Math 129 Problem Set 11

Lev Kruglyak

May 12, 2022

Problem 7.7. Let A be a set of primes having polar density m/n in a number field K.

(a) Show that

$$\zeta_K(s)^m \prod_{\mathfrak{p}\in A}\left(1-\frac{1}{\|\mathfrak{p}\|^s}\right)^n$$

extends to a nonzero analytic function in a neighborhood of $s=1$.

(b) Prove that

$$n\sum_{\mathfrak{p}\in A}\frac{1}{\|\mathfrak{p}\|^s}-m\sum_{\text{all }\mathfrak{p}}\frac{1}{\|\mathfrak{p}\|^s}$$

extends to a nonzero analytic neighborhood of $s=1$.

(c) Prove that

$$\lim_{s\to 1^+}\frac{\sum_{\mathfrak{p}\in A}\|\mathfrak{p}\|^{-s}}{\sum_{\text{all }\mathfrak{p}}\|\mathfrak{p}\|^{-s}}=\frac{m}{n}$$

This limit is called the *Dirichlet density* of A.

(a) By definition of polar density, we know that the function $\zeta_{K,A}(s)^n$ can be extended to a meromorphic function around $s=1$ with a pole of order m at $s=1$. This means that $\zeta_{K,A}(s)^n(s-1)^m=g(s)$ is a nonzero analytic function in some neighborhood of $s=1$. Then in this neighborhood,

$$\zeta_K(s)^m\prod_{\mathfrak{p}\in A}\left(1-\frac{1}{\|\mathfrak{p}\|^s}\right)^n=\zeta_K(s)^m\zeta_{K,A}(s)^{-n}=\frac{\zeta_K(s)^m(s-1)^m}{g(s)}=\frac{(\zeta_K(s)(s-1))^m}{g(s)}.$$

Recall that $\zeta_K(s)$ has a simple pole at $s=1$ so $\zeta_K(s)(s-1)$ is analytic around $s=1$. Since $g(s)$ is nonzero around $s=1$, it follows that this function is analytic around $s=1$.

(b) We've proved in (a) that there is complex function $g(s)$, analytic around $s=1$ with

$$\frac{\zeta_K(s)^m}{\zeta_{K,A}(s)^n}=g(s).$$

Let's use the principal branch of the logarithm, then we have

$$m\log\zeta_K(s)-n\log\zeta_{K,A}(s)=m\sum_{\text{all }\mathfrak{p}}\log\left(1-\frac{1}{\|\mathfrak{p}\|^s}\right)-n\sum_{\mathfrak{p}\in A}\log\left(1-\frac{1}{\|\mathfrak{p}\|^s}\right)=\log g(s)$$

Using the Taylor expansion $\log(1-z)=-\sum_{n=1}^{\infty}\frac{z^n}{n}$, we can rewrite this as

$$\log g(s)=\left(n\sum_{\mathfrak{p}\in A}\frac{1}{\|\mathfrak{p}\|^s}-m\sum_{\text{all }\mathfrak{p}}\frac{1}{\|\mathfrak{p}\|^s}\right)+\sum_{\text{all }\mathfrak{p}}O\left(\frac{1}{\|\mathfrak{p}\|^{2s}}\right)$$

So if we can show that the sum $\sum_{\text{all } \mathfrak{p}} O\left(\|\mathfrak{p}\|^{-2s}\right)$ is analytic around $s=1$, we are done. But $\sum_{\text{all } \mathfrak{p}} \|\mathfrak{p}\|^{-2s}$ is bounded by $\sum_{I \subset \mathcal{O}_K} \|I\|^{-2s} = \zeta_K(2s)$. $\zeta_K(2s)$ is analytic around $s=1$, so we are done.

