

# ANALYTIC NUMBER THEORY

ISHAN LEVY

## 1. ASYMPTOTICS

**Lemma 1.1.** *If  $a_i$  is an indexed sequence of numbers  $\geq 0$ , and  $f(n) = \sum_{i \leq n} a_i$ ,  $F(n) = \sum_{i \leq n} \log(i)a_i$ . If  $F(n) > 0$  for large  $n$ , then  $\limsup_n \frac{f(n)\log(n)}{F(n)} \leq 1$ . If  $f(\lceil n^{1-\epsilon} \rceil) = o(f(n))$  as  $n \rightarrow \infty$  for small  $\epsilon > 0$ , then  $\log(n)f(n) \sim F(n)$ .*

*Proof.*  $F(n) = \sum_{i \leq n} \log(i)a_i \leq \sum_{i \leq n} \log(n)a_i$ , showing the first statement. For the second, Observe that for any  $\epsilon > 0$ , we have  $F(n) \geq \sum_{\lceil n^{1-\epsilon} \rceil}^n \log(n^{1-\epsilon})a_n = (1 - \epsilon)\log(n)(f(n) - f(\lceil n^{1-\epsilon} \rceil))$ , so  $\frac{F(n)}{f(n)\log(n)} \geq (1 - \epsilon)(1 - \frac{f(n^{1-\epsilon})}{f(n)})$ , and letting  $n \rightarrow \infty, \epsilon \rightarrow 0$  gives the result.  $\square$

## 2. DIRICHLET SERIES AND PROPERTIES

A very powerful tool in mathematics for studying sequences of numbers is to study their generating functions. If  $a_n$  is a sequence, one way to turn  $a_n$  into a generating function is to consider  $F(z) = \sum_0^\infty a_n z^n$ . Properties of the sequence then relate to properties of the function, and vice versa. For example, we might expect the behavior of  $F(z)$  as  $z \rightarrow 1^-$  to be related to the asymptotics of the sequence. Also if  $F$  is analytic near 1, then the coefficients  $a_n$  can be obtained via Cauchy's integral formula. These generating functions are good at capturing additive properties of sequences, as  $x^n x^m = x^{n+m}$ .

Another type of generating function that can be made from sequences is an  $L$ -function. These capture more of the multiplicative structure of the sequence. These look like something of the form  $L(s) = \sum_0^\infty \frac{a_n}{n^s}$ , called a **Dirichlet series**. Both of these constructions are specializations of the more general construction where given two sequences  $\lambda_n, a_n$ , we can consider  $\sum a_n e^{-\lambda_n s}$ . The basic example is  $\zeta(s) = \sum \frac{1}{n^s}$ , the **Riemann zeta function**. Note the series converges absolutely and uniformly on compact sets for  $\text{Re}(s) > 1$ .

As any good generating function should,  $\zeta(s)$  tells us a great deal about the distribution of the primes. Below is a simple example of how it can be used.

**Theorem 2.1.** *The series  $\sum \frac{1}{p}$  diverges, where  $p$  ranges over the positive primes in  $\mathbb{Z}$ .*

*Proof.*  $\sum_1^\infty \frac{1}{n^s} = \prod_p \left( \frac{1}{1 - \frac{1}{p^s}} \right)$ , which diverges as  $s \rightarrow 1^+$ . Taking the log of the right hand side we get  $\sum_p -\log\left(1 - \frac{1}{p^s}\right) = \sum_p \frac{1}{p} + \sum_{m \geq 2, p} \frac{1}{mp^{ms}}$ . The second sum is  $\leq \sum_{m \geq 2, p} \frac{1}{p^{ms}} = \sum_p \frac{1}{p^{2s-p^s}} \leq 2 \sum_p \frac{1}{p^{2s}}$ , which is finite as  $s \rightarrow 1$ . Thus  $\sum_p \frac{1}{p}$  diverges.  $\square$

