Part III - Algebraic Number Theory

Lectured by Hanneke Wiersema

Artur Avameri

Contents

0 Introduction

19 Jan 2024, Lecture 1

The lecturer will provide typed notes at the end of the course. The topics of the course are

- global class field theory;
  - both ideal–theoretic and idele–theoretic.
- zeta functions;
- L–series;
- density theorems.

0.1 Rough goals of class field theory.

(1) Given a number field K, what are its abelian extensions? If $K = \mathbb{Q}$, we have the Kronecker–Weber theorem (which we will prove): Every finite abelian extension of $\mathbb{Q}$ is contained in some cyclotomic field, i.e. by adjoining a complex root of unity to $\mathbb{Q}$. We write $\mathbb{Q}(\zeta_n)$ for $\zeta_n = e^{2\pi i/n}$.

Finite abelian extensions of $\mathbb{Q}$ can be generated by special values of the exponential function $e^{2\pi iz}$. It is an open problem to explicitly construct all abelian extensions for arbitrary number fields. Kronecker solved the case of imaginary quadratic fields using special values of analytic functions (elliptic and modular functions).

In class field theory, we classify extensions introducing the notion of a **class field**: for any K we will show that any finite abelian extension will be contained in a class field. Moreover, the Galois group of this extension will be isomorphic to the generalized ideal class group (in the ideal case) or a subgroup of the Idele class group (in the idele case).

(2) Given a finite abelian extension, how do the prime ideals in the smaller field behave in the extension? In the quadratic case, we will prove quadratic reciprocity. There exist higher reciprocity laws. The most general answer we will see is the decomposition law, which is a consequence of the Artin reciprocity theorem.

Warning. There is no one convention for the notation for many objects – different textbooks may use different notation.

0.2 Review of basic Algebraic Number Theory

Let K be a number field and write $\mathcal{O}_K$ for its ring of integers. This is a Dedekind domain, so any ideal has a unique factorization into a product of prime ideals. Let L/K be an extension of number fields and and $\mathfrak{p}$ a prime ideal of K. Then $\mathfrak{p}\mathcal{O}_L$ is an ideal of L and by unique factorization $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_g^{e_g}$ with $\mathcal{P}_i$ distinct prime ideals in $\mathcal{O}_L$. Write $\mathcal{P}_i \mid \mathfrak{p}$ to mean that $\mathcal{P}_i$ appears in the factorization of $\mathcal{O}_L$. The number e_i is called the ramification index $\mathcal{P}_1/\mathfrak{p}$. We also write $e_i = e_{\mathcal{P}_i/\mathfrak{p}}$.

- If $e_i = 1$ for all i, we say $\mathfrak{p}$ is unramified in L.
- If $e_i > 1$ for some i, we say $\mathfrak{p}$ is ramified.
- If there is a unique prime $\mathcal{P}$ dividing $\mathfrak{p}$ with $e_{\mathcal{P}/\mathfrak{p}} = [L : K]$, we say $\mathfrak{p}$ is totally ramified.
- If $\mathfrak{p}\mathcal{O}_L$ is prime, we say $\mathfrak{p}$ is inert (or remains inert) in L.
- If $g = [L : K]$, we say $\mathfrak{p}$ splits completely.

The quotient $\mathcal{O}_K/\mathfrak{p}$ is a finite field of characteristic p ($\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$), called a residue field. If $\mathcal{P} \mid \mathfrak{p}$ (for $\mathcal{P} \in \mathcal{O}_L, \mathfrak{p} \in \mathcal{O}_K$), view $\mathcal{O}_K/\mathfrak{p}$ as a subfield of $\mathcal{O}_L/\mathcal{P}$. We call $f_{\mathcal{P}/\mathfrak{p}} = [\mathcal{O}_L/\mathcal{P} : \mathcal{O}_K/\mathfrak{p}]$ the residue field degree. If as before $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_g^{e_g}$, then $\sum_{i=1}^{g} e_{\mathcal{P}_i/\mathfrak{p}} f_{\mathcal{P}_i/\mathfrak{p}} = [L : K]$. If L/K is Galois, then the Galois group permutes the $\mathcal{P}_i$ transitively, so $e_1 = \dots = e_g = e$. Also if L/K is Galois, $f_{\mathcal{P}_1/\mathfrak{p}} = \dots f_{\mathcal{P}_g/\mathfrak{p}} = f$, so $efg = [L : K]$. Recall also that

- We can find the factorization of $\mathfrak{p}\mathcal{O}_L$ using the Kummer–Dedekind theorem.
- A prime $\mathfrak{p}$ in $\mathcal{O}_K$ ramifies in L/K if and only if $\mathfrak{p} \mid d_{L/K}$ for $d_{L/K}$ the discriminant.

If L/K is Galois, write $\mathrm{Gal}(L/K)$ for the Galois group. Let $\mathcal{P}$ be a prime ideal in $\mathcal{O}_L$.

Definition 0.1. The **decomposition subgroup** of $\mathcal{P}$ is

$$D_{\mathcal{P}} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathcal{P}) = \mathcal{P}\}.$$

The **inertial subgroup** of $\mathcal{P}$ is

$$I_{\mathcal{P}} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\alpha) \equiv \alpha \pmod{\mathcal{P}}\ \forall \alpha \in \mathcal{O}_L\}.$$

Remark. We have $I_{\mathcal{P}} \subset D_{\mathcal{P}}$. Easy exercise: show this.

Let $\sigma \in D_{\mathcal{P}}$. This induces an automorphism $\overline{\sigma} : \mathcal{O}_L/\mathcal{P} \to \mathcal{O}_L/\mathcal{P}$ such that $\overline{\sigma}|_{\mathcal{O}_K/\mathfrak{p}} = \mathrm{Id}|_{\mathcal{O}_K/\mathfrak{p}}$ for $\mathfrak{p} = \mathcal{P} \cap \mathcal{O}_K$. This gives a map $D_{\mathcal{P}} \to \mathrm{Gal}((\mathcal{O}_L/\mathcal{P})/(\mathcal{O}_K/\mathfrak{p}))$ by $\sigma \mapsto \overline{\sigma}$.

Proposition 0.2. (i) The Galois group $\mathrm{Gal}((\mathcal{O}_L/\mathcal{P})/(\mathcal{O}_K/\mathfrak{p}))$ is a cyclic group with canonical generator the Frobenius automorphism $x \mapsto x^q$ for $q = |\mathcal{O}_K/\mathfrak{p}|$.

(ii) The map $D_{\mathcal{P}} \overset{\sigma \mapsto \overline{\sigma}}{\to} \mathrm{Gal}((\mathcal{O}_L/\mathcal{P})/(\mathcal{O}_K/\mathfrak{p}))$ defines a surjective homomorphism with kernel $I_{\mathcal{P}}$.

(iii) $|I_{\mathcal{P}}| = e_{\mathcal{P}/\mathfrak{p}}$ and $|D_{\mathcal{P}}| = e_{\mathcal{P}/\mathfrak{p}} f_{\mathcal{P}/\mathfrak{p}}$.

Recall that if $\mathfrak{p}$ is a prime in $\mathcal{O}_K$ and $\mathcal{P}$ is a prime in $\mathcal{O}_L$ such that $\mathcal{P} \mid \mathfrak{p}$, then the norm of $\mathcal{P}$ is $N_{L/K}(\mathcal{P}) = \mathfrak{p}^{f_{\mathcal{P}/\mathfrak{p}}}$. Note that if $\mathfrak{p}$ is a prime of K, we also write $N(\mathfrak{p})$ for $N_{K/\mathbb{Q}}(\mathfrak{p})$ and $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$.

1 The Artin symbol

Lemma 1.1. Let L/K be a Galois extension and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$, unramified in L. Suppose $\mathcal{P} \subset \mathcal{O}_L$ such that $\mathcal{P} \mid \mathfrak{p}$. Then there exists a unique element $\sigma \in \mathrm{Gal}(L/K)$ such that for all $\alpha \in \mathcal{O}_L$,

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathcal{P}}.$$

Proof. Let $\sigma \in D_{\mathcal{P}}$ and $\overline{\sigma} \in \mathrm{Gal}((\mathcal{O}_L/\mathcal{P})/(\mathcal{O}_K/\mathfrak{p}))$ its image under the map from Proposition 0.2. By assumption, $\mathfrak{p}$ is unramified, so $|I_{\mathcal{P}}| = 1$, hence by Proposition 0.2 again, we have $D_{\mathcal{P}} \overset{(\star)}{\cong} \mathrm{Gal}((\mathcal{O}_L/\mathcal{P})/(\mathcal{O}_K/\mathfrak{p}))$. Recall that $\mathrm{Gal}((\mathcal{O}_L/\mathcal{P})/(\mathcal{O}_K/\mathfrak{p}))$ is generated by $x \mapsto x^q$ for $q = |\mathcal{O}_K/\mathfrak{p}|$. Let $\sigma \in D_{\mathcal{P}}$ be the unique element in $D_{\mathcal{P}}$ which maps to the Frobenius under $(\star)$. Then $\sigma(\alpha) \equiv \alpha^q \pmod{\mathcal{P}}$ for all $\alpha \in \mathcal{O}_L$ and $q = |\mathcal{O}_K/\mathfrak{p}| = N(\mathfrak{p})$. Uniqueness follows since any $\sigma \in \mathrm{Gal}(L/K)$ satisfying this condition will be an element of $D_{\mathcal{P}}$. □

22 Jan 2024, Lecture 2

Definition 1.2. This unique element is called the **Artin symbol** and we denote it by $\left(\frac{L/K}{\mathcal{P}}\right)$.

Definition 1.3. Let p be an odd prime and let a be any integer. Recall that the **Legendre symbol** is $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if} a \text{ is a QR mod } p. \\ -1 & \text{if } a \text{ is not a QR mod } p. \text{ Now let } n \in \mathbb{Z} \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases}$ be nonzero and write $= u p_1^{k_1} \dots p_u^{r_u}$ for $u = \pm 1$. Again let a be an integer, then the **Kronecker symbol** is

$$\left(\frac{a}{n}\right) = \left(\frac{a}{u}\right) \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{r_i}$$

with $\left(\frac{a}{p_i}\right)$ the Legendre symbol for odd primes, $\left(\frac{a}{2}\right) = \begin{cases} 0 & a \equiv 0 \pmod 2 \\ 1 & a \equiv \pm 1 \pmod 8 \\ -1 & a \equiv \pm 3 \pmod 8 \end{cases}$

and $\left(\frac{a}{1}\right) = 1$, $\left(\frac{a}{-1}\right) = \begin{cases} -1 & a < 0 \\ 1 & a \geq 0. \end{cases}$

The quadratic case. Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{N})$ for $N \neq 0, 1$ squarefree. Recall that

$$d_{L/\mathbb{Q}} = \begin{cases} N & N \equiv 1 \pmod 4 \\ 4N & N \not\equiv 1 \pmod 4 \end{cases}$$

with

$$\mathcal{O}_L = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{N}}{2}\right] & N \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{N}] & N \not\equiv 1 \pmod 4. \end{cases}$$

Then $\mathrm{Gal}(L/K)$ has order 2 with $1 : \sqrt{N} \to \sqrt{N}$ and $\sigma : \sqrt{N} \to -\sqrt{N}$ and we can identify $\mathrm{Gal}(L/K)$ with $\{\pm 1\}$.

