Reminder:

Consider a number field K and a subset A of the set P of maximal ideals of $\mathcal{O}_K$.

Proposition 7.2.5: We have

$$\sum_{\mathfrak{p}\in P} \mathrm{Nm}(\mathfrak{p})^{-s} = \log\frac{1}{s-1} + O(1) \text{ for real } s \to 1+.$$

Definition 7.4.1: The *Dirichlet density of* A, if it exists, is the value

$$\mu(A) \;:=\; \lim_{s\to 1+} \frac{\sum_{\mathfrak{p}\in A} \mathrm{Nm}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}\in P} \mathrm{Nm}(\mathfrak{p})^{-s}}.$$

Similarly the *upper Dirichlet density* $\overline{\mu}(A) := \limsup\ldots$ and the *lower Dirichlet density* $\underline{\mu}(A) := \liminf\ldots$.

Proposition 7.4.2: (a) We have $0 \leqslant \underline{\mu}(A) \leqslant \overline{\mu}(A) \leqslant 1$.

(b) For any subset $B \subset A$ we have $\overline{\mu}(B) \leqslant \overline{\mu}(A)$ and $\underline{\mu}(B) \leqslant \underline{\mu}(A)$, and also $\mu(B) \leqslant \mu(A)$ if these exist.

(c) We have $\mu(A) = 0$ if A is finite.

(d) We have $\mu(A) = 1$ if $P \smallsetminus A$ is finite.

(e) For any disjoint subsets $A, B \subset P$, if two of $\mu(A)$, $\mu(B)$, $\mu(A\cup B)$ exist, then so does the third and we have $\mu(A) + \mu(B) = \mu(A \cup B)$.

7.5 Primes of absolute degree 1

$= [k(\mathfrak{p})/\mathbb{F}_p]$

Definition 7.5.1: The *absolute degree* of a prime $\mathfrak{p}$ of $\mathcal{O}_K$ is the degree of $k(\mathfrak{p})$ over its prime field.

Proposition 7.5.2: The set of primes of absolute degree 1 has Dirichlet density 1.

Equivalent: ... ≥ 2 ... 0

Proof: Let $n = [K/\mathbb{Q}]$ $\Rightarrow$ $\forall p$ rational prime there are $\leq n$ primes $\mathfrak{p} < \mathcal{O}_K$ above p.

$$\Rightarrow \sum_{\substack{\mathfrak{p} \in P \\ \text{abs. degree} \geq 2}} Nm(\mathfrak{p})^{-s} \leq \sum_{\substack{p \text{ rat'l} \\ \text{prime}}} \sum_{\substack{\mathfrak{p} | p \\ \text{degree} \geq 2}} (p^2)^{-s} \leq n \cdot \sum_p p^{-2s} \leq n \cdot \zeta(2s) = O(1) \text{ near } s = 1.$$

$\Rightarrow$ dens $= 0$. qed.

Proposition 7.5.3: A subset $A \subset P$ has a Dirichlet density if and only if the set of all $\mathfrak{p} \in A$ of absolute degree 1 has a Dirichlet density, and then they are equal.

Proof: $A_1 := \{\mathfrak{p} \in A \mid \text{abs. degree } 1\} \subset A \overset{7.5.2}{\Rightarrow} \mu(A \setminus A_1) = 0$

$\Rightarrow \mu(A) = \mu(A_1)$. qed.

For any finite galois extension of number fields L/K we let $\mathrm{Split}_{L/K}$ denote the set of primes $\mathfrak{p} \subset \mathcal{O}_K$ that are totally split in $\mathcal{O}_L$.

$$\begin{array}{ccc} L & \mathcal{O}_L & \mathfrak{P} \\ | & | & | \\ K & \mathcal{O}_K & \mathfrak{p} \end{array}$$

Proposition 7.5.4: $\mathrm{Split}_{L/K}$ has Dirichlet density $\frac{1}{[L/K]}$. In particular it is infinite.