First we will prove some lemmas about Dirichlet series. Note that a necessary condition for convergence at some point is that  $|a_n|$  should be bounded by some polynomial. Here is a partial converse:

**Lemma 2.2.** *If  $|\sum_1^n a_n| = O(n^r)$ ,  $r > 0$ , then the Dirichlet series for  $a_n$  converges uniformly for  $\operatorname{Re}(s) \geq r + \epsilon$  for any  $\epsilon > 0$  to a holomorphic function. If  $|a_n| = O(n^r)$ , then it converges absolutely and uniformly for  $\operatorname{Re}(s) > r + 1 + \epsilon$ .*

*Proof.* Let  $f_n = \sum_1^n a_n$ . We will show that the partial sums are uniformly Cauchy by using summation by parts.  $\sum_k^m \frac{a_n}{n^s} = \sum_k^m \frac{f_n - f_{n-1}}{n^s} = \frac{f_m}{m^s} - \frac{f_{k-1}}{(k-1)^s} + \sum_k^{m-1} f_n \left( \frac{1}{n^s} - \frac{1}{(n+1)^s} \right)$ . The first two terms go to 0 uniformly as  $k \rightarrow \infty$ , and the difference in the sum is equal to  $\int_n^{n+1} (-s)x^{-(s+1)}$ , which in absolute value is at most  $|s|n^{-s+1}$ . But then since  $f_n = O(n^r)$ , the last term in absolute value is at most  $\sum_k^{m-1} \frac{cn^r}{n^{-(r+\epsilon+1)}}$ , which is uniformly bounded in  $m$  and goes to 0 as  $k \rightarrow \infty$  since  $\epsilon + 1 > 1$ . The last statement is clear.  $\square$

**Lemma 2.3.** *If  $F, G$  are Dirichlet series for  $a_n, b_n$  that converge, and  $F, G$  agree where they converge, then  $a_n = b_n$ .*

*Proof.* Let  $a_i$  be the first nonzero term of  $a_n$ . Then  $F \sim \frac{a_i}{i^s}$  as  $s \rightarrow \infty$ , so this behavior determines  $i$  and  $a_i$ . By subtracting this term off, we can recover the rest of the sequence. We have used properties of  $F$  that agree with  $G$ , so  $a_n = b_n$ .  $\square$

Note by analyticity, if they agree on a small set, they agree.

**Lemma 2.4.** *Suppose that  $F, G$  are convergent Dirichlet series for  $a_n, b_n$ . Then  $FG$  is the Dirichlet series for  $a_n \star b_n$ , where  $\star$  denotes the Dirichlet convolution.*

*Proof.* For sufficiently large  $s$ ,  $F, G$  converge absolutely and uniformly. Then when we take their product, we can change the order of summation to get the result.  $\square$

### 3. ZETA FUNCTIONS & THE CLASS NUMBER FORMULA

Given a number field  $K$ , let  $j_K(n)$  be the number of ideals of norm  $n$  in  $\mathcal{O}_K$ . The **Dedekind zeta function**  $\zeta_K(s)$  is the Dirichlet series for  $j_K(n)$

**Lemma 3.1.**  $\zeta_K(s)$  converges for  $\operatorname{Re}(s) > 1$ .

*Proof.* From the theorem on the distribution of ideals, it follows that  $\sum_{i \leq n} j_K(i) = O(n)$ , so that by Lemma 2.2 this is true.  $\square$

