-1)^{n+1}}{n^s} = \sum_{n\geq 1}\frac{1}{n^s}$$

is a simple formal manipulation. The fact that the series appearing in the left side defines a holomorphic function for $\Re(s) > 0$ is basic analysis. Since $(1-2^{1-s})^{-1}$ has a simple pole at $s = 1$ with residue $(\log 2)^{-1}$ and $\sum_{n\geq 1}\frac{(-1)^{n+1}}{n} = \log(2)$, the rest of the statement follows.

(c) This follows from a more advanced analysis of $\zeta(s)$. □

We now have the following general convergence result.

Proposition 2.2. *Consider a Dirichelt series $F(s) = \sum_{n\geq 1}\frac{a_n}{n^s}$, and put $S(x) = \sum_{n<x} a_n$.*

(a) Suppose $|S(x)| = O(x^b)$ for some $b > 0$. Then the series converges for $\Re(s) > b$ and $F(s)$ is a holomorphic function in this half-plane.
(b) Suppose $|S(x) - ax| = O(x^b)$ for some $0 < b < 1$ and some $a \in \mathbf{C}^\times$. Then $F(s)$ extends to a meromorphic function in the half-plane $\Re(s) > b$ that is holomorphic away from $s = 1$ and has a simple pole at $s = 1$ with residue a.

Proof. (a) is follows from elementary analysis. (b) follows by applying (a) to $F(s) - a\zeta(s)$ and using the properties of $\zeta(s)$ that we already know. □

3. Partial zeta functions

Let K be a number field. Fix a modulus $\mathfrak{m}$ and a class $\mathfrak{c} \in C_{\mathfrak{m}}$. Define the **partial zeta function** by

$$\zeta_K(s, \mathfrak{c}) = \sum_{\mathfrak{a} \in \mathfrak{c}} \frac{1}{\mathbf{N}(\mathfrak{a})^{-s}},$$

where the sum is over integral ideals $\mathfrak{a}$ that a prime to $\mathfrak{m}$ and belong to the class $\mathfrak{c}$. This Dirichlet series does not admit an Euler product in general. It is not really a main object of interest, but it is useful in analyzing other series we care more about. To analyze its behavior, put

$$S(x, \mathfrak{c}) = \#\{\mathfrak{a} \in \mathfrak{c} \mid \mathbf{N}(\mathfrak{a}) < x\},$$

that is, $S(x, \mathfrak{c})$ is the number of integral ideals in the class $\mathfrak{c}$ with norm less than x.

Proposition 3.1. *Let $d = [K : \mathbf{Q}]$. Then*

$$|S(x, \mathfrak{c}) - a(\mathfrak{m})x| = O(x^{1-1/d})$$

where $a(\mathfrak{m})$ is the constant given by

$$a(\mathfrak{m}) = \frac{2^{r-\#\mathfrak{m}_\infty}(2\pi)^s \operatorname{reg}(\mathfrak{m})}{w_{\mathfrak{m}} \mathbf{N}(\mathfrak{m}_f)|\Delta_{K/\mathbf{Q}}|^{1/2}}$$

and

- *r is the number of real places of K*
- *s is the number of complex places of K.*
- $\operatorname{reg}(\mathfrak{m})$ *is the regulator for $U \cap K^{\mathfrak{m},1}$*
- *$w_{\mathfrak{m}}$ is the number of roots of unity in $K^{\mathfrak{m},1}$*
- *$\Delta_{K/\mathbf{Q}}$ is the discriminant of $K/\mathbf{Q}$.*

Proof. Let $\mathfrak{b}$ be an integral ideal of class $\mathfrak{c}^{-1}$. Then if $\mathfrak{a}$ is an integral ideal in $\mathfrak{c}$ we have $\mathfrak{a}\mathfrak{b} = (\alpha)$ for some integral $\alpha \in K^{\mathfrak{m},1}$. Thus we are essentially counting the number of integral elements $\alpha \in K^{\mathfrak{m},1}$, up to units, with norm at most $\mathbf{N}(\mathfrak{b})x$. This can be done using techniques similar to those used in the proof of Dirichlet's unit theorem. □

