

## Problem Set 12.

1. Let  $K$  be a number field with maximal order  $\mathbf{O}_K$ . Show that there are infinitely many prime ideals  $P \subset \mathbf{O}_K$  such that  $NP$  is prime (that is, the residue degree  $f_P = 1$ ). Hint: Consider the behavior of  $\zeta_K(s)$  as  $s$  approaches 1, and use the fact that  $\sum n^{-2}$  converges. In many respects the zeta function near 1 only sees degree 1 primes.
2. “Elementary” proofs about the infinitude of primes in some arithmetic progressions can be obtained. Assume that we don’t use the density theorems of Dirichlet and Chebotarev. Let  $p$  be a fixed rational prime and let  $K = \mathbf{Q}(\zeta_p)$ ,  $F(x) = (x^p - 1)/(x - 1)$ .
  - a) Show that if  $m$  is an integer then all prime divisors of the ideal generated by  $F(m)$  in  $\mathbf{O}_K$  are primes of degree 1.
  - b) Suppose that  $Q$  is a prime of degree 1 in  $\mathbf{O}_K$ . Show that the norm of  $Q$  is either  $p$ , or a prime  $q$  congruent to 1 modulo  $p$ .
  - c) Prove that there are an infinite number of rational primes  $q$  congruent to 1 modulo  $p$  by using problem 1 and part b).
  - d) Alternatively, show that problem 1 can be avoided by considering a set of rational primes  $q_1, \dots, q_k$  which are congruent to 1 modulo  $p$ , and looking at prime factors of  $F(pq_1 \cdots q_k)$ , mimicking Euclid’s proof that there are infinitely many prime numbers
3. Let  $L/K$  be number fields and let  $S$  be the set of prime ideals in  $\mathbf{O}_K$  which split completely in  $L$ . The following exercises determine the Dirichlet density of  $S$ , that is

$$\lim_{s \rightarrow 1^+} \frac{\sum_{P \in S} NP^{-s}}{\sum_P NP^{-s}}.$$

- a) Show that as  $s$  approaches 1 through reals from above the function  $\log \zeta_K(s) - \sum_P NP^{-s}$  is bounded. Hint: take logarithms of the Euler product using that  $-\log(1 - z) = z + z^2/2 + \cdots$  and use the same idea as in problem 1.
- b) Let  $M/K$  be the Galois closure of  $L/K$ . Show that a prime splits completely in  $L/K$  if and only if it splits completely in  $M/K$ .
- c) Let  $T$  be the set of primes in  $\mathbf{O}_M$  lying above primes in  $S$ . Show that  $\log \zeta_M(s) - \sum_{Q \in T} NQ^{-s}$  is bounded as  $s$  approaches  $s$  from above by showing that  $T$  contains all primes  $Q$  with  $e_Q = 1, f_Q = 1$ .
- d) Show that  $\sum_{Q \in T} NQ^{-s} - [M : K] \sum_{P \in S} NP^{-s}$  is bounded as  $s$  approaches 1 from above. Hint: Compare the partial Euler product over primes in  $S$  and with that over primes in  $T$  and take logarithms.

- e) Use the results above to prove that  $\log \zeta_M(s) - [M : K] \sum_{P \in S} NP^{-s}$  is bounded as  $s$  approaches 1 from above. Conclude from the analytic class number formula that

$$\lim_{s \rightarrow 1^+} \frac{\sum_{P \in S} NP^{-s}}{-\log(s-1)} = \lim_{s \rightarrow 1^+} \frac{\sum_{P \in S} NP^{-s}}{\log(\zeta_M(s))} = \lim_{s \rightarrow 1^+} \frac{\sum_{P \in S} NP^{-s}}{\log(\zeta_K(s))} = 1/[M : K]$$

and that this equals the Dirichlet density given at the start of the problem.

