WEEK 6 SOLUTION

Exercise 1. *Let H be a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ and define*

$$\mathcal{S} = \{p \text{ prime in } \mathbb{Z} : p + n\mathbb{Z} \in H\}.$$

Compute the Dirichlet density $\delta(\mathcal{S})$ in terms of $|H|$, and prove your result.

Proof. Let $H \subset (\mathbb{Z}/n\mathbb{Z})^\times$ be a subgroup. Each element $h \in H$ corresponds to a residue $a \pmod n$. Then

$$\mathcal{S} = \bigcup_{a \in H} \{p \mid p \equiv a \pmod n\}.$$

Hence it suffices to compute the density of primes in a given residue class $p \equiv a \pmod n$.

For a Dirichlet character $\chi \pmod n$,

$$\log L(s,\chi) = \sum_p \frac{\chi(p)}{p^s} + R(s),$$

where $R(s)$ converges for $\mathrm{Re}(s) > 1/2$. Thus, as $s \to 1^+$,

$$\log L(s,\chi) \sim \sum_p \frac{\chi(p)}{p^s}.$$

Using orthogonality of Dirichlet characters,

$$\frac{1}{\varphi(n)} \sum_{\chi \bmod n} \overline{\chi}(a)\chi(p) = \begin{cases} 1, & p \equiv a \pmod n, \\ 0, & \text{otherwise.} \end{cases}$$

Applying this to $\log L(s,\chi)$, we get

$$\sum_{\chi \bmod n} \overline{\chi}(a) \log L(s,\chi) \sim \sum_{p \equiv a \pmod n} \varphi(n) \frac{1}{p^s}.$$

For the trivial character χ_0,

$$L(s,\chi_0) = \prod_{p \mid n} \left(1 - \frac{1}{p^s}\right) \zeta(s) \sim \zeta(s) \quad \text{as } s \to 1^+.$$

Hence

$$\sum_{p \equiv a \pmod n} \frac{1}{p^s} \sim \frac{1}{\varphi(n)} \log \zeta(s).$$

Summing over all residues $a \in H$ gives

$$\sum_{a \in H} \sum_{p \equiv a \pmod n} \frac{1}{p^s} \sim \frac{|H|}{\varphi(n)} \log \zeta(s).$$

By definition,

$$\delta(\mathcal{S}) = \lim_{s\to 1^+} \frac{\sum_{p\in\mathcal{S}} p^{-s}}{\log \frac{1}{s-1}}.$$

Since $\log\zeta(s) \sim \log\frac{1}{s-1}$ as $s \to 1^+$, we conclude

$$\delta(\mathcal{S}) = \frac{|H|}{\varphi(n)}.$$

□

Exercise 2. *Let K/F be a finite Galois extension of number fields and write $[K : F] = d$. Let*

$$\mathcal{S}_{K/F} = \{\mathfrak{p} \subset \mathcal{O}_F : \ \mathfrak{p} \text{ prime and } \mathfrak{p} \text{ splits completely in } K/F\}.$$

Then the Dirichlet density of $\mathcal{S}_{K/F}$ (relative to F) exists and

$$\delta_F(\mathcal{S}_{K/F}) = \frac{1}{[K : F]} = \frac{1}{d}.$$

Proof. Let $\zeta_K(s) = \prod_{\mathfrak{P}\subset\mathcal{O}_K}(1 - N\mathfrak{P}^{-s})^{-1}$ be the Dedekind zeta function of K, which converges for $\Re(s) > 1$. For $s > 1$ real we have

$$\log\zeta_K(s) \ = \ -\sum_{\mathfrak{P}} \log\big(1 - N\mathfrak{P}^{-s}\big) \ = \ \sum_{\mathfrak{P}}\sum_{n\geqslant 1} \frac{1}{n} N\mathfrak{P}^{-ns}.$$

Group the sum over prime ideals $\mathfrak{P}$ of $\mathcal{O}_K$ by the prime ideals $\mathfrak{p}$ of $\mathcal{O}_F$ below them. For each prime $\mathfrak{p} \subset \mathcal{O}_F$ write $g(\mathfrak{p})$ for the number of primes of $\mathcal{O}_K$ lying above $\mathfrak{p}$ (so $1 \leqslant g(\mathfrak{p}) \leqslant d$), and write $N\mathfrak{p}$ for the absolute norm from F to $\mathbb{Q}$. Then

Split the inner n–sum into the $n = 1$ term and the tail $n \geqslant 2$:

$$\log\zeta_K(s) = \sum_{\mathfrak{P},f(\mathfrak{P}/\mathfrak{p})=1=e(\mathfrak{P}/\mathfrak{p})} (N\mathfrak{p})^{-s} + \sum_{\mathfrak{P},n>1} (N\mathfrak{P})^{-ns} + \sum_{\mathfrak{P},f(\mathfrak{P}/\mathfrak{p})>1} (N\mathfrak{p})^{-f(\mathfrak{P}/\mathfrak{p})s} + \sum_{\mathfrak{P},f(\mathfrak{P}/\mathfrak{p})=1,e(\mathfrak{P}/\mathfrak{p})>1} (N\mathfrak{p})^{-s}$$

The second term converge when $s \to 1^+$, the forth term is finite as only finite primes ramified, and the third term converges because $f(\mathfrak{P}/\mathfrak{p}) > 1$.