Let $\mathfrak{p}$ be unramified in L and $\mathcal{P} \subset \mathcal{O}_L$ a prime lying above it (so $\mathcal{P} \mid \mathfrak{p}$). We then get $\sigma(\alpha) \equiv \alpha^{\mathfrak{p}} \pmod{\mathcal{P}}$ for all $\alpha \in \mathcal{O}_L$. We have

$$\left(\frac{L/K}{\mathfrak{p}}\right) = \left(\frac{\mathbb{Q}(\sqrt{N})/\mathbb{Q}}{\mathcal{P}}\right) = \left(\frac{d_{L/\mathbb{Q}}}{p}\right) = \pm 1$$

since $p \nmid d_{L/\mathbb{Q}}$ (more on this on Ex. Sheet 1).

Proposition 1.4. Suppose p is unramified in L. Then p splits in L if and only if $\left(\frac{d_{L/\mathbb{Q}}}{p}\right) = 1$.

The Artin symbol tells us about the decomposition, but more generally:

Lemma 1.5. Let L/K be any Galois extension. Let $\mathfrak{p} \subset \mathcal{O}_K$ be unramified with $\mathcal{P} \subset \mathcal{O}_L$ lying above it. Then:

(i) Let $\sigma \in \mathrm{Gal}(L/K)$. Then $\sigma \left(\frac{L/K}{\mathcal{P}}\right) \sigma^{-1} = \left(\frac{L/K}{\sigma(\mathcal{P})}\right)$.

(ii) The order of $\left(\frac{L/K}{\mathcal{P}}\right)$ is the residue field degree $f = f_{\mathcal{P}/\mathfrak{p}}$.

(iii) The prime $\mathfrak{p}$ splits completely in L if and only if $\left(\frac{L/K}{\mathcal{P}}\right) = 1$ (i.e. the Artin map is trivial).

Proof. Exercise! □

Definition 1.6. In this course, we say L/K is an abelian extension if it is a Galois extension of number fields with abelian Galois group $\mathrm{Gal}(L/K)$.

Suppose L/K is abelian and let $\mathfrak{p} \subset \mathcal{O}_K$ be unramified. Let $\mathcal{P}, \mathcal{P}' \subset \mathcal{O}_L$ be distinct prime ideals lying above $\mathfrak{p}$. Then $\mathcal{P}' = \sigma(\mathcal{P})$ for some $\sigma \in \mathrm{Gal}(L/K)$. Since the group is abelian, we find

$$\left(\frac{L/K}{\mathcal{P}'}\right) = \left(\frac{L/K}{\sigma(\mathcal{P})}\right) = \sigma \left(\frac{L/K}{\mathcal{P}}\right) \sigma^{-1} = \left(\frac{L/K}{\mathcal{P}}\right).$$

Notation. If L/K is abelian, we also write $\left(\frac{L/K}{\mathfrak{p}}\right)$ for the Artin symbol for any $\mathcal{P} \mid \mathfrak{p}$. So for L/K abelian, the Artin symbol defines a map

$$\begin{aligned} \{\text{unramified primes } \mathfrak{p} \subset \mathcal{O}_K \text{ in } L\} &\to \mathrm{Gal}(L/K) \\ \mathfrak{p} &\mapsto \left(\frac{L/K}{\mathfrak{p}}\right). \end{aligned}$$

We want to extend this map, for which we introduce fractional ideals. Quick review: recall that a **fractional ideal** of a number field K is a $\mathcal{O}_K$–submodule $\mathfrak{a}$ of K such that there exists $0 \neq x \in \mathcal{O}_K$ such that $x\mathfrak{a} \subset \mathcal{O}_K$. Equivalently, it is a set of the form αI for $\alpha \in K$ and some ideal I of $\mathcal{O}_K$.

A principal fractional ideal is a $\mathcal{O}_K$–submodule generated by a single nonzero element of K. Since $\mathcal{O}_K$ is a Dedekind domain, each fractional ideal is invertible and we obtain a group with identity $\mathcal{O}_K$.

Notation. Write I_K for the group of fractional ideals and P_K for the subgroup of principal fractional ideals. The quotient I_K/P_K is called the **ideal class group** $\mathrm{Cl}(K)$, which is a finite abelian group with order h_K called the **class number** of K.

Recall that for any $\mathfrak{a} \in I_K$, we have unique factorization

$$\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{p}_i^{r_i}, r_i \in \mathbb{Z}$$

with $\mathfrak{p}_i$ distinct prime ideals in $\mathcal{O}_K$.

Definition 1.7. Suppose L/K is an abelian unramified extension (i.e. every prime in K is unramified in L). Then we define the **Artin map** to be the homomorphism

$$\left(\frac{L/K}{\cdot}\right) : I_K \to \mathrm{Gal}(L/K)$$

by setting $\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{i=1}^{n} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i}$.

To define this more generally, we need to define **moduli**.

Interlude. Finite and infinite primes. Let K be a number field. Then a prime ideal is also called a finite prime to distinguish it from infinite primes.

Infinite primes are determined by the embeddings of K into $\mathbb{C}$. These correspond to archimedean absolute values (from local fields).

A real infinite prime is an embedding $\sigma : K \to \mathbb{R}$ and a complex infinite prime is a pair of conjugate embeddings $\sigma, \overline{\sigma} : K \to \mathbb{C}$ with $\sigma \neq \overline{\sigma}$.

Example 1.1.
- $\mathbb{Q}$ has one infinite real prime $\sigma\left(\frac{a}{b}\right) = \frac{a}{b}$.
- $\mathbb{Q}(\sqrt{2})$ has two infinite real primes $\sigma_1(\sqrt{2}) = \sqrt{2}$ and $\sigma_2(\sqrt{2}) = -\sqrt{2}$.
- $\mathbb{Q}(\sqrt{-2})$ has one infinite complex prime determined by $\sigma(\sqrt{-2}) = \sqrt{-2}$, $\overline{\sigma}(\sqrt{-2}) = -\sqrt{-2}$.

Remark. If we have an extension L/K, then an infinite prime σ of K **ramifies** in L is σ is real, but has an extension to L which is complex.

Example 1.2. The infinite prime of $\mathbb{Q}$ is unramified in $\mathbb{Q}(\sqrt{2})$, but it is ramified in $\mathbb{Q}(\sqrt{-2})$.

Definition 1.8. Let K be a number field. Then a **modulus** in K is a formal product

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$$

over all primes $\mathfrak{p}$, finite or infinite, of K, such that

(i) $n_{\mathfrak{p}} \geq 0$, and at most finitely many of these are nonzero.

(ii) $n_{\mathfrak{p}} = 0$ for $\mathfrak{p}$ infinite complex primes.

(iii) $n_{\mathfrak{p}} \leq 1$ for $\mathfrak{p}$ infinite real primes.

If $n_{\mathfrak{p}} = 0$ for all $\mathfrak{p}$, set $\mathfrak{m} = 1$.

Note that if K is a purely imaginary field (i.e. it has no real primes), then a modulus of K is just an ideal of $\mathcal{O}_K$. We can write any modulus $\mathfrak{m}$ as a product $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0$ is an ideal of $\mathcal{O}_K$ and $\mathfrak{m}_\infty$ is a product of distinct real infinite primes.

24 Jan 2024, Lecture 3

Recall we write $v_{\mathfrak{p}_i}(\mathfrak{a}) = r_i$. We now extend this map using moduli.

Definition 1.9. Let $\mathfrak{m}$ be a modulus. Define $I_K(\mathfrak{m})$ to be the group of fractional ideals coprime to $\mathfrak{m}$, where $\mathfrak{a} \in I_K$ is coprime to $\mathfrak{m}$ if $v_{\mathfrak{p}}(\mathfrak{a}) = 0$ for all primes $\mathfrak{p} \mid \mathfrak{m}_0$.

Non–infinite primes play no role in this definition, i.e. $I_K(\mathfrak{m}) = I_K(\mathfrak{m}_0)$.

Example 1.3.
- Let $\mathfrak{m} = (1)$, then $I_K(\mathfrak{m}) = I_K$.
- Let $K = \mathbb{Q}$ and $\mathfrak{m} = (m)$ for m a positive integer. Then $I_{\mathbb{Q}}(\mathfrak{m}) = \{\left(\frac{a}{b}\right)\mathbb{Z} \mid (a, m) = (b, m) = 1\}$.

Now let L/K be abelian, not necessarily unramified.

Definition 1.10. Let $\mathfrak{m}$ be a modulus of K divisible by all prime ideals that ramify in L. The Artin map for L/K and $\mathfrak{m}$ is a homomorphism

$$\Phi_{\mathfrak{m}} = \Phi_{L/K,\mathfrak{m}} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$$

given by $\mathfrak{a} \mapsto \left(\frac{L/K}{\mathfrak{a}}\right)$.

Example 1.4. Let $\mathfrak{m}$ be a positive integer and ζ_m a primitive m^{th} root of unity. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_m)$. Recall that $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ given by $\{\sigma : \zeta_m \mapsto \zeta_m^a\} \mapsto [a]$. Also, if a prime p ramifies in $\mathbb{Q}(\zeta_m)$, then $p \mid m$.

Hence let $\mathfrak{m} = (m)$, which contains all ramified prime ideals. We have a well–defined map $\Phi_{\mathfrak{m}} : I_{\mathbb{Q}}(\mathfrak{m}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$.

Let $\left(\frac{a}{b}\right)\mathbb{Z} \in I_{\mathbb{Q}}(\mathfrak{m})$ with $\frac{a}{b} > 0$, then

$$\Phi_{\mathfrak{m}}\left(\left(\frac{a}{b}\right)\mathbb{Z}\right) = [a][b]^{-1} \in (\mathbb{Z}/m\mathbb{Z})^\times.$$

Exercises: verify this above claim, show that (here?) the Artin map is surjective and work out its kernel.

Definition 1.11. Let $P_K(\mathfrak{m})$ be the subgroup of $I_K(\mathfrak{m})$ generated by

$$\{(\alpha) \mid \alpha \in \mathcal{O}_K, \alpha \equiv 1 \pmod{\mathfrak{m}_0}, \sigma(\alpha) > 0 \text{ for all real primes } \sigma \mid \mathfrak{m}_\infty\}.$$

Note $\alpha \equiv 1 \pmod{\mathfrak{m}_0}$ can also be written as $v_{\mathfrak{p}}(\alpha - 1) \geq v_{\mathfrak{p}}(\mathfrak{m}_0)$ (here $v_{\mathfrak{p}}(\alpha) = v_{\mathfrak{p}}(\alpha\mathcal{O}_K)$). This is called the **ray** or **ray group** for $\mathfrak{m}$.