Proposition 3.2. *The Dirichlet series defining $\zeta_K(s, \mathfrak{c})$ converges for $\Re(s) > 1$. The function $\zeta_K(s, \mathfrak{c})$ extends to a meromorphic function in the half-plane $\Re(s) > 1 - 1/d$ that is holomorphic away from $s = 1$ and has a simple pole at $s = 1$ with residue $\mathfrak{a}(\mathfrak{m})$.*

Proof. This follows from the previous proposition and our general results on Dirichlet series. □

Corollary 3.3 (Analytic class number formula)**.** *The Dirichlet series defining $\zeta_K(s)$ converges for $\Re(s) > 1$. The function $\zeta_K(s)$ extends to a meromorphic function in the half-plane $\Re(s) > 1 - 1/d$ that is holomorphic away from $s = 1$ and has a simple pole at $s = 1$ with residue*

$$\frac{2^r(2\pi)^s \operatorname{reg}(K)h_K}{w|\Delta_{K/\mathbf{Q}}|^{1/2}}$$

where h_K is the class number of K and w is the number of roots of unity in K.

Proof. The function $\zeta_K(s)$ is the sum of the partial zeta functions $\zeta_K(s, \mathfrak{c})$ over $\mathfrak{c} \in C_{\mathfrak{m}}$ with $\mathfrak{m}$ the trivial modulus. The result now follows from the proposition. □

Remark 3.4. The simple fact that $\zeta_K(s)$ has a pole at $s=1$ is already interesting. Indeed, let S be the set of split primes in K (i.e., those with residue field $\mathbf{F}_p$) and let T be the set of non-split primes. Then

$$\zeta_K(s) = \left[\prod_{\mathfrak{p}\in S}(1-\mathbf{N}(\mathfrak{p})^{-s})^{-1}\right]\left[\prod_{\mathfrak{p}\in T}(1-\mathbf{N}(\mathfrak{p})^{-s})^{-1}\right].$$

Now, the second factor above converges at $s=1$: indeed, if $\mathfrak{p}\in T$ is above p then $\mathbf{N}(\mathfrak{p})=p^f$ for some $f>1$, and the claim follows from the fact that $\sum_p p^{-2}$ converges. Thus, since $\zeta_K(s)$ has a pole at $s=1$, it follows that S is infinite, that is, there are infinitely many split primes. We will refine this result in the next section.

Applying this argument to the Galois closure of K, we see that there are infinitely many primes p of $\mathbf{Q}$ that split completely in K. As an application, we see that if $f(x)\in\mathbf{Q}[x]$ is irreducible then there are infinitely many primes p such that $f(x)$ splits into linear factors modulo p. □

Corollary 3.5. *Let χ be a non-trivial Dirichlet character of K with modulus $\mathfrak{m}$. Then the Dirichlet series defining $L(s,\chi)$ converges for $\Re(s)>1$. The function $L(s,\chi)$ extends to a* holomorphic *function in the half-plane $\Re(s)>1-1/d$; there is no pole at $s=1$.*

Proof. We have $L(s,\chi)=\sum_{\mathfrak{c}\in C_{\mathfrak{m}}}\chi(\mathfrak{c})\zeta_K(s,\mathfrak{c})$. The proposition thus shows that the series defining $L(s,\chi)$ converges for $\Re(s)>1$ and that $L(s,\chi)$ extends to a meromorphic function in the half-plane $\Re(s)>1$ that it holomorphic away from $s=1$ and has (at worst) a simple pole at $s=1$ with residue $a(\mathfrak{m})\sum_{\mathfrak{c}}\chi(\mathfrak{c})$. However, this sum vanishes since χ is non-trivial. □

We can now prove an extremely important and deep theorem:

Theorem 3.6. *Let χ be a non-trivial Dirichlet character of K. Then $L(1,\chi)\neq 0$.*

Proof. Let $\mathfrak{m}$ be a modulus for K, and let $K_{\mathfrak{m}}$ be the ray class field. By Corollary 1.9, we have

$$\zeta_{K_{\mathfrak{m}}}(s)=\prod_{\chi}L(s,\chi)$$

where the product is over all Dirichlet characters of modulus $\mathfrak{m}$. Let χ_0 be the trivial Dirichlet character. Then $L(s,\chi)=\zeta_K(s)$ and $\zeta_{K_{\mathfrak{m}}}(s)$ have simple poles at $s=1$ (Corollary 3.3). For $\chi\neq\chi_0$, the function $L(s,\chi)$ is holomorphic at $s=1$ (Corollary 3.5). Thus, comparing the order of pole on each side of the equation, we see that $L(1,\chi)\neq 0$ for all non-trivial χ. □