We will want to extend  $\zeta_K(s)$  to  $\operatorname{Re}(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$ , so that we can better study its behavior near 1. First  $\zeta(s)$  will be extended. Note that  $\zeta(s)(1 - 2^{1-s})$  is the Dirichlet series for the sequence  $(-1)^{n+1}$ , which converges for  $\operatorname{Re}(s) > 0$ . This lets us extend  $\zeta(s)$  to  $\operatorname{Re}(s) > 0$ , but it might have some singularities where  $1 - 2^{1-s}$  is 0. To reduce the number of possible poles,  $\zeta(s)(1 - 3^{1-s})$  also converges for  $\operatorname{Re}(s) > 0$  for the same reason, but the only common zeros of  $1 - 2^{1-s}$  and  $1 - 3^{1-s}$  are  $s = 1$ . Thus  $\zeta(s)$  can only have a simple pole at  $s = 1$ , and indeed it does since  $1 - 2^{1-s}$  has a simple zero. Now for some  $\kappa$ ,  $\zeta_K(s) - \kappa\zeta(s)$  is the Dirichlet series for some sequence  $f(n)$  with  $\sum_1^n f(i) = O(n^{1-\frac{1}{[K:\mathbb{Q}]}})$  so we can use this to extend  $\zeta_K(s)$ . Note that as a consequence,  $\zeta_K(s)$  also has a simple pole at 1.

**Theorem 3.2.**  *$\zeta_K(s)$  is an analytic function in the region  $\operatorname{Re}(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$ , and has a simple pole with residue  $\frac{h_K 2^{r+s} \pi^s \operatorname{reg}(K)}{\omega_K \sqrt{|\operatorname{disc}(K)|}}$ .*

*Proof.* Because of how we have shown that  $\zeta_K(s)$  is analytic near 1, we only need to compute the residue of  $\zeta(s)$  at 0. Note that the Dirichlet series for  $(-1)^{s+1}$  at 1 is  $\sum_i \frac{(-1)^{i+1}}{i} = \int_0^1 \sum_i (-1)^{i+1} x^{i+1} = \int_0^1 \frac{1}{1+x} = \log(2)$ . On the other hand, the  $s - 1$  term in the series expansion of  $(1 - 2^{1-s})$  is  $\frac{1}{\log(2)}$ .  $\square$

Now we can write  $\zeta_K(s)$  another way. But first a technical lemma.

**Lemma 3.3.** *Suppose that  $a_i \in \mathbb{C}$  satisfy  $|a_i| < 1$  and  $\sum_i |a_i| \leq \infty$ . Then  $\prod_1^\infty (1 - a_i)^{-1} = \sum_{S \subset \mathbb{N} \text{ finite}} \prod_S a_i$ , where the sum is absolutely convergent.*

*Proof.* Note that  $e^{-\sum_i |a_i|} = \prod_i e^{-|a_i|}$  converges and by Taylor's theorem is at least  $\prod_i (1 - |a_i|)$ . Thus the inverse, which is the left hand side, absolutely converges, and the partial products show that it converges to the right hand side.  $\square$

**Proposition 3.4.** *For  $\operatorname{Re}(s) > 1$ ,  $\zeta_K(s) = \sum_{I \subset \mathcal{O}_K} \frac{1}{N(I)} = \prod_{\mathfrak{p} \subset \mathcal{O}_K} \frac{1}{1 - N(\mathfrak{p})^{-s}}$ .*

*Proof.* These follow from Lemma 3.3, the fact that  $\mathcal{O}_K$  is a Dedekind domain, and the fact that  $\zeta_K(s)$  converges in that region.  $\square$

For any subset of primes  $S$ , we can also consider  $\zeta_{K,S}(s) = \prod_{\mathfrak{p} \in S} \frac{1}{1 - N(\mathfrak{p})^{-s}}$ . Note that it converges for  $\operatorname{Re}(s) > 1$  as well.