Proof: $\forall \mathfrak{p} \subset \mathcal{O}_K : [L/K] = r_\mathfrak{p} \cdot e_\mathfrak{p} \cdot f_\mathfrak{p}$

$\mathfrak{p} \in \mathrm{Split}_{L/K} \iff e_\mathfrak{p} = f_\mathfrak{p} = 1. \iff r_\mathfrak{p} = [L/K]$

$\exists$ precisely $[L/K]$ such $\mathfrak{P}$ over any $\mathfrak{p} \in \mathrm{Split}\, L/K$.

$\tilde{S} := \{ \mathfrak{P} \subset \mathcal{O}_L \mid \mathfrak{P} | \mathfrak{p} \in \mathrm{Split}_{L/K} \}$

$\Rightarrow \forall \mathfrak{P} \subset \mathcal{O}_L : \mathfrak{P} \notin \tilde{S} \iff$ $\left\{ \begin{array}{l} e_\mathfrak{p} > 1 \rightsquigarrow \mathfrak{p} \text{ ramified in } \mathcal{O}_L \Rightarrow \text{finitely many!} \\ \text{or } f_\mathfrak{p} > 1 \rightsquigarrow \mathfrak{P} \text{ has absolute degree} \geq f_\mathfrak{p} > 1. \end{array} \right\}$ These do not contribute to the Dirichlet density in L.

$\Rightarrow \mu(\{\mathfrak{P} \subset \mathcal{O}_L \mid \mathfrak{P} \notin \tilde{S}\}) = 0. \Rightarrow \mu(\tilde{S}) = 1$

$$\Rightarrow \mu(\mathrm{Split}_{L/K}) = \lim_{s \to 1+} \frac{\sum_{\mathfrak{p} \in \mathrm{Split}\, L/K} \mathrm{Nm}(\mathfrak{p})^{-s}}{\log\left(\frac{1}{s-1}\right)} = \lim_{s \to 1+} \frac{\frac{1}{[L/K]} \cdot \sum_{\mathfrak{P} \in \tilde{S}} \mathrm{Nm}(\mathfrak{P})^{-s}}{\log\left(\frac{1}{s-1}\right)} = \frac{1}{[L/K]} \mu(\tilde{S}) = \frac{1}{[L/K]}$$

good

Now consider two finite galois extensions of number fields $L, L'/K$.

Proposition 7.5.5: Then $\mathrm{Split}_{LL'/K} = \mathrm{Split}_{L/K} \cap \mathrm{Split}_{L'/K}$.

Proof: let $\Gamma := \mathrm{Gal}(L/K)$ $\qquad \tilde{\Gamma} \hookrightarrow \Gamma \times \Gamma'$

$\Gamma' := \mathrm{Gal}(L'/K)$

$$\begin{array}{ccc} \tilde{\Gamma}_{\tilde{\mathfrak{P}}} < \tilde{\Gamma} := \mathrm{Gal}(LL'/K) & \twoheadrightarrow & \Gamma, \quad \Gamma' \\ \vee & & \vee \quad\;\; \vee \\ \tilde{\Gamma}_{\tilde{\mathfrak{P}}} & \twoheadrightarrow & \Gamma_\mathfrak{P}, \quad \Gamma'_{\mathfrak{P}'} \end{array}$$

$\tilde{\Gamma}_{\tilde{\mathfrak{P}}}$ = decomposition group of $\tilde{\mathfrak{P}}$

$$\begin{array}{ccccc} & & \tilde{\mathfrak{P}} & & \\ & / & & \backslash & \\ \mathfrak{P} & & & & \mathfrak{P}' \\ & \backslash & & / & \\ & & \mathfrak{p} & & \end{array} \qquad \begin{array}{ccccc} & & LL' & & \\ & / & & \backslash & \\ L & & & & L' \\ & \backslash & & / & \\ & & K & & \end{array} \qquad \begin{array}{ccccc} & & 1 & & \\ & / & & \backslash & \\ \Delta & & & & \Delta' \\ \Gamma & \backslash & & / & \Gamma' \\ & & \tilde{\Gamma} & & \end{array}$$

$\mathfrak{p} \in \mathrm{Split}\, LL'/K \iff \tilde{\Gamma}_{\tilde{\mathfrak{P}}} = 1.$

$\iff \Gamma_\mathfrak{P} = \Gamma'_{\mathfrak{P}'} = 1$

$\iff \mathfrak{p} \in \mathrm{Split}_{L/K} \cap \mathrm{Split}_{L'/K}$.

qed.