Remark 3.7. The proof of the theorem makes crucial use of class field theory: without it, we would not be able to connect Artin and Dirichlet L-functions, and we would have no information about the behavior of $\prod_{\chi}L(s,\chi)$ at $s=1$. □

4. Densities

Let T be a set of primes of a number field K. There are a few ways to define a notion of density for T:

- The **natural density** of T is

$$\lim_{x\to\infty}\frac{\#\{\mathfrak{p}\in T\mid \mathbf{N}(\mathfrak{p})\leq x\}}{\#\{\mathfrak{p}\mid \mathbf{N}(\mathfrak{p})\leq x\}}.$$

- Let $\zeta_{K,T}(s) = \prod_{\mathfrak{p}\in T}(1-\mathbf{N}(\mathfrak{p})^{-s})^{-1}$. We say that T has **polar density** n/m if $\zeta_{K,T}(s)^m$ is meromorphic at $s=1$ with a pole of order n.
- The **Dirichlet density** of T is

$$(-1)\cdot \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in T}\mathbf{N}(\mathfrak{p})^{-s}}{\log(s-1)}.$$

The motivation for this definition comes from the observation that $\log\zeta_K(s)$ behaves like $-\log(s-1)$ as $s\to 1$, and

$$\begin{aligned}\log\zeta_K(s) &= \log\left[\prod_{\mathfrak{p}}(1-\mathbf{N}(\mathfrak{p})^{-s})^{-1}\right]\\ &= -\sum_{\mathfrak{p}}\log(1-\mathbf{N}(\mathfrak{p})^{-s})\\ &= \sum_{\mathfrak{p}}\sum_{n\geq 1}\frac{\mathbf{N}(\mathfrak{p})^{-ns}}{n}\\ &\sim \sum_{\mathfrak{p}}\mathbf{N}(\mathfrak{p})^{-s}\end{aligned}$$

where the final line is an asymptotic statement near $s=1$, which comes from the fact that $\sum_{\mathfrak{p}}\mathbf{N}(\mathfrak{p})^{-n}$ converges for $n>1$.

None of these densities need to exist. They are related as follows:

Proposition 4.1. *If the polar density of T exists then so does the Dirichlet density, and they are equal. Similar, if the natural density of T exists then so does the Dirichlet density, and they are equal.*

Proof. Left as an exercise. □

Theorem 4.2. *Let L/K be an extension of number fields, and let M be the Galois closure of L over K. Let T be the set of primes of K that split completely in L. Then T has polar density $1/[M:K]$.*

Proof. First note that a prime $\mathfrak{p}$ of K splits completely in L if and only if it splits (completley) in M. So we can just concentrate on M. Let S be the set of primes of K that do not split completely in K. We have

$$\zeta_M(s) = \left[\prod_{\mathfrak{q}\mid\mathfrak{p}\in T}(1-\mathbf{N}(\mathfrak{q})^{-s})^{-1}\right]\cdot\left[\prod_{\mathfrak{q}\mid\mathfrak{p}\in S}(1-\mathbf{N}(\mathfrak{q})^{-s})^{-1}\right].$$

In the first product, we have $\mathbf{N}(\mathfrak{q}) = \mathbf{N}(\mathfrak{p})$ since $\mathfrak{p}$ splits. Moreover, over each $\mathfrak{p}$ there are exact $[M:K]$ $\mathfrak{q}$'s. Thus the first factor is exactly $\zeta_{K,T}(s)^{[M:K]}$. In the second factor, if $\mathfrak{p}$ lies over the rational prime p then $\mathbf{N}(\mathfrak{q}) = p^f$ with $f>1$ (away from the finitely many primes that ramify). Thus this product converges as $s\to 1$. We thus find

$$\zeta_M(s) = \zeta_{K,T}(s)^{[M:K]}\cdot(\text{a function that is holomorphic and non-zero at } s=1).$$