(c) Recall from (b) that we have

$$n \sum_{\mathfrak{p} \in A} \frac{1}{\|\mathfrak{p}\|^s} - m \sum_{\text{all } \mathfrak{p}} \frac{1}{\|p\|^s} = O(\log g(s) - \zeta_K(2s)).$$

In the limit as $s \to 1^+$, $\log g(s) - \zeta_K(2s)$ is constant since $g(s)$ is defined and nonzero at $s=1$, so we get

$$\lim_{s \to 1^+} \left(n \sum_{\mathfrak{p} \in A} \frac{1}{\|\mathfrak{p}\|^s} - m \sum_{\text{all } \mathfrak{p}} \frac{1}{\|\mathfrak{p}\|^s} \right) = \kappa \quad \text{for some } \kappa \in \mathbb{C}.$$

Rearranging, this means that

$$\lim_{s \to 1^+} \left(\frac{\sum_{\mathfrak{p} \in A} \|\mathfrak{p}\|^{-s}}{\sum_{\text{all } \mathfrak{p}} \|\mathfrak{p}\|^{-s}} \right) = \lim_{s \to 1^+} \left(\frac{\kappa}{n \sum_{\text{all } \mathfrak{p}} \|\mathfrak{p}\|^{-s}} \right) + \frac{m}{n} = \frac{m}{n}.$$

The limit in the middle vanishes because

$$\lim_{s \to 1^+} \sum_{\text{all } \mathfrak{p}} \|\mathfrak{p}\|^{-s} \to \infty.$$

Problem 7.8. Use Corollary 2 of Theorem 43 to determine the density of the set of primes $p \in \mathbb{Z}$ such that

(a) 2 is a square mod p,

(b) 2 is a cube mod p,

(c) 2 is a fourth power mod p.

As a reminder, the corollary states

Corollary. Let K be a number field and let f be a monic irreducible polynomial over $\mathcal{O}_K$. Let A be the set of primes $\mathfrak{p}$ of $\mathcal{O}_K$ such that f splits into linear factors over $\mathcal{O}_K/\mathfrak{p}$. Then A has polar density $1/[L:K]$ where L is the splitting field of f over K.

Let $K = \mathbb{Q}$ so that $\mathcal{O}_K = \mathbb{Z}$.

(a) Let $f(x) = x^2 - 2 \in \mathbb{Z}[x]$. This is monic irreducible over $\mathbb{Z}$, and A is the set of primes p such that $x^2 - 2$ splits in $\mathbb{Z}_p[x]$, which is exactly the set of primes p for which 2 is a square mod p. The corollary then tells us that $\delta(A) = 1/2$.

(b) First suppose $p \not\equiv 1 \mod 3$. Then there is a group homomorphism $\mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$ which sends $x \mapsto x^3$. Since $\mathbb{Z}_p^\times$ is cyclic, the kernel of this map is the set of elements whose order divides 3, yet since $3 \nmid p-1$, this map is an isomorphism so every number is a cube mod p. The set of primes with $p \not\equiv 1 \mod 3$ has density $1/2$.

Next, if $p \equiv 1 \mod 3$, we claim that $x^3 - 2$ splits completely mod p if and only if 2 is a cube mod p. This can also be seen in a similar way using the homomorphism $\mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$. Then applying the corollary, we see that the density of these primes is $1/6$ since the splitting field of $x^3 - 2$ is $\mathbb{Q}[\sqrt[3]{2}, i\sqrt{3}]$. So the total density is $1/2 + 1/6 = 2/3$ by a result proved on the previous homework set.

(c) We can use the same argument as in the previous part to deduce that $x^4 - 2$ splits completely when $p \equiv 1 \mod 4$ iff 2 is a 4-th power mod p. The density here is $1/8$ since the splitting field of $x^4 - 2$ is $\mathbb{Q}[\sqrt[4]{2}, i]$. If $p \equiv 3$

mod 4, we have two cases, $p \equiv 3 \mod 8$ and $p \equiv 7 \mod 8$. In the first case, 2 is not a quadratic residue mod p, so it cannot be a quartic residue. When $p \equiv 7 \mod 8$, 2 is a quadratic residue, so either $\sqrt{2}$ or $-\sqrt{2}$ is a quadratic residue mod p, so 2 must be a 4-th power mod p. The density here is $1/4$. Thus the total density is $3/8$.