- f) Let  $S(L)$  be the function that assigns to each Galois extension  $L$  of a number field  $K$  the set of primes of  $K$  which split completely in  $L$ . Show that if  $S(L)$  and  $S(L')$  agree except for a finite number of primes, then  $L$  and  $L'$  are isomorphic. Show by example that there exist field extensions  $E, E'$  (not necessarily Galois over  $K$ ) for which the set of primes splitting in  $E, E'$  agree but  $E, E'$  are not isomorphic fields.
- 4) The order of vanishing of various L-functions near  $s=1$  is crucial in many applications. These exercises give a proof of a form of the Chebotarev density theorem using one unproved analytic fact. The starting point is an Artin representation, that is a finite dimensional complex vector space  $V$  together with a homomorphism  $\rho$  of a Galois group  $Gal(L/K)$  to the linear automorphisms of  $V$ . For each prime  $v$  of  $K$ , let  $V^{I_v}$  be the subspace of vectors in  $V$  fixed by the linear maps coming from the inertia subgroup at  $v$ . The Artin L-function of this Artin representation is

$$L(s, V) = \prod_v \det(1 - Nv^{-s} \rho(Frob_v)|V^{I_v})^{-1}.$$

Note that even though the Frobenius element is only defined up to conjugation and a coset of  $I_v$ , the expression is well defined in that any choice of a Frobenius element gives the same factor.

- a) Let  $\chi(g) = \text{trace}(\rho(g))$  and  $\chi(Frob_v) = \text{trace}(Frob_v|V^{I_v})$ . Show that the function  $\log L(s, V) - \sum_P \chi(Frob_P) NP^{-s}$  is a continuous function for  $s > 1$  which is bounded as  $s$  approaches 1 from above. Conclude that the Artin L-series converges absolutely for real part of  $s$  greater than 1. Hint: for a matrix  $A$  the polynomial  $\det(1 - At) = 1 - \text{trace}(A)t + \dots$

The fact that we will not prove in general is that the order of vanishing of  $L(s, V)$  at  $s = 1$  is  $m_V = -\sum_{g \in G} \chi(g)/|G|$  (in the sense that  $\lim_{s \rightarrow 1^+} L(s, V)/(s-1)^{m_V}$  exists and is not zero). This fact can be derived from the Dirichlet class number formula and theorems describing  $L(s, V)$  as a product of ratios of Artin L-series for 1-dimensional representations.

- b) Let  $K = \mathbf{Q}$  and let  $L = \mathbf{Q}(\zeta_m)$  be the  $m$ -th cyclotomic field so that  $Gal(L/K)$  is an abelian group. Let  $V$  be a one dimensional representation of  $Gal(L/K)$ . Verify the fact above for  $V$  by showing that  $\lim_{s \rightarrow 1^+} (s-1)L(V, s)$  is nonzero if  $V$  is the trivial representation, while  $\lim_{s \rightarrow 1^+} L(V, s)$  is nonzero if  $V$  is not trivial, thus verifying the order of vanishing statement above for one dimensional Artin representations coming from cyclotomic extensions of the rationals. Hint: Use

the analytic class number formula for  $K$ , and for  $L$ , checking that the product of  $L(s, V)$  over all one dimensional representations  $V$  of the abelian group  $\text{Gal}(L, K)$  is the zeta function  $\zeta_L(s)$ .

- c) Show that if  $f(g)$  is a complex valued function on  $G = \text{Gal}(L/K)$  which is a complex linear combination of traces of Artin representations, then

$$\lim_{s \rightarrow 1^+} \frac{\sum f(\text{Frob}_v) N v^{-s}}{\log(\zeta_K(s))} = \sum_{g \in G} f(g) / |G|.$$

Note that  $f(\text{Frob}_v)$  is defined as the linear combination of the  $\chi(\text{Frob}_v)$  defined in a) when  $f(g)$  is a linear combination of traces.

- d) It is an algebraic fact that any complex function on a finite group  $G$  which is constant on conjugacy classes is a linear combination of traces of representations. Prove this for an abelian group.
- e) Let  $B$  be a conjugacy class in  $G$ . Using the fact preceding b) and that of d), use c) to prove the following version of Chebotarev density:

$$\lim_{s \rightarrow 1^+} \frac{\sum_{P | \text{Frob}_P \in B} N P^{-s}}{\log(\zeta_K(s))} = \lim_{s \rightarrow 1^+} \frac{\sum_{P | \text{Frob}_P \in B} N P^{-s}}{\sum_P N P^{-s}} = \frac{|B|}{|G|}.$$

- f) Conclude unconditionally that for a cyclotomic extension  $L/\mathbf{Q}$  and a fixed element  $g \in \text{Gal}(L/\mathbf{Q})$  there are infinitely many rational primes  $p$  for which  $\text{Frob}_p = g$ , and that the Dirichlet density of such primes is  $1/|\text{Gal}(L/\mathbf{Q})|$ . This proves Dirichlet's theorem on primes in arithmetic progression.