Proposition 7.5.6: The following are equivalent:

(a) $L \subset L'$.

(b) $\mathrm{Split}_{L'/K} \subset \mathrm{Split}_{L/K}$.

(c) $\mu(\mathrm{Split}_{L'/K} \setminus \mathrm{Split}_{L/K}) < \frac{1}{2[L'/K]}$.

Proof: (a) $\Rightarrow$ (b) $L \subset L' \Rightarrow LL' = L' \overset{7.5.5}{\Rightarrow} \mathrm{Split}_{L'/K} = \mathrm{Split}_{L/K} \cap \mathrm{Split}_{L'/K}$.

(b) $\Rightarrow$ (c) ✓

(c) $\Rightarrow$ (a) If $L \not\subset L' \Rightarrow [LL'/L'] \geq 2 \Rightarrow \mu(\mathrm{Split}_{L'/K} \setminus \mathrm{Split}_{L/K}) =$

$$= \mu(\mathrm{Split}_{L'/K} \setminus \mathrm{Split}_{LL'/K})$$

$$= \mu(\mathrm{Split}_{L'/K}) - \mu(\mathrm{Split}_{LL'/K}) = \frac{1}{[L'/K]} - \frac{1}{[LL'/K]}$$

$$\geq \frac{1}{2[L'/K]}.$$

qed

Proposition 7.5.7: The following are equivalent:

(a) $L = L'$.

(b) $\mathrm{Split}_{L'/K}$ and $\mathrm{Split}_{L/K}$ differ only by a set of Dirichlet density 0.

Proof: Apply 7.5.6 twice.

In particular, a number field K that is galois over $\mathbb{Q}$ is uniquely determined by the set of rational primes p that split totally in K.

7.6 Dirichlet L-series

Definition 7.6.1: (a) A homomorphism $\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ is called a *Dirichlet character of modulus* $N \geqslant 1$.

(b) The *conductor* of such χ is the smallest divisor $N'|N$ such that χ factors through a homomorphism $(\mathbb{Z}/N'\mathbb{Z})^\times \to \mathbb{C}^\times$.

$N'|N \Rightarrow (\mathbb{Z}/N\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/N'\mathbb{Z})^\times$

(c) Such χ is called *primitive* if $N' = N$.

(d) Such χ is called *principal* if $N' = 1$, that is, if χ is the trivial homomorphism.

Convention 7.6.2: Often one identifies a Dirichlet character χ of modulus N with a function $\chi\colon \mathbb{Z} \to \mathbb{C}$ by setting

$$\chi(a) := \begin{cases} \chi(a \bmod (N)) & \text{if } \gcd(a, N) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Caution 7.6.3: When the conductor N' is smaller than the modulus N, one has to be somewhat careful with the divisors of N/N'.

Example: For any prime p the Legendre symbol defines a Dirichlet character $a \mapsto \left(\frac{a}{p}\right)$ of modulus p.

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } p \nmid a \text{ and } a \text{ square mod } p \\ -1 & \text{else} \end{cases}$$

Definition 7.6.4: The *Dirichlet L-function* associated to any Dirichlet character χ is

$$\boxed{L(\chi, s) := \sum_{n\geqslant 1} \chi(n) n^{-s}.}$$

Proposition 7.6.5: This series converges absolutely and locally uniformly for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$ and defines a holomorphic function there.

Proof: $\forall n: |\chi(n)| \leq 1. \Rightarrow$ dominated by $\zeta(\mathrm{Re}\, s) = \sum_{n\geq 1} n^{-\mathrm{Re}(s)}$. qed.