**Lemma 3.5.** *Let  $S$  be a set of primes in  $\mathcal{O}_K$ . Then  $|\sum_{\mathfrak{p} \in S} \frac{1}{N(\mathfrak{p})^s} - \log(\zeta_{K,S}(s))| = O(1)$  for  $\operatorname{Re}(s) > 1$ .*

*Proof.*  $\log(\zeta_K(s)) = \sum_{\mathfrak{p} \in S} -\log(1 - N(\mathfrak{p})^{-s}) = \sum_{\mathfrak{p} \in S} \frac{1}{N(\mathfrak{p})^s} + \sum_{\mathfrak{p} \in S, m \geq 2} \frac{1}{m N(\mathfrak{p})^{ms}}$ . The second term is at most  $\sum_{\mathfrak{p}, m \geq 2} \frac{1}{N(\mathfrak{p})^{ms}} = \sum_{\mathfrak{p} \in S} \frac{1}{N(\mathfrak{p})^{2s - N(\mathfrak{p})^s}} \leq 2 \sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-2} < \infty$ .  $\square$

The **Dirichlet density** of a set of primes  $S$  is the limit as  $s \rightarrow 1$ , if it exists, of  $\frac{\sum_{p \in S} \frac{1}{N(p)^s}}{\sum_p \frac{1}{N(p)^s}}$ . We can similarly define the upper and lower Dirichlet densities using  $\liminf$  and  $\limsup$ . It clearly satisfies natural properties one might expect. We say that  $S$  has **polar density**  $\frac{n}{m}$  if  $\zeta_{K,S}(s)^m$  has a pole of order  $n$ . Polar density also satisfies natural properties. The following is easy to see because of Lemma 3.5.

**Lemma 3.6.** *If the polar density exists, so does the Dirichlet density, and the two are equal.*

**Lemma 3.7.** *Let  $A$  be a set of primes with residual degree  $> 1$  over  $\mathbb{Z}$ . Then  $\zeta_{K,A}(s)$  is holomorphic for  $\operatorname{Re}(s) > \frac{1}{2}$  and  $A$  has polar density 0.*

*Proof.* Split  $A$  up by residual degree  $f$ , and note that the terms corresponding zeta function is bounded by  $\zeta_K(fs)^n$ , so by Lemma 2.2 each is holomorphic on  $\operatorname{Re}(s) > \frac{1}{f}$ .  $\square$

**Corollary 3.8.** *The primes in  $K$  that split completely in a Galois extension  $L$  have polar density  $\frac{1}{[M:K]}$  where  $M$  is the Galois closure of  $L/K$ .*

*Proof.* First assume  $L$  is Galois. WLOG, we can restrict to primes that have residual degree 1 over  $\mathbb{Q}$ . But then this is clear, since if  $A$  are the primes of residual degree 1 in  $L$  and  $B$  are the primes of residual degree 1 splitting completely, then  $\zeta_{L,A}(s)$  is the  $[L:K]^{th}$  power of the  $\zeta_{K,B}(s)$ , so the result follows. Now we can remove the Galois assumption by noting that a prime splits completely in  $L$  iff it splits completely in the Galois closure.  $\square$

**Corollary 3.9.** *Let  $H$  be a subgroup of  $\mathbb{Z}/m\mathbb{Z}^\times$ . Then the primes congruent to  $H$  have polar density  $\frac{|H|}{m}$ .*

*Proof.* Apply the previous result to the corresponding abelian extension of  $\mathbb{Q}$ .  $\square$

A **Dirichlet character** mod  $n$  (usually denoted  $\chi$ ) is a totally multiplicative function on the natural numbers factoring through  $\mathbb{Z}/n\mathbb{Z}$ , and supported on  $\mathbb{Z}/n\mathbb{Z}^\times$ . The character corresponding to the trivial homomorphism is called the trivial character, and denoted 1. We can define  $L(s, \chi) = \sum_1^\infty \frac{\chi(n)}{n^s}$  to be the Dirichlet  $L$ -series.