Remark. Definitions in the literature might differ a bit, but we use the one above.

Example 1.5. Let $K = \mathbb{Q}, L = \mathbb{Q}(\zeta_m)$. Suppose $\mathfrak{m} = (m)$, then $P_{\mathbb{Q}}(\mathfrak{m}) = \{\left(\frac{a}{b}\right)\mathbb{Z} \in I_{\mathbb{Q}}(\mathfrak{m}) \mid a \equiv b \pmod{m}\}$. Note $I_{\mathbb{Q}}(\mathfrak{m}) = I_{\mathbb{Q}}(\mathfrak{m}_0)$, which is not true for $P_{\mathbb{Q}}(\mathfrak{m})$!

Now suppose $\mathfrak{m} = (m)\infty$ – the infinite prime of $\mathbb{Q}$. Then

$$P_{\mathbb{Q}}(\mathfrak{m}) = \left\{\left(\frac{a}{b}\right)\mathbb{Z} \in I_{\mathbb{Q}}(\mathfrak{m}) \mid a \equiv b \pmod{m}, \frac{a}{b} > 0\right\}.$$

We have $I_{\mathbb{Q}}((m))/P_{\mathbb{Q}}((m)) \cong (\mathbb{Z}/m\mathbb{Z})^\times/\{\pm 1\}$ and $I_{\mathbb{Q}}((m)\infty)/P_{\mathbb{Q}}((m)\infty) \cong (\mathbb{Z}/m\mathbb{Z})^\times$.

In general, $P_K(\mathfrak{m})$ has finite index in $I_K(\mathfrak{m})$.

Definition 1.12. The quotient $I_K(\mathfrak{m})/P_K(\mathfrak{m})$ is called the **ray class group**.

Our goal is to show that this is a finite group. Recall by Ostrowski's theorem that every nontrivial absolute value is equivalent to either $|\cdot|_{\mathfrak{p}}$ for some prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ or $|\cdot|_\sigma$ for some embedding $\sigma : K \to \mathbb{C}$, where $|\cdot|_\sigma = |x|_{\mathbb{C}}$ with $|\cdot|_{\mathbb{C}}$ the complex absolute value; and $|x|_{\mathfrak{p}} = C^{v_{\mathfrak{p}}(x)}$ for $x \neq 0$ for some $0 < C < 1$ (often $C = \frac{1}{p}$) and 0 for 0. (Recall $v_{\mathfrak{p}}(x) = \alpha$ if $x\mathcal{O}_K = \mathfrak{p}^\alpha \mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_r^{\alpha_r}$.)

We quote a result proved in Local Fields:

Theorem 1.13 (Approximation theorem)**.** Let $|\cdot|_1, \dots, |\cdot|_n$ be nontrivial pairwise inequivalent absolute values on K. Let $\beta_1, \dots, \beta_n \in K$ be nonzero. Then for any $\epsilon > 0$, there exists $\alpha \in K$ such that $|\alpha - \beta_j|_j < \epsilon$ for each $j = 1, \dots, n$.

Consequences.

- Let $\mathfrak{p}$ be a real infinite prime corresponding to $\sigma : K \to \mathbb{R}$. If $\alpha\beta \neq 0$ and $|\alpha - \beta|_{\mathfrak{p}} < \epsilon$, then $\sigma\left(\frac{\alpha}{\beta}\right) > 0$.
- Let $\mathfrak{p}$ be a finite prime. Then $|\alpha - \beta|_{\mathfrak{p}} < \epsilon$ is equivalent to $\left|\frac{\alpha}{\beta} - 1\right|_{\mathfrak{p}} < \frac{\epsilon}{|\beta|_{\mathfrak{p}}}$. Let $\epsilon' = \frac{\epsilon'}{|\beta|_{\mathfrak{p}}}$. If ϵ' is small, say $\epsilon' < C^n$ for some n, then $v_{\mathfrak{p}}\left(\frac{\alpha}{\beta} - 1\right) > n$ and so $\alpha \equiv \beta \pmod{\mathfrak{p}^n}$.

Remark/Exercise. Let I be an ideal of $\mathcal{O}_K$, then every class in $\mathrm{Cl}(K)$ has a representative which is coprime to I.

Definition 1.14. Let $P_{\mathfrak{m}} \subset I_K(\mathfrak{m})$ be the subgroup of principal fractional ideals which are coprime to $\mathfrak{m}$.

Proposition 1.15. Let $P_{\mathfrak{m}} \subset I_K(\mathfrak{m})$ be as above. Then we have two exact sequences

$$1 \to P_{\mathfrak{m}} \to I_K(\mathfrak{m}) \to \mathrm{Cl}(K) \to 1$$
$$1 \to P_{\mathfrak{m}}/P_K(\mathfrak{m}) \to I_K(\mathfrak{m})/P_K(\mathfrak{m}) \to \mathrm{Cl}(K) \to 1.$$

Proof. Let $\mathfrak{a} \in I_K(\mathfrak{m})$ and define $f : I_K(\mathfrak{m}) \to \mathrm{Cl}(K)$ by $\mathfrak{a} \mapsto [a]$. This is a group homomorphism, it is surjective by the previous remark with kernel $P_{\mathfrak{m}}$, so $1 \to P_{\mathfrak{m}} \to I_K(\mathfrak{m}) \to \mathrm{Cl}(K) \to 1$. The second sequence follows immediately because f is trivial on $P_K(\mathfrak{m})$. □

26 Jan 2024, Lecture 4

Definition 1.16. For $\mathfrak{m}$ a modulus, let

$$K_{\mathfrak{m}} = \{\alpha \in K^\times \mid (\alpha) \in I_K(\mathfrak{m})\}$$
$$K_{\mathfrak{m},1} = \{\alpha \in K^\times \mid \alpha \equiv 1 \pmod{\mathfrak{m}_0}, \sigma(\alpha) > 0 \ \forall \sigma \mid \mathfrak{m}_\infty\}.$$

Note $P_k(\mathfrak{m}) = \{(\alpha) \in I_K(\mathfrak{m}) \mid \alpha \in K_{\mathfrak{m},1}\}$.

Theorem 1.17. The ray class group $I_K(\mathfrak{m})/P_K(\mathfrak{m})$ is a finite group with size

$$h_K(\mathfrak{m}) = |I_K(\mathfrak{m})/P_K(\mathfrak{m})| = \frac{h_K \cdot \phi(\mathfrak{m})}{[\mathcal{O}_K^\times : (\mathcal{O}_K^\times \cap K_{\mathfrak{m},1})]},$$

where h_K is the class number of K and $\phi(\mathfrak{m}) = \phi(\mathfrak{m}_0)\phi(\mathfrak{m}_\infty)$ with $\phi(\mathfrak{m}_0) = |(\mathcal{O}_K/\mathfrak{m}_0)^\times| = N(\mathfrak{m}_0) \cdot \prod_{\mathfrak{p}|\mathfrak{m}_0}(1 - N(\mathfrak{p}^{-1}))$ and $\phi(\mathfrak{m}_\infty) = 2^{\#\mathfrak{m}_\infty}$ where $\#\mathfrak{m}_\infty$ is the number of infinite real primes dividing $\mathfrak{m}$.

Proof. **Step 1.** $P_{\mathfrak{m}}/P_K(\mathfrak{m}) \cong K_{\mathfrak{m}}/\mathcal{O}_K^\times K_{\mathfrak{m},1}$.

Proof of Step 1. Consider $K_{\mathfrak{m}} \to P_{\mathfrak{m}}/P_K(\mathfrak{m})$ by $\alpha \mapsto (\alpha)P_K(\mathfrak{m})$. This is a surjective homomorphism with kernel

$$\begin{aligned}
&\{\alpha \in K_{\mathfrak{m}} \mid (\alpha) \in P_K(\mathfrak{m})\} \\
=&\{\alpha \in K_{\mathfrak{m}} \mid \exists \beta \in K_{\mathfrak{m},1} \text{ s.t. } (\alpha) = (\beta)\} \\
=&\{\alpha \in K_{\mathfrak{m}} \mid \exists \beta \in K_{\mathfrak{m},1} \text{ s.t. } \beta = \alpha \cdot \epsilon \text{ for some } \epsilon \in \mathcal{O}_K^\times\}.
\end{aligned}$$

□

Step 2. $K_{\mathfrak{m}}/K_{\mathfrak{m},1} \cong \{\pm 1\}^{\#\mathfrak{m}_\infty} \times (\mathcal{O}_K/\mathfrak{m}_0)^\times$.

Proof of Step 2. We can write $\alpha \in K_{\mathfrak{m}}$ as $\alpha = \frac{a}{b}$ for $a, b \in \mathcal{O}_K$ coprime, and (a), (b) coprime to $\mathfrak{m}_0$. For such a, b, the images $\overline{a}, \overline{b} \in \mathcal{O}_K/\mathfrak{m}_0$ lie in $(\mathcal{O}_K/\mathfrak{m}_0)^\times$. Consider the map

$$\begin{aligned}
K_{\mathfrak{m}} &\to \left(\prod_{\sigma|\mathfrak{m}_\infty} \{\pm 1\}\right) \times (\mathcal{O}_K/\mathfrak{m}_0)^\times \\
\alpha &\mapsto \left(\prod_{\sigma|\mathfrak{m}_\infty} \operatorname{sgn}(\sigma(\alpha))\right) \times \overline{\alpha}
\end{aligned}$$

for $\overline{\alpha} = \overline{a}\overline{b}^{-1} \in (\mathcal{O}_K/\mathfrak{m}_0)^\times$. This map is surjective: this is on Ex. Sheet 1, use the Approximation Theorem. It has kernel

$$\{\alpha \in K_{\mathfrak{m}} \mid \sigma(\alpha) > 0 \ \forall \sigma \mid \mathfrak{m}_\infty,\ \alpha \equiv 1 \pmod{\mathfrak{m}_0}\} = K_{\mathfrak{m},1}.$$

□

Step 3. $\mathcal{O}_K^\times K_{\mathfrak{m},1}/K_{\mathfrak{m},1} \cong \mathcal{O}_K^\times/(\mathcal{O}_K^\times \cap K_{\mathfrak{m},1})$.