Hence as $s \to 1^+$ the main growth of $\log\zeta_K(s)$ comes from the first term

$$\sum_{\mathfrak{p}} g(\mathfrak{p})\,(N\mathfrak{p})^{-s}.$$

Now separate the contribution from primes that split completely and the rest. Therefore

$$\log\zeta_K(s) \sim \sum_{\mathfrak{p}\in\mathcal{S}_{K/F}} d\,(N\mathfrak{p})^{-s} \qquad \text{as } s \to 1^+,$$

where "$\sim$" means the difference is bounded as $s \to 1^+$.

On the other hand $\zeta_K(s)$ and $\zeta_F(s)$ both have a simple pole at $s = 1$, hence

$$\log\zeta_K(s) \sim \log\zeta_F(s) \sim \log\frac{1}{s-1} \qquad (s \to 1^+).$$

Combining the two asymptotics yields

$$\log \frac{1}{s-1} \sim d \sum_{\mathfrak{p} \in \mathcal{S}_{K/F}} (N\mathfrak{p})^{-s} \qquad (s \to 1^+).$$

Rearranging and using the definition of Dirichlet density relative to F,

$$\delta_F(\mathcal{S}_{K/F}) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in \mathcal{S}_{K/F}} (N\mathfrak{p})^{-s}}{\log \frac{1}{s-1}} = \frac{1}{d},$$

as desired. □

Exercise 3. *Let E and K be number fields, each of which is Galois over $\mathbb{Q}$. Show that for any prime $p \in \mathbb{Z}$, p splits completely in both $E/\mathbb{Q}$ and $K/\mathbb{Q}$ if and only if p splits completely in their compositum extension $L = EK$ over $\mathbb{Q}$.*

Proof. Let $L = EK$. Since both $E/\mathbb{Q}$ and $K/\mathbb{Q}$ are Galois, so is $L/\mathbb{Q}$.

We first recall a simple fact: if $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ restricts to the identity on both E and K, then $\sigma = \mathrm{id}_L$. Indeed, since L is generated by E and K, for any $x = \sum_i e_i k_i$ with $e_i \in E, k_i \in K$, we have

$$\sigma(x) = \sum_i \sigma(e_i)\sigma(k_i) = \sum_i e_i k_i = x.$$

(⇒) Suppose p splits completely in $L/\mathbb{Q}$. Let $\mathfrak{P}$ be a prime of $\mathcal{O}_L$ lying above p. Then the residue degree and ramification index of $\mathfrak{P}$ over p are both 1. Let $\mathfrak{p}_E = \mathfrak{P} \cap \mathcal{O}_E$ and $\mathfrak{p}_K = \mathfrak{P} \cap \mathcal{O}_K$. Then $f(\mathfrak{p}_E|p)$ and $f(\mathfrak{p}_K|p)$ must divide $f(\mathfrak{P}|p) = 1$, so they are also 1, and the same holds for ramification indices. Thus p splits completely in both E and K.

Equivalently, if the Frobenius element $\mathrm{Frob}_{\mathfrak{P}}$ in $\mathrm{Gal}(L/\mathbb{Q})$ is the identity, its images in $\mathrm{Gal}(E/\mathbb{Q})$ and $\mathrm{Gal}(K/\mathbb{Q})$ are also identities, so p splits completely in E and K.

(⇐) Conversely, suppose p splits completely in both $E/\mathbb{Q}$ and $K/\mathbb{Q}$. Then p is unramified in both fields, hence also unramified in L. Let $\mathfrak{P}$ be a prime of L above p, and let $\mathrm{Frob}_{\mathfrak{P}} \in \mathrm{Gal}(L/\mathbb{Q})$ denote its Frobenius element.

Since p splits completely in E and K, the Frobenius elements in $\mathrm{Gal}(E/\mathbb{Q})$ and $\mathrm{Gal}(K/\mathbb{Q})$ are both trivial. Thus the restrictions of $\mathrm{Frob}_{\mathfrak{P}}$ to E and K are both the identity. By the fact noted above, this implies $\mathrm{Frob}_{\mathfrak{P}} = \mathrm{id}_L$. Hence p splits completely in L.