Since $\zeta_M(s)$ has a pole of order 1 at $s=1$, the result follows. □

Corollary 4.3. *Let $\mathfrak{m}$ be a modulus of K and let T be the set of primes of T in the trivial class of the ray class group $C_{\mathfrak{m}}$. Then T has polar density $1/\#C_{\mathfrak{m}}$.*

Proof. Let $K_{\mathfrak{m}}$ be the ray class field, so that $\mathrm{Gal}(K_{\mathfrak{m}}/K) = C_{\mathfrak{m}}$ via the global Artin map. A prime $[\mathfrak{p}] \in C_{\mathfrak{m}}$ corresponds to $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(K_{\mathfrak{m}}/K)$, we see that $\mathfrak{p}$ splits completely in $K_{\mathfrak{m}}$ if and only if $[\mathfrak{p}] = 0$ in $C_{\mathfrak{m}}$. Thus the result follows from the theorem. □

Corollary 4.4. *Given any integer $m > 1$, there are infinitely many prime numbers p congruent to 1 modulo m.*

5. Dirichlet's theorem and consequences

We now improve the above corollaries by considering other congruence classes.

Theorem 5.1. *Let $\mathfrak{m}$ be a modulus of K, let H be a subgroup of $C_{\mathfrak{m}}$, and let $\mathfrak{k} \in C_{\mathfrak{m}}$. Let T be the set of primes $\mathfrak{p}$ of K such that $[\mathfrak{p}] \in \mathfrak{k} + H$. Then T has Dirichlet density $1/[C_{\mathfrak{m}} : H]$.*

Proof. For a Dirichlet character χ, we have

$$\log L(s, \chi) \sim \sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p})}{\mathbf{N}(\mathfrak{p})^{-s}}.$$

If χ is trivial, this is asymptotic to $-\log(s-1)$ as $s \to 1^+$. If χ is non-trivial, then this is bounded as $s \to 1^+$: this follows from the fact that $L(s, \chi)$ is holomorphic and non-vanishing at $s = 1$. Now, by Fourier analysis on the group $C_{\mathfrak{m}}/H$, we have

$$\frac{1}{[C_{\mathfrak{m}} : H]} \sum_{\chi \colon C_{\mathfrak{m}}/H \to \mathbf{C}^\times} \chi^{-1}(\mathfrak{k})\chi(\mathfrak{p}) = \begin{cases} 1 & \text{if } [\mathfrak{p}] \in \mathfrak{k} + H \\ 0 & \text{otherwise} \end{cases}$$

and so

$$\frac{1}{[C_{\mathfrak{m}} : H]} \sum_{\chi \colon C_{\mathfrak{m}}/H \to \mathbf{C}^\times} \chi^{-1}(\mathfrak{k}) L(s, \chi) \sim \sum_{\mathfrak{p} \in T} \mathbf{N}(\mathfrak{p})^{-s}.$$

The result thus follows. □

Corollary 5.2. *Let a and m be coprime positive integers. Then the set of primes p congruent to a modulo m has Dirichlet density $1/\varphi(m)$. In particular, there are infinitely many such primes.*

Corollary 5.3. *Let L/K be a finite abelian extension. Let $g \in \mathrm{Gal}(L/K)$ be a given element, and let T be the set of primes $\mathfrak{p}$ of K such that $\mathrm{Frob}_{\mathfrak{p}} = g$ (and $\mathfrak{p}$ is unramified in L). Then T has Dirichlet density $1/[L : K]$. In particular, every element of $\mathrm{Gal}(L/K)$ is a Frobenius element, and in fact, in infinitely many ways.*

Proof. This follows by combining the theorem and class field theory. Specifically, we have $L = K_{\mathfrak{m}}^H$ for some modulus $\mathfrak{m}$ and subgroup $H \subset C_{\mathfrak{m}}$, and the Artin map gives an isomorphism $\mathrm{Gal}(L/K) = C_{\mathfrak{m}}/H$. Thus $g \in \mathrm{Gal}(L/K)$ corresponds to some $\mathfrak{k} \in C_{\mathfrak{m}}/H$. We thus see that $\mathrm{Frob}_{\mathfrak{p}} = g$ if and only if $[\mathfrak{p}] \in \mathfrak{k} + H$, and so we are exactly in the situation of the theorem. □