Proof of Step 3. This is just the second isomorphism theorem. □

Putting it all together:

$$[I_K(\mathfrak{m}) : P_K(\mathfrak{m})] = [I_K(\mathfrak{m}) : P_\mathfrak{m}][P_\mathfrak{m} : P_K(\mathfrak{m})]$$

and

$$\begin{aligned}(P_\mathfrak{m}/P_K(\mathfrak{m})) &\overset{\text{(i)}}{\cong} K_\mathfrak{m}/\mathcal{O}_K^\times K_{\mathfrak{m},1} \\ &\cong (K_\mathfrak{m}/K_{\mathfrak{m},1})/(\mathcal{O}_K^\times K_{\mathfrak{m},1}/K_{\mathfrak{m},1}) \\ &\overset{\text{(iii)}}{\cong} (K_\mathfrak{m}/K_{\mathfrak{m},1})/(\mathcal{O}_K^\times/(\mathcal{O}_K^\times \cap K_{\mathfrak{m},1}))\end{aligned}$$

and

$$I_K(\mathfrak{m})/P_\mathfrak{m} \cong \mathrm{Cl}(K)$$

by Proposition 1.15.

This gives

$$\begin{aligned}[I_K(\mathfrak{m}) : P_K(\mathfrak{m})] &= [I_K(\mathfrak{m}) : P_\mathfrak{m}][P_\mathfrak{m} : P_K(\mathfrak{m})] \\ =|\mathrm{Cl}(K)|\frac{[K_\mathfrak{m} : K_{\mathfrak{m},1}]}{[\mathcal{O}_K : (\mathcal{O}_K^\times \cap K_{\mathfrak{m},1})]} &\overset{\text{(ii)}}{=} \frac{h_K \cdot \phi(\mathfrak{m})}{[\mathcal{O}_K : (\mathcal{O}_K^\times \cap K_{\mathfrak{m},1})]}.\end{aligned}$$

□

Next we have more general class groups, i.e. $I_K(\mathfrak{m})/H$ with $P_K(\mathfrak{m}) \subset H$.

Definition 1.18. A subgroup $H \subset I_K(\mathfrak{m})$ is a **congruence subgroup** for $\mathfrak{m}$ if it satisfies $P_k(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m})$.

Motivation: For "suitably chosen" moduli $\mathfrak{m}$, the congruence subgroup will be the kernel of the Artin map $\Phi_\mathfrak{m}$.

Definition 1.19. Let H be a congruence subgroup for $\mathfrak{m}$, then the quotient $I_K(\mathfrak{m})/H$ is called a **generalized ideal class group** for $\mathfrak{m}$.

Remark. Recall that for $K = \mathbb{Q}$ and $\mathfrak{m} = (m)\infty$ for m a positive integer, we saw $I_K(\mathfrak{m})/P_K(\mathfrak{m}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ and

$$(\mathbb{Z}/m\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong I_K(\mathfrak{m})/P_K(\mathfrak{m})$$

via the Artin map, so $\ker(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},\mathfrak{m}}) = P_K(\mathfrak{m})$.

The idea of class field theory is that generalized ideal class groups are Galois groups of abelian extensions and that the link between them is given by the Artin map. We will prove that the Artin map is surjective. Determining the kernel is a lot more difficult (not done in this course).

What is the meaning of "suitably chosen" above? For L/K abelian, we want to know for which moduli $\mathfrak{m}$ will $\ker(\Phi_{\mathfrak{m}})$ be a congruence subgroup.

Lemma 1.20. Let L/K be abelian and let $\mathfrak{m}$ be a modulus divisible by all ramified primes. If $\mathfrak{n}$ is another modulus such that $\mathfrak{m} \mid \mathfrak{n}$, then

$$P_K(\mathfrak{m}) \subset \ker(\Phi_{\mathfrak{m}}) \implies P_K(\mathfrak{n}) \subset \ker(\Phi_{\mathfrak{n}}).$$

Proof. Note first that if $\mathfrak{m} \mid \mathfrak{n}$, then $I_K(\mathfrak{n}) \subset I_K(\mathfrak{m})$, so $\Phi_{\mathfrak{n}} : I_K(\mathfrak{n}) \to \mathrm{Gal}(L/K)$ is well–defined and $\Phi_{\mathfrak{n}} = \Phi_{\mathfrak{m}}|_{I_K(\mathfrak{n})}$, so $\ker(\Phi_{\mathfrak{n}}) = \ker(\Phi_{\mathfrak{m}}) \cap I_K(\mathfrak{n})$. If $\mathfrak{m} \mid \mathfrak{n}$, then $P_K(\mathfrak{n}) \subset P_K(\mathfrak{m})$. Now $P_K(\mathfrak{n}) \subset P_K(\mathfrak{m}) \subset \ker(\Phi_{\mathfrak{m}})$, so

$$(\alpha) \in P_K(\mathfrak{n}) \subset P_K(\mathfrak{m}) \cap I_K(\mathfrak{n}) \subset \ker(\Phi_{\mathfrak{m}}) \cap I_K(\mathfrak{n}) = \ker(\Phi_{\mathfrak{n}}). \qquad \square$$

In the above situation, if $\ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$, then $\ker(\Phi_{\mathfrak{n}})$ is a congruence subgroup for $\mathfrak{n}$.

Now we find a special modulus that works for each extension, called **the conductor**.

29 Jan 2024, Lecture 5

Statements of global class field theory (ideal theoretic). For L/K abelian, we are interested to find out for which $\mathfrak{m} \subset \mathcal{O}_K$ is $\ker(\Phi_{L/K,\mathfrak{m}})$ a congruence subgroup (i.e. $P_K(\mathfrak{m}) \subset \ker(\Phi_{L/K,\mathfrak{m}})$).

Theorem 1.21 (The Conductor Theorem)**.** Let L/K be abelian. Then there is a modulus $\mathfrak{f} = \mathfrak{f}(L/K)$ such that

- a prime of K, finite or infinite, ramifies in L if and only if it divides $\mathfrak{f}_{L/K}$.
- If $\mathfrak{m}$ is divisible by all primes that ramify, then $\ker(\Phi_{L/K,\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$ if and only if $\mathfrak{f}_{L/K} \mid \mathfrak{m}$.

Definition 1.22. The modulus $\mathfrak{f}_{L/K}$ is uniquely determined by L/K and called the **conductor**.

Example 1.6. Let $K = \mathbb{Q}$ and let $L = \mathbb{Q}(\sqrt{N})$ for $N \neq 0, 1$ squarefree. Then $\mathfrak{f}_{L/K} = \begin{cases} \left|d_{L/K}\right| & N > 0 \\ \left|d_{L/K}\right| \infty & N < 0. \end{cases}$ ($\left|D_{L/K}\right| \infty$ is the real infinite place of $\mathbb{Q}$).

Remark. The conductor is not just the product of ramified primes. In Ex. Sheet 1, there will be a cubic extension $L/\mathbb{Q}$ which is ramified only at 3. However, for $\mathfrak{m} = (3)$ or $\mathfrak{m} = (3)\infty$, $\ker(\Phi_{L/\mathbb{Q},\mathfrak{m}})$ is not a congruence subgroup, so $\mathfrak{f}_{L/Q} \nmid (3)$ and $\mathfrak{f}_{L/\mathbb{Q}} \nmid (3)\infty$.

Next we focus on the kernel. Recall that if $\mathcal{P} \subset \mathcal{O}_L$ is a prime ideal, then we have $N_{L/K}(\mathcal{P}) = \mathfrak{p}^{f_{\mathcal{P}/\mathfrak{p}}}$ if $\mathfrak{p} = \mathcal{P} \cap \mathcal{O}_K$.

Notation. Let $N_{L/K} : I_K \to I_K$ be the norm map, given by $\mathfrak{a} \mapsto N_{L/K}(\mathfrak{a})$. If $\mathfrak{a} = \prod_{i=1}^n \mathcal{P}_i^{r_i}$, then $N_{L/K}(\mathfrak{a}) = \prod_{i=1}^n (N(\mathcal{P}_i)^{r_i}) = \prod_{i=1}^n (\mathfrak{p}_i^{f_{\mathcal{P}_i/\mathfrak{p}_i}})^{r_i}$.

Definition 1.23. Let L/K be abelian and let $\mathfrak{m}$ be a modulus of K divisible by $\mathfrak{f}(L/K)$. Then the **norm group** (also called a Takagi group) is the congruence subgroup

$$T_{L/K}(\mathfrak{m}) = P_K(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m})),$$

where $I_L(\mathfrak{m})$ is the subgroup of I_L with elements fractional ideals that are coprime to $\mathfrak{m}\mathcal{O}_L$.

Theorem 1.24 (Artin Reciprocity Theorem)**.** Let L/K be abelian and let $\mathfrak{m}$ be a modulus of K divisible by all ramified primes (both finite and infinite). Then the Artin map $\Phi_{L/K,\mathfrak{m}}(I_K(\mathfrak{m})) \to \mathrm{Gal}(L/K)$ is surjective.

If also $\mathfrak{f}_{L/K} \mid \mathfrak{m}$, so that $\ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup, then $\ker(\Phi_{L/K,\mathfrak{m}}) = T_{L/K}(\mathfrak{m})$ and the Artin map defines an isomorphism

$$I_K(\mathfrak{m})/T_{L/K}(\mathfrak{m}) \cong \mathrm{Gal}(L/K).$$

So $\mathrm{Gal}(L/K)$ is the generalized ideal class group for $\mathfrak{m}$.

Artin reciprocity gives us information about the decomposition of primes:

Theorem 1.25 (Decomposition law)**.** Let L/K be abelian of degree n and let $\mathfrak{p} \subset \mathcal{O}_K$ be an unramified prime ideal. Let $\mathfrak{m}$ be divisible by $\mathfrak{f}(L/K)$, but not by $\mathfrak{p}$. Let $H = \ker(\Phi_{\mathfrak{m}})$ be the congruence subgroup for $\mathfrak{m}$. Let f be the smallest positive integer such that $\mathfrak{p}^f \in H$, i.e. f is the order of $\mathfrak{p}$ mod H in $I_K(\mathfrak{m})/H$. Then $\mathfrak{p}$ decomposes in L into a product

$$\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1 \dots \mathcal{P}_g$$

for $g = \frac{n}{f}$ of distinct prime ideals of degree f over $\mathfrak{p}$.

Proof. Let $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1 \dots \mathcal{P}_g$ be the prime decomposition in L. These have to be distinct as $\mathfrak{p}$ is unramified, and all $\mathcal{P}_i$ have the same residue field degree $f_{\mathcal{P}_i/\mathfrak{p}}$ (as the extension is abelian, in particular Galois). We know that $f_{\mathcal{P}_i/\mathfrak{p}}$ is the order of $\left(\frac{L/K}{\mathfrak{p}}\right)$ and so under the isomorphism $I_K(\mathfrak{m})/H \cong \mathrm{Gal}(L/K)$, this means it is also the order of $\mathfrak{p}$ mod H in $I_K(\mathfrak{m})/H$. The result follows since $[L : K] = n = efg = fg$. □

Next we want to show that every generalized ideal class group is the Galois group of some abelian extension and that this extension is unique.

Theorem 1.26 (The Existence Theorem)**.** Let $\mathfrak{m}$ be a modulus of f and let H be a congruence subgroup for $\mathfrak{m}$. Then there exists a unique abelian extension L/K with the following properties:

- All its ramified primes, finite or infinite, divide $\mathfrak{m}$.