Problem 7.10. Let L be a normal extension of K with cyclic Galois group G of order n. For each divisor d of n, let A_d be the set of primes $\mathfrak{p}$ of K which are unramified in L and such that $\phi(\mathfrak{q} \mid \mathfrak{p})$ has order d for some prime $\mathfrak{q}$ of L lying over $\mathfrak{p}$. Equivalently, this holds for all $\mathfrak{q}$ over $\mathfrak{p}$. Prove that A_d has polar density $\varphi(d)/n$.

Let B_d be the set of unramified primes $\mathfrak{p}$ of K such that $\phi(\mathfrak{p} \mid \mathfrak{q})$ has order dividing d. This corresponds to the subgroup $H \subset \mathrm{Gal}(L/K)$ of elements of order dividing d. Then Corollary 4 implies that $\delta(B_d) = d/n$ since $|H| = d$. Then

$$B_d = \bigsqcup_{d' \mid d} A_{d'} \implies \delta(B_d) = \sum_{d' \mid d} \delta(A_{d'}) = \frac{d}{n}$$

Applying Möbius inversion to this summation, we get

$$n\delta(A_d) = \sum_{d' \mid d} \mu(d') \frac{d}{d'} = \varphi(d).$$

And so $\delta(A_d) = \frac{\varphi(d)}{n}$ as desired.

Problem 7.13. Let K be a number field and let g be a monic irreducible polynomial over $\mathcal{O}_K$. Let M be the splitting field of g over K and let $L = K[\alpha]$ for some root α of g.

(a) Prove that for all but finitely many primes $\mathfrak{p}$ of K, the following are equivalent:

(i) g has a root mod $\mathfrak{p}$;

(ii) $f(\mathfrak{q} \mid \mathfrak{p}) = 1$ for some prime $\mathfrak{q}$ of L lying over $\mathfrak{p}$;

(iii) $\phi(\mathfrak{u} \mid \mathfrak{p})$ fixes L for some prime $\mathfrak{u}$ of M lying over $\mathfrak{p}$.

(b) Show that a finite group G cannot be the union of the conjugates of a proper subgroup H.

(c) Prove that there are infinitely many primes $\mathfrak{p}$ of K such that g has no roots mod $\mathfrak{p}$.

(a) Let's start with (i) $\to$ (ii). Since g has a root mod $\mathfrak{p}$, then g must have some linear factor $(x - \beta)$ in $(\mathcal{O}_K/\mathfrak{p})[x]$. By Theorem 27, for all but finitely many $\mathfrak{p}$, there must be a $\mathfrak{q}_i$ lying over $\mathfrak{p}$ with $f(\mathfrak{q}_i \mid \mathfrak{p}) = \deg(x - \beta) = 1$ as desired.

Next we'll prove (ii) $\to$ (iii). Suppose $f(\mathfrak{q} \mid \mathfrak{p}) = 1$. Let $\mathfrak{u}$ be a prime of M lying over $\mathfrak{p}$. Then $\phi(\mathfrak{u} \mid \mathfrak{p})$ is the generator of $\mathrm{Gal}((\mathcal{O}_M/\mathfrak{u})/(\mathcal{O}_K/\mathfrak{p}))$. Then $\phi(\mathfrak{u} \mid \mathfrak{p})$ lifts to an element in $D(\mathfrak{u} \mid \mathfrak{p})$. Since $f(\mathfrak{q} \mid \mathfrak{p})$, we have $\mathcal{O}_L/\mathfrak{q} \cong \mathcal{O}_K/\mathfrak{p}$, so $\phi(\mathfrak{u} \mid \mathfrak{p})$ generates the aforementioned Galois group. Then it also must lift to a Galois automorphism in $\mathrm{Gal}(M/L)$ so $\phi(\mathfrak{u} \mid \mathfrak{p})$ fixes L.

Finally, let's prove (iii) $\to$ (i). Suppose $\phi(\mathfrak{u} \mid \mathfrak{p})$ fixes L. Then letting $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/L)$ and $\phi(\mathfrak{u} \mid \mathfrak{p}) \in H\sigma_i$, it follows from Theorem 33 that $f(\mathfrak{q}_i \mid \mathfrak{p}) = 1$ and so we are done.