6. Chebotarev's theorem

Chebotarev's theorem improves the previous corollary to the setting of non-abelian extensions:

Theorem 6.1. *Let L/K be a finite Galois extension of number fields with group G. Let $C \subset G$ be a conjugacy class and let T be the set of primes $\mathfrak{p}$ of K such that $\mathrm{Frob}_{\mathfrak{p}} \in C$. The T has Dirichlet density $\#C/\#G$.*

Proof. Pick $\sigma \in C$ and let $M = L^\sigma$ be its fixed field. Let $f = [L : M]$ be the order of σ, let $c = \#C$, and let $d = \#G$. Let S be the set of primes $\mathfrak{q}$ of M such that $\mathrm{Frob}_\mathfrak{q} = \sigma$ and $f(\mathfrak{q} \mid \mathfrak{p}) = 1$, where $\mathfrak{p}$ is the contraction of $\mathfrak{q}$ to K. Let R be the set of primes $\mathfrak{P}$ of L such that $\mathrm{Frob}_\mathfrak{P} = \sigma$. We claim that (a) contraction induces a bijection $R \to S$; and (b) contraction induces a map $R \to T$ that is exactly d/cf to 1. Since S has density $1/f$ (abelian version of Chebotarev, proved in previous section), it will follow that T has density c/d, as desired.

(a) Let $\mathfrak{P} \in R$, let $\mathfrak{q}$ be its contraction to M, and let $\mathfrak{p}$ be its contraction to K. By definition, $\mathrm{Frob}_\mathfrak{q} = \mathrm{Frob}_\mathfrak{P}$, and is thus σ. Thus $f(\mathfrak{P}|\mathfrak{q}) = f = [L : M]$, and so $\mathfrak{P}$ is the unique prime above $\mathfrak{q}$; thus the contraction map is injective. Since $f(\mathfrak{P}|\mathfrak{p}) = f$ as well, it follows that $f(\mathfrak{q}|\mathfrak{p}) = 1$, and so $\mathfrak{q} \in S$. Thus contraction gives a well-defined injection $R \to S$. Finally, if $\mathfrak{q} \in S$ and $\mathfrak{P}$ is any prime over $\mathfrak{q}$ then $\mathrm{Frob}_\mathfrak{P} = \mathrm{Frob}_\mathfrak{q}$ by definition, and thus belongs to R.

(b) Let $\mathfrak{p} \in T$ and let $\mathfrak{P}_0 \in R$ be a prime of L over it with $\mathrm{Frob}_{\mathfrak{P}_0} = \sigma$. For $\tau \in G$ we have $\mathrm{Frob}_{\tau\mathfrak{P}_0} = \tau\sigma\tau^{-1}$, and so $\tau\mathfrak{P}_0 \in R$ if and only if $\tau \in Z(\sigma)$ (the centralizer of σ). Moreover, $\tau\mathfrak{P}_0 = \mathfrak{P}_0$ if and only if $\tau \in G_{\mathfrak{P}_0} = \langle\sigma\rangle$, the decomposition group at $\mathfrak{P}_0$. We thus see that the primes $\mathfrak{P}$ over $\mathfrak{p}$ with $\mathrm{Frob}_\mathfrak{P} = \sigma$ are in bijection with the set $Z(\sigma)/\langle\sigma\rangle$. Now, $\langle\sigma\rangle$ has order f, while $G/Z(\sigma) \cong C$, and so $Z(\sigma)$ has order d/c. The result follows. □

Corollary 6.2. *Let L/K and G be as above. Given any $\sigma \in G$ there exist infinitely many primes $\mathfrak{P}$ of L such that* $\mathrm{Frob}_\mathfrak{P} = \sigma$.