- $H = T_{L/K}(\mathfrak{m})$.
- $I_K(\mathfrak{m})/H \cong \mathrm{Gal}(L/K)$ under the Artin map $\Phi_{L/K,\mathfrak{m}}$.

So for any number field K, we can find abelian extensions with specified ramification.

Definition 1.27. Let $\mathfrak{m}$ be any modulus and let $H = P_K(\mathfrak{m})$. The **ray class field** is the unique abelian extension $K(\mathfrak{m})$ of K such that $P_K(\mathfrak{m}) = \ker(\Phi_{K(\mathfrak{m})/K,\mathfrak{m}})$. This explains the name $\mathrm{Gal}(K(\mathfrak{m})/K) \cong I_K(\mathfrak{m})/P_K(\mathfrak{m})$.

Example 1.7. Let $K = \mathbb{Q}$ and let $\mathfrak{m} = (m)\infty$ for m odd or divisible by 4. Then $\mathbb{Q}(\mathfrak{m}) = \mathbb{Q}(\zeta_m)$. Taking $\mathfrak{m} = (m)$ instead gives $\mathbb{Q}(\mathfrak{m}) = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$.

Next we want to show that every abelian extension is contained in a ray class field. In other words, given $K, \mathfrak{m}$, there is a unique abelian extension $K(\mathfrak{m})/K$ such that $P_K(\mathfrak{m}) = \ker(\Phi_{K(\mathfrak{m})/K,\mathfrak{m}})$.

31 Jan 2024, Lecture 6

Proposition 1.28. Let $K \leq L \leq M$ be a tower of abelian extensions. Suppose $\mathfrak{m}$ contains all prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ that ramify in M. Write $\mathrm{res} : \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$ for the restriction map $\sigma \mapsto \sigma_L$. Then we have a commutative diagram

$$\begin{array}{ccc} I_K(\mathfrak{m}) & \xrightarrow{\Phi_{M/K,\mathfrak{m}}} & \mathrm{Gal}(M/K) \\ & \searrow^{\Phi_{L/K,\mathfrak{m}}} & \downarrow \mathrm{res} \\ & & \mathrm{Gal}(L/K) \end{array}.$$

Proof. Exercise on Example Sheet 1. □

Lemma 1.29. Let L/K and M/K be abelian extensions. Then $L \subset M$ if and only if there is a modulus $\mathfrak{m}$ divisible by all primes of K which ramify in either L or M such that $P_K(\mathfrak{m}) \subset \ker(\Phi_{M/K}, \mathfrak{m}) \subset \ker(\Phi_{L/K}, \mathfrak{m})$.

Proof. Suppose $L \subset M$. Then by Artin reciprocity, there exists $\mathfrak{m}_1$ for L/K and $\mathfrak{m}_2$ for M/K such that $P_K(\mathfrak{m}_1) \subset \ker(\Phi_{L/K}, \mathfrak{m}_1)$ and $P_K(\mathfrak{m}_2) \subset \ker(\Phi_{M/K,\mathfrak{m}_2})$. By Lemma 1.20, we can find $\mathfrak{m}$ such that $P_K(\mathfrak{m}) \subset \ker(\Phi_{L/K,\mathfrak{m}})$ and $P_K(\mathfrak{m}) \subset \ker(\Phi_{M/K,\mathfrak{m}})$. By Proposition 1.28, we have $\mathrm{res} \circ \Phi_{M/K,\mathfrak{m}} = \Phi_{L/K,\mathfrak{m}}$, so $P_K(\mathfrak{m}) \subset \ker(\Phi_{M/K}, \mathfrak{m}) \subset \ker(\Phi_{L/K,\mathfrak{m}})$.

Now suppose we have $\mathfrak{m}$ such that $P_K(\mathfrak{m}) \subset \ker(\Phi_{M/K}, \mathfrak{m}) \subset \ker(\Phi_{L/K,\mathfrak{m}})$. Then we get that under the map $\Phi_{M/K,\mathfrak{m}} : I_K(\mathfrak{m}) \to \mathrm{Gal}(M/K)$, the subgroup $\ker(\Phi_{L/K,\mathfrak{m}}) \subset I_K(\mathfrak{m})$ maps to a subgroup $H \subset \mathrm{Gal}(M/K)$. By Galois theory, H corresponds to an intermediate field $K \subset \tilde{L} \subset M$. Now apply the first part of the proof to $\tilde{L} \subset M$ to obtain $\ker(\Phi_{L/K,\mathfrak{m}}) = \ker(\Phi_{\tilde{L}/M,\mathfrak{m}})$. By uniqueness, in the Existence Theorem, $L = \tilde{L} \subset M$. □

Corollary 1.30. Let K be a number field. Then any abelian extension is contained in a ray class field.

Proof. Suppose L/K is abelian and let $\mathfrak{m}$ be a modulus of K such that $\mathfrak{f}_{L/K} \mid \mathfrak{m}$. Then $H = \ker(\Phi_{L/K,\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$. So $P_K(\mathfrak{m}) = \ker(\Phi_{K(\mathfrak{m})/K,\mathfrak{m}}) \subset H = \ker(\Phi_{L/K}, \mathfrak{m})$. By Lemma 1.29, $L \subset K(\mathfrak{m})$. □

Before stating the Classification Theorem, we define an equivalence relation on the set of congruence subgroups. Why?

- If $\ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$, then $\ker(\Phi_{\mathfrak{n}})$ is a congruence subgroup for $\mathfrak{n}$ for any modulus $\mathfrak{m} \mid \mathfrak{n}$.
- Say a prime $\mathfrak{p}$ is in the support of $\mathfrak{m}$ if $\mathfrak{p} \mid \mathfrak{m}$. If $\mathfrak{m}$ and $\mathfrak{n}$ have the same support, then $I_K(\mathfrak{m}) = I_K(\mathfrak{n})$, but $P_K(\mathfrak{m})$ may differ from $P_K(\mathfrak{n})$.

Definition 1.31. We say two congruence subgroups H_1 and H_2 are equivalent, written $H_1 \sim H_2$ if there is a modulus $\mathfrak{m}$ such that $I_K(\mathfrak{m}) \cap H_1 = I_K(\mathfrak{m}) \cap H_2$.

Let L/K be abelian. Let $\mathfrak{m}$ be such that $P_K(\mathfrak{m}) \subset \ker(\Phi_{L/K,\mathfrak{m}})$ and let $\mathfrak{m}'$ be such that $P_K(\mathfrak{m}') \subset \ker(\Phi_{L/K,\mathfrak{m}'})$. Then $\ker(\Phi_{L/K,\mathfrak{m}}) \sim \ker(\Phi_{L/K,\mathfrak{m}'})$ because

$$\ker(\Phi_{L/K,\mathfrak{m}}) \cap I_K(\mathfrak{m}\mathfrak{m}') = \ker(\Phi_{L/K}, \mathfrak{m}\mathfrak{m}') = \ker(\Phi_{L/K,\mathfrak{m}'}) \cap I_K(\mathfrak{m}\mathfrak{m}').$$

The collection of congruence subgroups H for $\mathfrak{m}$ with $\mathfrak{m}$ such that $P_K(\mathfrak{m}) \subset \ker(\Phi_{L/K,\mathfrak{m}})$ lie in a single equivalence class of congruence subgroups. We write $H(L/K)$ for this class.

Theorem 1.32 (The Classification Theorem)**.** Let K be a number field. Then there is a one–to–one inclusion–reversing correspondence

$$\{\text{abelian extensions } L/K\} \leftrightarrow \{\text{congruence subgroups}/\sim\}$$
$$L/K \mapsto H(L/K).$$

"Applications" of main theorems.

Theorem 1.33 (Kronecker–Weber theorem)**.** Let $L/\mathbb{Q}$ be abelian. Then there is a positive integer m such that $L \subset \mathbb{Q}(\zeta_m)$.

Proof. By Artin reciprocity, there is a modulus $\mathfrak{m}$ satisfying the inclusions $P_{\mathbb{Q}}(\mathfrak{m}) \subset \ker(\Phi_{L/\mathbb{Q}}, \mathfrak{m}) \subset I_{\mathbb{Q}}(\mathfrak{m})$. Any modulus of $\mathbb{Q}$ will be (m) or $(m)\infty$ for some m. By Lemma 1.20, we may assume $\mathfrak{m} = (m)\infty$. We have $P_{\mathbb{Q}}(\mathfrak{m}) = \ker(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},\mathfrak{m}})$, so $P_{\mathbb{Q}}(\mathfrak{m}) = \ker(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},\mathfrak{m}}) \subset \ker(\Phi_{L/\mathbb{Q},\mathfrak{m}})$. By Lemma 1.29, we have $L \subset \mathbb{Q}(\zeta_m)$. □

Remark. There exist proofs of Kronecker–Weber that don't use class field theory (see e.g. *Number Fields* by Marcus).

Hilbert Class Field: Given a number field K, by the Existence Theorem we can find an abelian extension and "control" the ramification. Now take $\mathfrak{m} = (1)$,

then the corresponding abelian extension $K(\mathfrak{m})/K$ will be unramified at all primes (finite and infinite). We have $\Phi_{\mathfrak{m}} : I_K = I_K(1) \to \mathrm{Gal}(K(1)/K)$ with kernel $P_K((1)) = P_K$, so we obtain $\mathrm{Cl}(K) = I_K/P_K \cong \mathrm{Gal}(K(1)/K)$. By the Existence Theorem, we obtain an unramified abelian extension with Galois group equal to the ideal class group.

Definition 1.34. The Hilbert class field F is the ray class field for the modulus $\mathfrak{m} = (1)$.

Example 1.8. Let $K = \mathbb{Q}$. This is its own Hilbert class group (as $\mathrm{Cl}(K) = 1$).

02 Feb 2024, Lecture 7

Theorem 1.35. The Hilbert class field F is the maximal unramified extension of K.

Proof. Let M be another unramified abelian extension. By the Conductor theorem, $\mathfrak{f}_{M/K} = (1)$. For $\mathfrak{m} = (1)$ we have

$$P_K(\mathfrak{f}_{M/K}) = \underbrace{P_K(\mathfrak{m})}_{=\ker(\Phi_{F/K,\mathfrak{m}})} \subset \ker(\Phi_{M/K,\mathfrak{f}_{M/K}}).$$

By Lemma 1.29, we have $M \subset F$. □

Corollary 1.36. Let K be a number field. There is a one–to–one correspondence between unramified abelian expressions M of K and subgroups of the ideal class group $\mathrm{Cl}(K)$. Furthermore, if M/K corresponds to $H \subset \mathrm{Cl}(K)$, then the Artin map induces an isomorphism

$$\mathrm{Cl}(K)/H \xrightarrow{\cong} \mathrm{Gal}(M/K).$$

Proof. Let F be the Hilbert class field at K. Then $\mathrm{Gal}(F/K) \cong \mathrm{Cl}(K)$. By Galois theory, there is a one-to-one inclusion-reversing correspondence between intermediate fields and subgroups of $\mathrm{Gal}(F/K) \cong \mathrm{Cl}(K)$. Since each unramified abelian extension is contained in F, the first part of the corollary follows.