**Lemma 3.10.**  *$L(s, \chi)$  is holomorphic on  $\operatorname{Re}(s) > 0$  when  $\chi$  is nontrivial, and has a simple pole when  $\chi$  is trivial.*

*Proof.* Note that  $\sum_{\mathbb{Z}/n\mathbb{Z}} \chi(a) = 0$  for a nontrivial character mod  $n$ , so that  $\sum_1^m \chi(a) = O(1)$ , giving the first result.  $L(s, 1) = \zeta(s) \prod_{p|n} (1 - p^{-s})$ , giving the second result.  $\square$

More generally, given an abelian extension  $L$  of a number field  $K$ , we can consider characters  $\chi \in \hat{G}$  on the Galois group  $G$ , and we can define a corresponding character

on the set of ideals via the Artin map composed with the character. For simplicity, let  $\chi(I)$  be shorthand for  $\chi((\frac{L/K}{I}))$ . Then  $L_K(s, \chi) = \prod_{\mathfrak{p} \in \text{Spec}(\mathcal{O}_K)^{ur}} (1 - \frac{\chi(\mathfrak{p})}{\mathfrak{p}^s}) = \sum_{I \in I^{ur}} \frac{\chi(I)}{N(I)^s}$ .

**Proposition 3.11.** *Let  $f_{\mathfrak{p}}$  be the residual degree of every prime over  $\mathfrak{p}$  in  $L$ , and let  $r_{\mathfrak{p}}$  be the number of factors  $\mathfrak{p}$  splits into.  $\zeta_L(s) = \prod_{\mathfrak{p} \notin \text{Spec}(\mathcal{O}_K)^{ur}} (1 - N(\mathfrak{p})^{-f_{\mathfrak{p}}s})^{r_{\mathfrak{p}}} \prod_{\chi \in \hat{G}} L(s, \chi)$ .  $\zeta_K(s, 1) = \zeta_{K, \text{Spec}(\mathcal{O}_K)^{ur}}(s)$ .*

*Proof.* The last identity is obvious, so we'll focus on the first. We can split the factors of  $(1 - N(\mathfrak{P})^{-s})^{-1}$  on the left hand side into Galois orbits. For each prime  $\mathfrak{p}$ , we will get  $\prod_{\mathfrak{P}/\mathfrak{p}} (1 - \frac{1}{N(\mathfrak{P})^s})^{-r_{\mathfrak{p}}}$ , and for the unramified primes, this factors into  $\prod_{\chi \in \hat{G}} (1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s})^{-1}$  by basic facts about characters of abelian groups, and how Frobenius relates to splitting.  $\square$

**Corollary 3.12.** *If  $\chi$  is a nontrivial Dirichlet character, then  $L(1, \chi) \neq 0$ .*

*Proof.* This follows from the above proposition, the fact that  $L(s, \chi)$  are holomorphic at 1 for nontrivial  $\chi$ , and the fact that  $L(s, 1), \zeta_{\mathbb{Q}[\zeta_m]}(s)$  have a simple pole at 1.  $\square$

From the proposition, it follows that if  $K$  is a subfield of a cyclotomic field (i.e. any abelian extension) where primes dividing  $m$  ramify, then the residue at 1 of  $\zeta_K(s)$  is also given by  $\prod_{p \nmid m} (1 - \frac{1}{p^{f_p}})^{r_p} (1 - \frac{1}{p})^{-1} \prod_{1 \neq \chi \in \hat{G}} L(1, \chi)$ , giving a class number formula. To compute this, we will need to evaluate  $L(1, \chi)$  for nontrivial characters.

**Theorem 3.13.** *Let  $\chi$  be a nontrivial Dirichlet character mod  $m$ . Then  $L(1, \chi) = -\frac{1}{m} \sum_1^{m-1} \tau_k(\chi) \log(1 - \omega^{-k})$  where  $\tau_k(\chi)$  is the Gauss sum  $\sum_{\mathbb{Z}/m\mathbb{Z}^\times} \chi(a) \omega^{ak}$ , and  $\omega$  a primitive  $m^{\text{th}}$  root of unity.*