Proof. Let T be the set of primes $\mathfrak{p}$ of K such that the conjugacy class $\mathrm{Frob}_\mathfrak{p}$ is equal to the conjugacy class of σ. This set is infinite by the theorem. Let $\mathfrak{p} \in T$ be given, and let $\mathfrak{P}$ be a prime of L above $\mathfrak{p}$. Then $\mathrm{Frob}_\mathfrak{p}$ is by definition the conjugacy class of $\mathrm{Frob}_\mathfrak{P}$, and so $\mathrm{Frob}_\mathfrak{P}$ is conjugate to σ, say it's $\tau\sigma\tau^{-1}$. Letting $\mathfrak{P}' = \tau\mathfrak{P}$, we have $\mathrm{Frob}_{\mathfrak{P}'} = \sigma$. Thus for every prime in T there is a prime above it in L whose Frobenius element is σ. This completes the proof. □

Corollary 6.3. *Let K be a number field, let S be a finite set of places of K, and let $G_{K,S}$ be the Galois group of the maximal extension of K unramified away from S. Then the Frobenius elements of $G_{K,S}$ are dense.*

Proof. Density exactly means that in any finite quotient of $G_{K,S}$, every element is represented by a Frobenius element, and this is exactly the previous corollary. □

7. An application of Chebotarev's theorem

Let X be a smooth projective variety over a field k. Recall that if ℓ is a prime different from the characteristic of k then one has the étale cohomology group $\mathrm{H}^i_{\mathrm{et}}(X_{\overline{k}}, \mathbf{Q}_\ell)$, which is a $\mathbf{Q}_\ell$ vector space. The general theory of étale cohomology establishes the following:

- Each $\mathrm{H}^i_{\mathrm{et}}(X_{\overline{k}}, \mathbf{Q}_\ell)$ is finite dimensional, and only finitely many are non-zero.
- The absolute Galois group G_k of k acts continuously on $\mathrm{H}^i_{\mathrm{et}}(X_{\overline{k}}, \mathbf{Q}_\ell)$.
- If k is a finite field then the trace of Frobenius on $\mathrm{H}^*_{\mathrm{et}}(X_{\overline{k}}, \mathbf{Q}_\ell)$ is $\#X(k)$. (This is the Grothendieck–Lefschetz trace formula.)
- If $k = \mathbf{C}$ then $\mathrm{H}^i_{\mathrm{et}}(X_{\overline{k}}, \mathbf{Q}_\ell)$ is naturally identified with the singular cohomology of $X(k)$ with coefficients in $\mathbf{Q}_\ell$.
- Suppose $\mathfrak{X}$ is a smooth projective scheme over a DVR R, and ℓ is different from the residue character of R. Then the étale cohomologies of the special and generic

fibers are canonically identified; moreover, this identification is compatible with Galois actions (the Galois action on the generic fiber being unramified).

Combining this theory with the Cheobtarev density theorem can yield some very interesting results. For example:

Theorem 7.1. *Let X and Y be smooth projective varieties over $\mathbf{Q}$. Suppose that $\#X(\mathbf{F}_p) = \#Y(\mathbf{F}_p)$ for a set of primes p of Dirichlet density 1. Then the topological spaces $X(\mathbf{C})$ and $Y(\mathbf{C})$ have the same Euler characteristic.*

Proof. Pick a prime number ℓ. Let S be a finite set of primes, including ℓ, such that X and Y extend to smooth projective varieties over $\mathbf{Z}[1/S]$. Then $\mathrm{H}^i(X_{\overline{\mathbf{Q}}}, \mathbf{Q}_\ell)$ is a continuous representation of $G_{\mathbf{Q},S}$. Let V be the alternating sum of these representations, considered as a virtual representation of $G_{\mathbf{Q},S}$. Let W be the analogous thing for Y. Our hypothesis, combined with Grothendieck–Lefschetz, shows that $\mathrm{tr}(\mathrm{Frob}_p|V) = \mathrm{tr}(\mathrm{Frob}_p|W)$ for a set of primes p of Dirichlet density 1. By Chebotarev, the Frobenius elements are dense in $G_{K,S}$. We thus see that $\mathrm{tr}(\sigma|V) = \mathrm{tr}(\sigma|W)$ for all $\sigma \in G_{K,S}$. Taking $\sigma = 1$, we obtain the stated equality of Euler characteristics. ∎

References

[K] K. Kedlaya. Notes on class field theory. http://www.math.mcgill.ca/darmon/courses/cft/refs/kedlaya.pdf

[K] J.S. Milne. Class field theory. https://www.jmilne.org/math/CourseNotes/cft.html

[S] D. Speyer, Mathoverflow answer, https://mathoverflow.net/questions/234358/

[W] L. Washington. *Introduction to Cyclotomic Fields*, Chapter 14