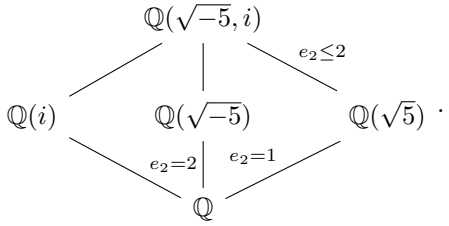
Let H be a subgroup of $\mathrm{Gal}(F/K)$ and let

$$M = F^H = \{x \in F \mid \sigma(x) = x \ \forall \sigma \in H\}.$$

By Proposition 1.28, $\Phi_{M/K,\mathfrak{m}} : \mathrm{Cl}(K) \to \mathrm{Gal}(M/K)$ with $\Phi_{M/K,\mathfrak{m}} = \mathrm{res} \circ \Phi_{F/K,\mathfrak{m}}$ and $\mathrm{res} : \mathrm{Gal}(F/K) \to \mathrm{Gal}(M/K)$ by $\sigma \mapsto \sigma_M$. Now if $[a] \in H$, then $\Phi_{M/K,\mathfrak{m}}([a]) = 1$. □

Fact. Let M_1/K and M_2/K be extensions of number fields and $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal. If $\mathfrak{p}$ is unramified in both M_1 and M_2, then $\mathfrak{p}$ is unramified in the composite field M_1M_2.

Example 1.9. Let $K = \mathbb{Q}(\sqrt{-5})$. We want to show the Hilbert class field F is $\mathbb{Q}(\sqrt{-5}, i)$. We know that $h_K = 2$ and $|\mathrm{Gal}(F/K)| = |\mathrm{Cl}(K)| = 2$, so F is a quadratic unramified extension of K. Consider the diagram



Fact. If $\mathfrak{p}_F \subset \mathcal{O}_F$ and $\mathfrak{p}_M \subset \mathcal{O}_M$ with M any of the intermediate fields, and if $p \in \mathbb{Z}$ is such that $\mathfrak{p}_F \mid \mathfrak{p}_M$ and $\mathfrak{p}_M \mid p$, then $e_{\mathfrak{p}_F/p} = e_{\mathfrak{p}_F/\mathfrak{p}_M} e_{\mathfrak{p}_M/p} \leq [F : \mathbb{Q}] = 4$.

Since $\mathbb{Q}(i)/\mathbb{Q}$ has discriminant 8, the only ramified prime is 2. Similarly the only prime that ramifies in $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ is 5.If $p \neq 2, 5$, then p is unramified in $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{5})$, hence in $\mathbb{Q}(\sqrt{5}, i)$. So p is unramified in $\mathbb{Q}(\sqrt{-5}, i)/\mathbb{Q}(\sqrt{-5})$.

Now $d_{K/\mathbb{Q}} = -20$, so the only ramified primes are 2 and 5. Suppose 2 is ramified in $\mathbb{Q}(\sqrt{-5}, i)/\mathbb{Q}(\sqrt{-5})$. Then $e_{\mathcal{P}_2/\mathfrak{p}_2} = 2$, where $\mathfrak{p}_2$ is an ideal in $\mathbb{Q}(\sqrt{-5})$ such that $\mathfrak{p}_2 \mid 2$, $\mathcal{P}_2 \in \mathcal{O}_F$, $\mathcal{P}_2 \mid \mathfrak{p}_2$. Since 2 is unramified in $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$, write $\mathfrak{q}_2$ for an ideal in $\mathbb{Q}(\sqrt{5})$ such that $\mathfrak{q}_2 \mid 2$. Then $e_{\mathcal{P}_2/2} = e_{\mathcal{P}_2/\mathfrak{q}_2} e_{\mathfrak{q}_2/2} = e_{\mathcal{P}_2/\mathfrak{q}_2} \cdot 1 \leq 2$ since $e_{\mathcal{P}_2/\mathfrak{q}_2}$ is at most $[F : \mathbb{Q}(\sqrt{5})]$. As $e_{\mathcal{P}_2/2} \neq 4$, 2 is unramified in $\mathbb{Q}(\sqrt{-5}, i)/\mathbb{Q}(\sqrt{-5})$. In other words, just look at the diagram above (the notation here is bad but it's an easy example). The case $p = 5$ is similar. Hence $\mathbb{Q}(\sqrt{-5}, i)/\mathbb{Q}(\sqrt{-5})$ is unramified at all finite primes. In $\mathbb{Q}(\sqrt{-5})$ we only have one infinite prime, which is complex, so unramified by definition. Hence $(\sqrt{-5}, i)$ is the Hilbert class field of $\mathbb{Q}(\sqrt{-5})$.

Definition 1.37. The **narrow Hilbert class field** is the maximal abelian extension unramified at all finite primes.

Corollary 1.38. Let f be the Hilbert class field of K. Let $\mathfrak{p}$ be a prime ideal of K. Then $\mathfrak{p}$ splits completely in $F \iff \mathfrak{p}$ is a principal ideal.

We can prove this in two ways: either we deduce this from the decomposition law, or we prove it directly, which we will now do.

Proof. We know $\mathfrak{p}$ splits completely in F if and only if $\left(\frac{F/K}{\mathfrak{p}}\right) = 1$, and $\mathrm{Cl}(K) \cong \mathrm{Gal}(F/K)$. So

$$\left(\frac{F/K}{\mathfrak{p}}\right) = 1 \iff [p] = [1] \text{ in } \mathrm{Cl}(K). \qquad \square$$

Theorem 1.39 (Principal ideal theorem)**.** In the Hilbert class field, any ideal $\mathfrak{a}$ of K becomes a principal ideal.

We don't prove this.

Example 1.10. Let $K = \mathbb{Q}(\sqrt{-5})$. Then $\mathrm{Cl}(K) = \langle [\mathcal{O}_K], [(2, 1+\sqrt{-5})] \rangle$, $F = \mathbb{Q}(\sqrt{-5}, i)$ and $(2, 1+\sqrt{-5})\mathcal{O}_F$ is generated by $(1+i)$ in $\mathcal{O}_F$.

1.1 Reciprocity theorems

Let K be a number field containing a primitive n^{th} root of unity ζ. Then for $\alpha \in \mathcal{O}_K$ coprime to $\mathfrak{p}$, we have Fermat's little theorem: $\alpha^{N(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}}$.

Exercise: Suppose $\mathfrak{p} \subset \mathcal{O}_K, \alpha \in \mathcal{O}_K$ such that $n, \alpha \notin \mathfrak{p}$. Prove that:

(i) $1, \zeta, \zeta^{n-1}$ are distinct mod $\mathfrak{p}$.

(ii) $n \mid N(\mathfrak{p}) - 1$.

(iii) $\alpha^{N(\mathfrak{p}-1)/n}$ is congruent to a unique n^{th} root of unity mod $\mathfrak{p}$.

Definition 1.40. This unique root of unity is called the n^{h} power Legendre symbol, written $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$.

05 Feb 2024, Lecture 8

Let K be a number field containing a primitive n^{th} root of ζ. Let $\alpha \in \mathcal{O}_K$ and $\mathfrak{p} \subset \mathcal{O}_K$ such that $n\alpha \notin \mathfrak{p}$. We saw that there was a unique n^{th} root of unity congruent to $\alpha^{(N(\mathfrak{p})-1)/n}$ mod $\mathfrak{p}$.

Next let $I \subset \mathcal{O}_K$ be an ideal prime to both n and α, then if $I = \mathfrak{p}_1 \dots \mathfrak{p}_r$,

$$\left(\frac{\alpha}{I}\right)_n = \prod_{i=1}^{r} \left(\frac{\alpha}{\mathfrak{p}_i}\right).$$

Let $\mathfrak{m}$ be a modulus containing all primes that contain $n\alpha$. Then we get a homomorphism $\left(\frac{\alpha}{\cdot}\right)_n : I_K(\mathfrak{m}) \to \mu_n$ with $\mu_n \subset \mathbb{C}^\times$ the group of n^{th} roots of unity. Let $L = K(\sqrt[n]{\alpha})$. Then L/K is a Galois extension. If $\sigma \in \mathrm{Gal}(L/K)$, then $\sigma(\sqrt[n]{\alpha}) = \zeta \sqrt[n]{\alpha}$ for some n^{th} root of unity, i.e. we obtain an injective homomorphism $\mathrm{Gal}(L/K) \hookrightarrow \mu_n$ by $\sigma \mapsto \zeta$.

Exercises. 1. Show that if $n\alpha \notin \mathfrak{p}$, then $\mathfrak{p}$ is unramified in L.

2. Show that $\left(\frac{L/K}{\mathfrak{p}}\right)(\sqrt[n]{\alpha}) = \left(\frac{\alpha}{\mathfrak{p}}\right)_n \sqrt[n]{\alpha}$.

Theorem 1.41 (Weak reciprocity)**.** Let K be a number field containing a primitive n^{h} root of unity. Let $\alpha \in \mathcal{O}_K$ be nonzero and $L = K(\sqrt[n]{\alpha})$. Let $\mathfrak{m}$ be a modulus divisible by all primes of K containing $n\alpha$, and assume that $\ker(\Phi_{L/K,\mathfrak{m}})$ is a congruence subgroup. Then there is a commutative diagram

$$\begin{array}{ccc} I_K(\mathfrak{m}) & \xrightarrow{\Phi_{L/K,\mathfrak{m}}} & \mathrm{Gal}(L/K) \\ & \searrow^{\left(\frac{\alpha}{\cdot}\right)_n} & \downarrow \\ & & \mu_n \end{array}$$

. Let G be the image of $\mathrm{Gal}(L/K)$ in μ_n, then $\left(\frac{\alpha}{\cdot}\right)_n$

induces a surjective homomorphism

$$\left(\frac{\alpha}{\cdot}\right)_n : I_K(\mathfrak{m})/P_K(\mathfrak{m}) \to G \subset \mu_n.$$

Proof. Commutativity follows from the second exercise above. Based on our assumptions, we have $P_K(\mathfrak{m}) \subset \ker(\Phi_{L/K,\mathfrak{m}}) \subset I_K(\mathfrak{m})$. So by the commutative diagram, $\left(\frac{\alpha}{\cdot}\right)_n$ induces a surjective homomorphism

$$I_K(\mathfrak{m})/P_K(\mathfrak{m}) \to I_K(\mathfrak{m})/\ker(\Phi_{L/K}, \mathfrak{m}) \cong \mathrm{Gal}(L/K) \to G \subset \mu_n.$$

□

Strong reciprocity gives a formula for computing $\left(\frac{\alpha}{\cdot}\right)_n$ using Hilbert symbols. We can use Weak reciprocity to prove:

Theorem 1.42 (Quadratic reciprocity)**.** Let p and q be distinct odd primes. Then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

Proof. A series of exercises. □

2 Characters, zeta functions and L–series

Motivation. In number theory, many arithmetic properties are captured in analytic objects.