(b) Let H be a proper subgroup of G. The number of conjugates is the index of the normalizer, which is at most the index of H because $H \subset N_G(H)$ for any H. Let n be the number of distinct elements in the conjugates of H. Since all conjugates of H contain the identity, we have $n < |H|[G : N_G(H)]$. Then $n < |H|[G : N_G(H)] \leq |H|[G : H] = |G|$. This is a contradiction because Gcontains more elements than conjugates of H can cover, so G cannot be the union of conjugates of H.

(c) Let $H = \mathrm{Gal}(M/L)$, and suppose $\mathfrak{p}$ is a prime such that g has no roots mod $\mathfrak{p}$. Then (a) tells us that apart from finitely many primes, $\phi(\mathfrak{u} \mid \mathfrak{p}) \in H$. Furthermore, the conjugacy class of $\phi(\mathfrak{u} \mid \mathfrak{p})$ is uniquely determined by $\mathfrak{p}$. Let's pick a representative $\sigma \in H$ from each conjugacy class of G that intersects H nontrivially. Then by the Chebotarev density theorem, the density of the primes such that g has a root mod $\mathfrak{p}$ is $\sum_\sigma c_\sigma/|G|$. It's clear to see that $0 < d < 1$, so we are done.

Problem 7.14. Let K, L, M, and g be as in the previous exercise.

(a) Prove that for all but finitely many primes $\mathfrak{p}$ of K, the following are equivalent:

(i) g is irreducible mod $\mathfrak{p}$.

(ii) $\mathfrak{p}$ is inert in L.

(iii) $f(\mathfrak{q} \mid \mathfrak{p})$ is equal to the degree of g for some prime $\mathfrak{q}$ of L lying over $\mathfrak{p}$.

(b) Prove that if g has prime degree p, then g is irreducible mod $\mathfrak{p}$ for infinitely many primes $\mathfrak{p}$ of K.

(a) Theorem 27 immediately shows that these are equivalent.

(b) Let $\sigma \in \mathrm{Gal}(M/K)$ be an element of order p. Then Chebotarev density theorem tells us that the set of primes $\mathfrak{p}$ of K unramified in M such that $\phi(\mathfrak{u} \mid \mathfrak{p}) = \sigma$ has nonzero density. So there are infinitely many such primes. The result then follows since if we have some $\mathfrak{u}$ over $\mathfrak{p}$ such that $f(\mathfrak{u} \mid \mathfrak{p}) = p$, then g is irreducible mod $\mathfrak{p}$.

Problem 7.15.

(a) Let G be a cyclic group of order n. Show that the character group $\widehat{G}$ is also cyclic of order n.

(b) Let G and H be finite abelian groups. Show that there is an isomorphism

$$\widehat{G} \times \widehat{H} \to \widehat{G \times H}.$$

(c) Let G be a finite abelian group. Prove that $\widehat{G}$ is isomorphic G.

(a) Let g be a generator of G. Then consider the character $\chi_g : G \to \mathbb{C}$ which sends g to a primitive n-th root of unity. This clearly has order n, so $\chi_g^n = \mathrm{Id}$ and $n \mid |\widehat{G}|$. Now suppose $\chi \in \widehat{G}$ is some arbitrary character. Since $\chi^n = \mathrm{Id}$, and it is entirely determined by where the identity element of the group maps to. However this identity element maps to any n-th root of unity. The group of n-th roots of unity are exactly G so we are done.

(b) Let $\chi_1 : G \to \mathbb{C}$ and $\chi_2 : H \to \mathbb{C}$ be characters. Consider the character $\chi_1 \times \chi_2 : G \to H \to \mathbb{C}$ given by $(\chi_1 \times \chi_2)(g, h) = \chi_1(g) \cdot \chi_2(h)$. This is clearly reversible since given $\chi \in \widehat{G \times H}$ we can set $\chi_1 = \chi(-, 1)$ and $\chi_2 = \chi(1, -)$.

(c) Since $\mathbb{Z}/n\mathbb{Z} \cong \widehat{\mathbb{Z}/n\mathbb{Z}}$ by (a), for any finite abelian group of the form $\prod_i \mathbb{Z}/n_i\mathbb{Z}$ we apply (b) to show that it is isomorphic to $\widehat{\prod_i \mathbb{Z}/n_i\mathbb{Z}}$.