□

Exercise 4. *Let F be a number field and let $\mathfrak{m} \subset \mathcal{O}_F$ be a non-zero ideal. Let $P^+_{F,\mathfrak{m}}$ be the subgroup of P_F generated by*

$$\big\{ \langle \alpha \rangle : \alpha \in \mathcal{O}_F,\ \alpha \equiv 1 \pmod{\mathfrak{m}},\ \alpha \gg 0 \big\}.$$

Show the two equalities:

$$P^+_{F,\mathfrak{m}} = \big\{ \langle \alpha \rangle : \alpha \in F^\times,\ \alpha \gg 0,\ \alpha \overset{\times}{\equiv} 1 \pmod{\mathfrak{m}} \big\}$$

$$= \big\{ \langle \tfrac{\alpha}{\beta} \rangle : \alpha, \beta \in \mathcal{O}_F \text{ prime to } \mathfrak{m},\ \alpha \equiv \beta \pmod{\mathfrak{m}},\ \tfrac{\alpha}{\beta} \gg 0 \big\}.$$

Proof. We first prove the second equality.

$$\begin{aligned}
P^+_{F,\mathfrak{m}} &= \langle\, \langle\alpha\rangle : \alpha \in \mathcal{O}_F,\ \alpha \equiv 1 \pmod{\mathfrak{m}},\ \alpha \gg 0 \,\rangle \\
&= \left\{ \left\langle \prod_i \alpha_i^{\delta_i} \right\rangle \;\middle|\; \alpha_i \in \mathcal{O}_F,\ \alpha_i \equiv 1 \pmod{\mathfrak{m}},\ \alpha_i \gg 0,\ \delta_i = \pm 1 \right\} \\
&\subset \left\{ \left\langle \frac{\prod_{\delta_i>0} \alpha_i}{\prod_{\delta_j<0} \alpha_j} \right\rangle \;\middle|\; \alpha_i, \alpha_j \in \mathcal{O}_F,\ \alpha_i, \alpha_j \equiv 1 \pmod{\mathfrak{m}},\ \frac{\prod_{\delta_i>0} \alpha_i}{\prod_{\delta_j<0} \alpha_j} \gg 0 \right\} \\
&\subset \left\{ \left\langle \tfrac{\alpha}{\beta} \right\rangle : \alpha, \beta \in \mathcal{O}_F \text{ prime to } \mathfrak{m},\ \alpha \equiv \beta \pmod{\mathfrak{m}},\ \tfrac{\alpha}{\beta} \gg 0 \right\}.
\end{aligned}$$

To prove the reverse inclusion, take $\langle \frac{\alpha}{\beta} \rangle$ with $\alpha, \beta \in \mathcal{O}_F$ prime to $\mathfrak{m}$ and $\alpha \equiv \beta \pmod{\mathfrak{m}}$. Then $(\alpha) + \mathfrak{m} = \mathcal{O}_F$, so we can find $\gamma \in \mathcal{O}_F$ such that $\alpha\gamma \equiv 1 \pmod{\mathfrak{m}}$. Hence $\langle \frac{\alpha}{\beta} \rangle = \langle \alpha\gamma \rangle \langle \beta\gamma \rangle^{-1} = \langle (\alpha\gamma)^2 \rangle \langle (\beta\gamma)(\alpha\gamma) \rangle^{-1}$, and both $(\alpha\gamma)^2$ and $(\beta\gamma)(\alpha\gamma)$ satisfy the defining conditions ($(\alpha\gamma)^2 \equiv 1 \pmod{\mathfrak{m}}$ and $(\alpha\gamma)^2 \gg 0$), so the reverse inclusion holds. Thus the second equality is proved.

Now we prove the first equality. One direction is trivial:

$$\left\{ \left\langle \tfrac{\alpha}{\beta} \right\rangle : \alpha, \beta \in \mathcal{O}_F \text{ prime to } \mathfrak{m},\ \alpha \equiv \beta \pmod{\mathfrak{m}},\ \tfrac{\alpha}{\beta} \gg 0 \right\} \subset \{ \langle \alpha \rangle : \alpha \in F^\times,\, \alpha \gg 0,\, \alpha \overset{\times}{\equiv} 1 \pmod{\mathfrak{m}} \}.$$

Conversely, let $\alpha \in F^\times$ with $\alpha \gg 0$ and $\alpha \overset{\times}{\equiv} 1 \pmod{\mathfrak{m}}$. Write $\alpha = \beta/\gamma$ with $\beta, \gamma \in \mathcal{O}_F$. Let

$$\beta = \prod_{p \mid \mathfrak{m}} p^{e_p} \prod_{q \nmid \mathfrak{m}} q^{e_q}, \qquad \gamma = \prod_{p \mid \mathfrak{m}} p^{f_p} \prod_{q \nmid \mathfrak{m}} q^{f_q}.$$

Since $\alpha \overset{\times}{\equiv} 1 \pmod{\mathfrak{m}}$, we have $e_p = f_p$ for all $p \mid \mathfrak{m}$. Choose an element ω satisfying

$$\begin{cases} v_p(\omega) = -f_p, & \text{for all } p \mid m, \\ v_q(\omega) > 0, & \text{for all } q \nmid m. \end{cases}$$

Then both $\beta\omega$ and $\gamma\omega$ are in $\mathcal{O}_F$, prime to $\mathfrak{m}$, and $\beta\omega \equiv \gamma\omega \pmod{\mathfrak{m}}$. Hence

$$\langle \alpha \rangle = \langle \tfrac{\beta}{\gamma} \rangle = \langle \tfrac{\beta\omega}{\gamma\omega} \rangle,$$

so the reverse inclusion holds. This completes the proof. □