2.1 Dirichlet series

Definition 2.1. A **Dirichlet series** is a series of the form

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

where $a_n \in \mathbb{C}$ and $s \in \mathbb{C}$.

Lemma 2.2 (Abel summation/Abel's lemma)**.** If (a_n) and (b_n) are sequences of complex numbers, then

$$\sum_{n=N}^{M} a_n b_n = \sum_{n=N}^{M-1} \left(\sum_{k=N}^{n} a_k\right)(b_n - b_{n+1}) + \left(\sum_{k=N}^{M} a_k\right) b_M.$$

Proof. Exercise. □

Interlude: Convergence review.

- We say a series $\sum_{n=1}^{\infty} a_n$ of complex numbers converges to L if the sequence of partial sums (A_n) with $A_n = \sum_{k=1}^{n} a_k$ converges to L.
- We say a series $\sum_{n=1}^{\infty} a_n$ of complex numbers converges absolutely if the series $\sum_n |a_n|$ of nonnegative real numbers converges.
- A sequence of complex functions $(f_n(z))$ is uniformly convergent on $S \subset \mathbb{C}$ if $\forall \epsilon > 0\ \exists N \in \mathbb{N}$ such that if $n > N$, then $|f_n(z) - f(z)| < \epsilon\ \forall z \in S$.
- A series of complex functions $\sum_{n=1}^{\infty} f_n(z)$ converges on S if for each $z_0 \in S$, $\sum_{n=1}^{\infty} f_n(z_0)$ converges as a series of complex numbers. It converges uniformly on S if the sequence of partial sums $(A_n(z))$ converges uniformly on S.
- An infinite product $\prod_n a_n$ of nonzero complex numbers is absolutely convergent when the sum $\sum_n \log a_n$ is, in which case $\prod_n a_n = \exp(\sum_n \log a_n)$.

Theorem 2.3. Let (a_n) be a sequence of complex numbers. If $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges for some $s = s_0$, then it converges for any $s \in \mathbb{C}$ with $\mathrm{Re}(s) > \mathrm{Re}(s_0)$. Moreover, it converges uniformly on every domain of the form $\{s \mid \mathrm{Re}(s) > \mathrm{Re}(s_0), |\mathrm{Arg}(s - s_0)| \leq \theta\}$ for $\theta < \frac{\pi}{2}$.[1]

Proof. Note that

$$\begin{aligned} f(s) &= \sum_{n=1}^{\infty} \frac{1}{n^{s_0}} \frac{a_n}{n^{s-s_0}} \\ &= \sum_{n=1}^{\infty} \frac{\tilde{a}_n}{n^{s-s_0}}, \end{aligned}$$

where $\tilde{a}_n = \frac{a_n}{n^{s_0}}$. We can assume $s_0 = 0$, so $\sum_{n=1}^{\infty} a_n$ converges. Let $\epsilon > 0$. Since $\sum_{n=1}^{\infty} a_n$ converges, there is a sufficiently large number N_0 such that if $M > N \geq N_0$, then $\left|\sum_{n=N}^{M} a_n\right| < \epsilon$. Let $b_n = n^{-s}$ and apply Abel's lemma to get

$$\sum_{n=N}^{M} a_n n^{-s} = \sum_{n=N}^{M-1} \left(\sum_{k=N}^{n} a_k \right) \left(n^{-s} - (n+1)^{-s} \right) + \left(\sum_{n=N}^{M} a_n \right) M^{-s}.$$

We have

$$\left| e^{-cs} - e^{-ds} \right| \leq |s| \int_c^d e^{-t\mathrm{Re(s)}} \mathrm{d}t = \frac{|s|}{\mathrm{Re}(s)} \left(e^{-c\mathrm{Re}(s)} - e^{-d\mathrm{Re}(s)} \right)$$

[1] We also need that our domain is compact.

and $\frac{|s|}{\mathrm{Re}(s)}$ is bounded by some B in our domain $\mathrm{Re}(s) > 0$, and $|\mathrm{Arg}(s)| < \theta$ for some $\theta < \frac{\pi}{2}$. Choosing $c = \log n$ and $d = \log(n+1)$ gives

$$\left|n^{-s} - (n+1)^{-s}\right| \leq \frac{|s|}{\mathrm{Re}(s)} \left(n^{-\mathrm{Re}(s)} - (n+1)^{-\mathrm{Re}(s)}\right) \leq B(n^{-\mathrm{Re}(s)} - (n+1)^{-\mathrm{Re}(s)}).$$

This gives

$$\begin{aligned}
&\left|\sum_{n=N}^{M} a_n n^{-s}\right| \leq \sum_{n=N}^{M-1} \left|\sum_{k=N}^{n} a_k\right| \left|n^{-s} - (n+1)^{-s}\right| + \left|\sum_{n=N}^{M} a_n\right| \left|M^{-s}\right| \\
\leq & B\epsilon \sum_{n=N}^{M-1} \left(n^{-\mathrm{Re}(s)} - (n+1)^{-\mathrm{Re}(s)}\right) + \epsilon M^{-\mathrm{Re}(s)} \\
\leq & \epsilon(B+1)
\end{aligned}$$

for N, M large enough. The final part follows since any s with $\mathrm{Re}(s) > 0$ is contained in a domain of the form $\{s \mid \mathrm{Re}(s) > 0, |\mathrm{Arg}(s)| \leq \theta\}$ for some $\theta < \frac{\pi}{2}$. □

07 Feb 2024, Lecture 9

Corollary 2.4. Let $f(s) = \sum a_n/n^s$ be a Dirichlet series.

(i) If the a_n are bounded, then $f(s)$ converges absolutely for $\mathrm{Re}(s) > 1$.

(ii) If $f(s)$ converges at $s = s_0$, then it converges absolutely for $\mathrm{Re}(s) > \mathrm{Re}(s_0) + 1$.

Proof. Exercise. □

Definition 2.5. Suppose a Dirichlet series $\sum a_n/n^s$ converges for some s. Then the smallest real number σ_0 such that the series converges for $\mathrm{Re}(s) > \sigma_0$ is called the **abscissa of convergence**.

Theorem 2.6. Assume there exists a number C and $\sigma_1 \geq 0$ such that $|A_n| = |a_1 + \ldots + a_n| \leq Cn^{\sigma_1} \ \forall n$. Then the abscissa of convergence of $\sum a_n/n^s$ is $\leq \sigma_1$.

Proof. We omit this. See e.g. *Algebraic Number Theory* by Lang for the proof. □

2.2 The Riemann zeta function

Definition 2.7. Let $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$. Then the Riemann zeta function is

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

By Theorem 2.6, we have $\sigma_1 = 1$, so we know $\zeta(s)$ converges for $\mathrm{Re}(s) > 1$.

We will extend $\zeta(s)$ meromorphically to $\mathrm{Re}(s) > 0$. Recall first that a function is (complex) analytic on some open $S \subset \mathbb{C}$ if for any $z_0 \in S$, we can write $f(z) = \sum_{n=0}^{\infty} a_n (z - z_0)^n$, where $a_n \in \mathbb{C}$ and the series converges to $f(z)$ for z in a neighborhood of z_0. This is equivalent to being holomorphic.

A function is meromorphic on $S \subset \mathbb{C}$ if it is holomorphic on all of S, except for a set of isolated points called poles. If f is meromorphic, a pole of f is a zero of $\frac{1}{f}$. Suppose z_0 is a pole, then for some integer n, $(z - z_0)^n f(z)$ is holomorphic and nonzero in a neighborhood of z_0, and then z_0 is a pole of order n. If $n = 1$, then z_0 is called a simple pole and the residue is $\mathrm{Res}(f, z_0) = \lim_{z \to z_0} (z - z_0) f(z)$.

If f is a meromorphic/analytic function defined on some open $S \subset \mathbb{C}$ with $S \subset T$, $T \subset \mathbb{C}$ open, and F is a meromorphic/analytic function defined on T such that $F(z) = f(z)\ \forall z \in S$, then F is called a meromorphic/analytic continuation of f.

Theorem 2.8. The Riemann zeta function $\zeta(s)$ has a meromorphic continuation to $\mathrm{Re}(s) > 0$ with a simple pole at $s = 1$ with residue equal to 1. If $\delta > 0$, then the series $\sum_{n=1}^{\infty} 1/n^s$ converges absolutely in the region $\mathrm{Re}(s) \geq 1 + \delta$.

(In fact, the Riemann zeta function is analytic for $\mathrm{Re}(s) > 0$ except for the simple pole at $s = 1$.)

Proof. Let $s > 1$ be real. Then

$$\frac{1}{s-1} \leq \int_1^{\infty} \frac{1}{x^s} \mathrm{d}x \leq \zeta(s) \leq 1 + \frac{1}{s-1},$$

so for $s > 1$, $1 \leq (s-1)\zeta(s) \leq s$ and so $\lim_{s \to 1^+} (s-1)\zeta(s) = 1$. If we show that we can continue (i.e. extend) $\zeta(s)$, we can conclude that $\zeta(s)$ has a simple pole at $s = 1$ with residue 1.

To continue $\zeta(s)$, consider the alternating Riemann zeta function

$$\zeta_2(s) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^s} = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \dots.$$

Since the partial sums of the coefficients are 1 or 0, they are bounded, hence by Theorem 2.6, this converges for $\mathrm{Re}(s) > 0$. We have

$$\begin{aligned} \frac{2}{2^s}\zeta(s) + \zeta_2(s) &= \zeta(s) \\ \implies \zeta(s) &= \zeta_2(s) \left(1 - \frac{1}{2^{s-1}}\right)^{-1}. \end{aligned}$$

This gives us an analytic continuation to the line $\mathrm{Re}(s) = 0$. We show there are no poles except at $s = 1$. From our expression for $\zeta_2(s)$, we see the only possible poles other than $s = 1$ satisfy $1 - 2^{1-s} = 0 \iff 2^{s-1} = 1 \iff s = \frac{2\pi i n}{\log 2} + 1$ for some integer n. Consider for $r = 2, 3, \ldots$ the function

$$\zeta_r(s) = \frac{1}{1^s} + \frac{1}{2^s} + \ldots + \frac{1}{(r-1)^s} - \frac{r-1}{r^s} + \frac{1}{(r+1)^s} + \ldots,$$

e.g. for $r = 3$ we get

$$\zeta_3(s) = \sum_{n=0}^{\infty} \frac{1}{(3n+1)^3} + \frac{1}{(3n+2)^3} - \frac{2}{(3n+3)^3}.$$

The partial sums of the coefficients are bounded by r, so $\zeta_r(s)$ converges for $\mathrm{Re}(s) > 0$ by Theorem 2.6. We have

$$\zeta(s) = \frac{\zeta_r(s)}{1 - \frac{1}{r^{s-1}}}$$
$$\implies \zeta(s) = \frac{\zeta_3(s)}{1 - 3^{1-s}},$$

so the only poles occur when $3^{s-1} = 1 \iff s = \frac{2\pi i m}{\log 3} + 1$ for some integer m. Hence at any such pole we need $3^n = 2^m$, so $n = m = 0$. □

Theorem 2.9. Let (a_n) be a sequence of complex numbers and let $A_n = a_1 + \ldots + a_n$. Let $0 \leq \sigma_1 \leq 1$ and assume there is $z_0 \in \mathbb{C}$ and a constant $C > 0$ such that for all n, $|A_n - nz_0| \leq Cn^{\sigma_1}$. Then $f(s) = \sum_{n=1}^{\infty} a_n/n^s$ (defined say for $\mathrm{Re}(s) > 1$) has an analytic continuation to $\mathrm{Re}(s) > \sigma_1$ where it is analytic, except for a simple pole with residue z_0 at $s = 1$.