*Proof.*  $L(s, \chi) = \sum_a \frac{\chi(a)}{a^s} = \sum_{b \in \mathbb{Z}/m\mathbb{Z}^\times} \chi(b) \sum_{a \equiv b \pmod{m}} \frac{\chi(a)}{a^s} = \frac{1}{m} \sum_{b \in \mathbb{Z}/m\mathbb{Z}^\times} \chi(b) \sum_a \frac{\sum_0^{m-1} \omega^{(b-a)k}}{a^s} = \frac{1}{m} \sum_1^{m-1} \tau_k(\chi) \sum_a \frac{\omega^{-ak}}{a^s}$ , and evaluating at  $s = 1$  gives the result.  $\square$

We can simplify this formula as follows: If  $\chi$  is a character mod  $m$  and is not induced from one mod  $n \neq m$ , then it is **primitive**. If  $\chi$  mod  $m$  is induced from  $\chi'$  mod  $n$ , then we have the formula  $L(s, \chi) = L(s, \chi') \prod_{p|m, p \nmid n} (1 - \frac{\chi'(p)}{p^s})$ , and every character is induced from a primitive one, so we only need to be able to compute  $L(s, \chi)$  for primitive characters. Let  $\tau(\chi) = \tau_1(\chi)$ . Then for any character mod  $m$ , if  $(k, m) = 1$ , it is easy to see  $\tau_k(\chi) = \bar{\chi}(k) \tau(\chi)$ . More generally,  $\tau_k(\chi) = \chi(1 + i \frac{m}{(m, k)}) \tau_k(\chi)$ , and so if  $\chi$  is primitive and  $(k, m) > 1$ , then we have  $\tau_k(\chi) = 0$ .

Thus  $L(1, \chi) = -\frac{\tau(\chi)}{m} \sum_{\mathbb{Z}/m\mathbb{Z}^\times} \bar{\chi}(k) \log(1 - \omega^{-k})$ .

## 4. DISTRIBUTION OF PRIMES

**Theorem 4.1** (Dirichlet's Theorem). *The polar density of primes in each relatively prime congruence class mod  $m$  are  $\frac{1}{\phi(m)}$ .*

*Proof.* Let  $(a, m) = 1$ ,  $\text{Re}(s) > 1$ .  $\sum_{p \equiv a \pmod{m}} \frac{1}{p^s} = \frac{1}{\phi(m)} \sum_p \frac{\sum_{\chi} \chi(a^{-1}p)}{p^s} = \frac{1}{\phi(m)} \sum_{\chi} \bar{\chi}(a) \sum_p \frac{\chi(p)}{p^s} = \frac{1}{\phi(m)} \sum_{\chi} \bar{\chi}(a) \log(L(s, \chi)) + O(1)$ . Now letting  $s$  near 1 and applying Corollary 3.12, it follows that all the terms in the sum are  $O(1)$  except for  $\log(L(s, 1))$ , which is  $\log(\zeta(s)) + O(1)$ , so we get  $= \frac{1}{\phi(m)} \log(\zeta(s)) + O(1)$ .  $\square$

One should note that the proof above works for any cyclotomic extension of number fields without any change other than restricting to primes with residual degree 1 over  $\mathbb{Q}$ .

We can improve the results of Theorem 3.8. First suppose that  $L/K$  has cyclic Galois group of order  $n$ .

**Lemma 4.2.** *The Dirichlet density of elements of order  $d|n$  is  $\frac{\phi(d)}{n}$ .*

*Proof.* The density of elements of order dividing  $d$  is  $\frac{d}{n}$  by Theorem 3.8. But then by Möbius inversion, we are done.  $\square$

**Theorem 4.3** (Frobenius Density Theorem). *Let  $L$  be a Galois extension of  $K$  with Galois group  $G$ , and let  $\sigma \in G$  be an element of order  $n$ . Then the set of primes in  $K$  with Frobenius  $\sigma^k$  has Dirichlet density  $c \frac{\phi(n)}{|G|}$ , where  $c$  is the index of the normalizer of  $\langle \sigma \rangle$  in  $G$ .*