Proposition 7.6.6: For all $\mathrm{Re}(s) > 1$ we have the *Euler product*

$$\boxed{L(\chi, s) = \prod_{p\nmid N} (1 - \chi(p)p^{-s})^{-1}.}$$

Proof: $\forall m:$

$$\prod_{\substack{p\nmid N \\ p\leq m}} (1-\chi(p)p^{-s})^{-1} = \prod_{\substack{p\nmid N \\ p\leq m}} \sum_{\nu\geq 0} \underbrace{\chi(p)^{\nu}}_{\chi(p^{\nu})} \cdot p^{-\nu s} = \sum_{\substack{\nu_p \geq 0 \\ \text{for all } p\nmid N \\ p\leq m}} \chi\Big(\prod_p p^{\nu_p}\Big) \cdot \Big(\prod_p p^{\nu_p}\Big)^{-s}$$

$$= \sum_{\substack{n\geq 1 \\ (n,N)=1 \\ \text{all prime factors} \leq m}} \chi(n) \cdot n^{-s}.$$

let $m \to \infty$.

qed.

$$(\mathbb{Z}/N\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/N'\mathbb{Z})^\times \xrightarrow{\chi'} \mathbb{C}^\times$$

χ

Proposition 7.6.7: If a Dirichlet character χ of modulus N corresponds to a primitive Dirichlet character χ' of modulus N', then

$$L(\chi', s) \;=\; L(\chi, s) \cdot \prod_{p|N,\, p\nmid N'} (1 - \cancel{p^{-s}})^{-1}. \quad \chi'(p)\cdot p^{-s})^{-1}$$

Proof: For $p|N$, $p\nmid N'$: $\left.\begin{array}{l}\chi(p)=0\\ \chi'(p)\neq 0\end{array}\right] \Rightarrow$ Euler Factor $\left[\begin{array}{l}\text{of } L(\chi,s) \text{ is: } 1\\ \text{of } L(\chi',s) \text{ is: } (1-\chi'(p)p^{-s})^{-1}.\end{array}\right.$ qed.

Proposition 7.6.8: (a) For the principal Dirichlet character χ of modulus 1 we have $L(\chi, s) = \zeta(s)$. ✓

(b) For every non-principal Dirichlet character χ the function $L(\chi, s)$ extends uniquely to a holomorphic function on the region $\mathrm{Re}(s) > 0$.

Proof (b) $L(\chi,s) = \sum_{n\geq 1} \chi(n)\, n^{-s} = \sum_{n\geq 1} \chi(n) \cdot \int_n^\infty s\cdot x^{-s-1}\, dx$

$= \int_1^\infty \Big(\sum_{1\leq n\leq x} \chi(n)\Big) \cdot s\cdot x^{-s-1}\, dx.$

If $\chi \neq 1$ then $\forall k$: $\sum_{k<n\leq k+N} \chi(n) = \sum_{k=1}^{N} \chi(k) = \sum_{a\in(\mathbb{Z}/N\mathbb{Z})^\times} \chi(a) = 0$

$\Rightarrow \forall x: \Big|\sum_{1\leq n\leq x} \chi(n)\Big| \leq N.$

dominated by $\int_1^\infty N s\, x^{-s-1}\, dx$ convergent for $\mathrm{Re}(s) > 0$.

q.e.d.

Lemma: Γ finite group, $\chi: \Gamma \to \mathbb{C}^\times$ non-trivial homom. $\Rightarrow$

$\sum_{\gamma\in\Gamma} \chi(\gamma) = 0.$

Proof: $\exists \delta\in\Gamma: \chi(\delta)\neq 1$

$\underbrace{\sum_{\gamma\in\Gamma} \chi(\gamma)} = \sum_{\gamma\in\Gamma} \chi(\gamma\delta)$

$= \underbrace{\Big(\sum_{\gamma\in\Gamma} \chi(\gamma)\Big)}_{\shortparallel} \cdot \underline{\chi(\delta)}$

$\Rightarrow \ldots = 0.$ qed