*Proof.* We will ignore ramifying primes, and those in  $L^\sigma$  and  $K$  with inertial degree  $> 1$  over  $\mathbb{Q}$ . Let  $L^\sigma$  be the fixed field of  $\sigma$ . By the previous lemma, the set  $A$  of primes in  $L^\sigma$  with Frobenius  $\sigma^k$  has polar density  $\frac{\phi(d)}{n}$ . Now let  $B$  be the set of prime in  $K$  with Frobenius  $\sigma^k$  for some prime over them. Each prime in  $B$  has  $\frac{|G|}{n}$  primes above it in  $L$ , and the Galois group acts on these transitively, which acts on the decomposition group transitively by conjugation. Thus  $\frac{|G|}{nc}$  primes above the prime in  $B$  must have a Frobenius that works. Each of these gives a different element of  $A$  that restricts to  $B$ , so the restriction map from  $A$  to  $B$  is  $\frac{|G|}{nc}$  to 1. Looking at the level of zeta functions for  $A, B$ , since everything is inertial degree 1 over  $\mathbb{Q}$ , we immediately get that the polar density of  $B$  is  $\frac{c\phi(n)}{|G|}$ .  $\square$

The Chebotarev Density Theorem is a common generalization of both of the previous theorems. Here is a relatively simple approach to the Dirichlet density version of the theorem:

**Theorem 4.4** (Chebotarev Density Theorem). *Let  $L/K$  be a Galois extension of number fields, and let  $[\sigma]$  be a conjugacy class in the Galois group. The Dirichlet density of primes in the class  $[\sigma]$  is  $\frac{[\sigma]}{|G|}$ .*

*Proof.* First we'll reduce to the case of a cyclic extension using the same technique as in the previous. Given a prime  $p$  with Frobenius  $[\sigma]$ , note that it splits into  $\frac{|G|}{o(\sigma)}$  primes in  $L$ , and exactly  $\frac{1}{[\sigma]}$  of those have Frobenius actually  $\sigma$ . Combining this with the Dirichlet density for the cyclic case, along with ignoring primes ramifying or having nontrivial residual degree over  $\mathbb{Q}$ , we get the result.

Next, we will reduce to the case that  $L$  is a cyclotomic extension of  $K$ , which was proven in the remark after Dirichlet's theorem. If  $L$  is a cyclic extension, note that we only need to show that  $\frac{1}{|G|}$  is a lower bound on the lower Dirichlet density as the same lower bound on the rest of the elements of  $G$  will give the desired upper bound. This will be shown as follows: pick a prime  $m$  linearly disjoint from  $K$ , and consider  $L[\zeta_m]$ , whose Galois group can be identified with  $G \times \mathbb{Z}/m\mathbb{Z}^\times$ . Then if  $a \in \mathbb{Z}/m\mathbb{Z}^\times$  is an element with  $n$  dividing its order, then  $\langle(\sigma, a)\rangle \cap G \times \{1\}$  is a trivial group, which by Galois theory means that  $L[\zeta_m]/L[\zeta_m]^{(\sigma, a)}$  is a cyclotomic extension, so the density of primes for  $(\sigma, a)$  is what we want. In addition, the sum of the lower Dirichlet densities for the elements  $(\sigma, a)$  as  $a$  ranges in  $\mathbb{Z}/m\mathbb{Z}^\times$  is at most the lower density of  $\sigma$ . If  $H_m$  is the number of elements of  $\mathbb{Z}/m\mathbb{Z}^\times$  with  $n$  dividing its order, then the lower Dirichlet density is at least  $\frac{H_m}{(m-1)|G|}$ . Now we can choose by Dirichlet's theorem  $m \equiv 1 \pmod{n^k}$  for large  $k$  so that  $\frac{H_m}{m-1} \rightarrow 1$ .  $\square$