Proof. Consider $f(s) - z_0\zeta(s)$ and apply Theorem 2.6 and Theorem 2.8. □

Proposition 2.10. We have

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}.$$

Proof. We write $E(s) = \prod_p \frac{1}{1-p^{-s}}$, then $\log E(s) = \sum_p \sum_{n=1}^{\infty} \frac{1}{np^{ns}}$. Let $\mathrm{Re}(s) > 1 + \delta$. Then $|p^{ns}| = p^{n\mathrm{Re}(s)} \geq p^{(1+\delta)n}$, so

$$\sum_p \sum_{n=1}^{\infty} \left(\frac{1}{p^{1+\delta}}\right)^n = \sum_p \frac{1}{p^{1+\delta} - 1} \leq 2 \sum_p \frac{1}{p^{1+\delta}}$$

which converges, so the series $E(s)$ converges absolutely. We need to show equality, so again use $\frac{1}{1-p^{-s}} = 1 + p^{-s} + p^{-2s} + \ldots$. Fix $N \in \mathbb{N}$ and let $p_1, \ldots, p_r$

be the primes less than N. Then

$$\prod_{p\leq N}\frac{1}{1-p^{-s}}=\prod_{v_1,\dots,v_r\geq 0}^{\infty}\frac{1}{(p_1^{v_1}\dots p_r^{v_r})^s}=\sum_n{}'\frac{1}{n^s}$$

where Σ' denotes the sum over all natural numbers only divisible by primes $p\leq N$. It contains all $n\leq N$, so

$$\begin{aligned}\prod_{p\leq N}\frac{1}{1-p^{-s}}&=\sum_{n\leq N}\frac{1}{n^s}+\sum_{n>N}{}'\frac{1}{n^s}\\ \implies\left|\prod_{p\leq N}\frac{1}{1-p^{-s}}-\zeta(s)\right|&\leq\left|\sum_{n>N,p_i\nmid n}\frac{1}{n^s}\right|\leq\sum_{n>N}\frac{1}{n^{1+\delta}}\overset{N\to\infty}{\to}0.\end{aligned}$$ □

09 Feb 2024, Lecture 10

Remark. If a Dirichlet series is convergent on some half plane $\mathrm{Re}(s)>\sigma_0$, then it defines an analytic function on this half plane. This follows from Theorem 2.3.

Definition 2.11. The **gamma function** is the absolutely convergent integral

$$\Gamma(s)=\int_0^\infty e^{-y}y^s\frac{\mathrm{d}y}{y},$$

defined for $\mathrm{Re}(s)>0$.

Proposition 2.12. (i) The gamma function is analytic and admits a meromorphic continuation to all of $\mathbb{C}$.

(ii) The gamma function is nowhere zero and only has simple poles at $s=-n, n=0,1,2,\dots$ with residues $\frac{(-1)^n}{n!}$.

(iii) We have the functional equations

- $\Gamma(s+1)=s\Gamma(s)$,
- $\Gamma(s)\Gamma(1-s)=\frac{\pi}{\sin(\pi s)}$,
- $\Gamma(s)\Gamma\left(s+\frac{1}{2}\right)=\frac{2\sqrt{\pi}}{2^{2s}}\Gamma(2s)$.

(iv) The gamma function has special values

- $\Gamma\left(\frac{1}{2}\right)=\sqrt{\pi}$,
- $\Gamma(1)=1$,
- $\Gamma(k+1)=k!\ \forall k\in\mathbb{Z}_{\geq 0}$.

Proof. Omitted. □

We use $\Gamma(s)$ to complete the Riemann zeta function. For $\Gamma(s) = \int_0^\infty e^{-y} y^s \frac{\mathrm{d}y}{y}$, substitue $y \mapsto \pi n^2 y$ to get

$$\pi^{-s}\Gamma(s)\frac{1}{n^{2s}} = \int_0^\infty e^{-\pi n^2 y} y^s \frac{\mathrm{d}y}{y}$$

and summing over all n gives

$$\pi^{-s}\Gamma(s)\zeta(2s) = \int_0^\infty \sum_{n=1}^\infty e^{-\pi n^2 y} y^s \frac{\mathrm{d}y}{y}.$$

Note we can swap the order of the ingral and the sum, since

$$\sum_{n=1}^\infty \int_0^\infty \left| e^{-\pi n^2 y} y^s \right| \frac{\mathrm{d}y}{y} = \sum_{n=1}^\infty \int_0^\infty e^{-\pi n^2 y} y^{\mathrm{Re}(s)} \frac{\mathrm{d}y}{y} = \pi^{-\mathrm{Re}(s)}\Gamma(\mathrm{Re}(s))\zeta(2\mathrm{Re}(s))$$

for $\mathrm{Re}(s) > 1$.

Definition 2.13. The function

$$Z(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

is called the **complete zeta function**.

Definition 2.14. Let $\theta(z) = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 z}$ be the **Jacobi theta series**.

Proposition 2.15. The series $\theta(z)$ is analytic on $\mathfrak{h} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ and satisfies $\theta\left(-\frac{1}{z}\right) = \sqrt{\frac{z}{i}}\theta(z)$, where $\sqrt{\frac{z}{i}} = e^{\frac{1}{2}\log(z/i)}$.

Proof. Omitted. □

Proposition 2.16. We have $Z(s) = \frac{1}{2}\int_0^\infty (\theta(iy) - 1)\, y^{s/2} \frac{\mathrm{d}y}{y}$.

Proof. Follows from the above and the fact that $\theta(z) = 1 + 2\sum_{n=1}^\infty e^{\pi i n^2 z}$. □

Definition 2.17. Let $f : \mathbb{R}_+ \to \mathbb{C}$ be a continuous function (here $\mathbb{R}_+$ is the group of positive real numbers). Then the **Mellin transform** is the improper integral

$$M(f, s) = \int_0^\infty (f(y) - f(\infty)) y^s \frac{\mathrm{d}y}{y}$$

provided that the limit $f(\infty) = \lim_{y\to\infty} f(y)$ and the integral exist.

Theorem 2.18 (Mellin principle)**.** Let $f, g : \mathbb{R}_+ \to \mathbb{C}$ be continuous such that $f(y) = a_0 + O(e^{-c_0 y^\alpha})$ and $g(y) = b_0 + O(e^{-c_0 y^\alpha})$ with c_0, α positive constants. If $f\left(\frac{1}{y}\right) = Cy^k g(y)$ for some real $k > 0$ and some $0 \neq C \in \mathbb{C}$, then:

(i) The integrals $M(f,s)$ and $M(g,s)$ converge absolutely and uniformly for s in a compact subset of $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > k\}$ and admit holomorphic continuations to $\mathbb{C} \setminus \{0,k\}$.

(ii) The integrals have simple poles at $s=0$ and $s=k$ such that

$$\begin{aligned} \mathrm{Res}_{s=0} M(f,s) &= -a_0 & \mathrm{Res}_{s=k} M(f,s) &= Cb_0 \\ \mathrm{Res}_{s=0} M(g,s) &= -b_0 & \mathrm{Res}_{s=k} M(g,s) &= C^{-1}a_0. \end{aligned}$$

(iii) We have $M(f,s) = CM(g,k-s)$.

Proof. Omitted. □

Theorem 2.19. The completed zeta function $Z(s)$ admits an analytic continuation to $\mathbb{C} \setminus \{0,1\}$. It has simple poles at $s=0$ and $s=1$ with residues -1 and 1, and satisfies the functional equation $Z(s) = Z(1-s)$.

Proof. By Proposition 2.16 and Definition 2.17, we have $Z(2s) = M(f,s)$ for $f(y) = \frac{1}{2\theta(iy)}$. Note $\theta(iy) = 1 + 2e^{-\pi y}(1 + \sum_{n=2}^{\infty} e^{-\pi(n^2-1)y})$, so we have $f(y) = \frac{1}{2} + O(e^{-\pi y})$. By Proposition 2.15, we have

$$f\left(\frac{1}{y}\right) = \frac{1}{2}\theta(\frac{-1}{iy}) = \frac{1}{2}y^{1/2}\theta(iy) = y^{1/2}f(y).$$

So by the Mellin principle, $M(f,s)$ has a holomorphic continuation to $\mathbb{C} \setminus \left\{0, \frac{1}{2}\right\}$ with simple poles at 0 and $\frac{1}{2}$ with residues $\frac{1}{2}$ and $-\frac{1}{2}$, and $M(f,s) = M(f, \frac{1}{2} - s)$.

Hence $Z(s) = M\left(f, \frac{s}{2}\right)$ has a holomorphic continuation to $\mathbb{C} \setminus \{0,1\}$ with simple poles at $s=0$ and $s=1$ with residues -1 and 1, and we obtain $Z(s) = M\left(f, \frac{s}{2}\right) = M\left(f, \frac{1-s}{2}\right) = Z(1-s)$. □

Corollary 2.20. The function $\zeta(s)$ admits an analytic continuation to $\mathbb{C} \setminus \{1\}$, has a simple pole at $s=1$ with residue 1 and satisfies

$$\zeta(1-s) = 2(2\pi)^{-s}\Gamma(s)\sin\left(\frac{\pi(1-s)}{2}\right)\zeta(s).$$

Proof. Recall $z(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$, which has a simple pole at $s=0$ and so does $\Gamma\left(\frac{s}{2}\right)$, hence $\zeta(s)$ has no pole at 0. At $s=1$, $Z(s)$ has a simple pole and $\Gamma\left(\frac{s}{2}\right)$ does not, so $\zeta(s)$ does. Now

$$\mathrm{Res}_{s=1}\zeta(s) = \pi^{1/2}\Gamma\left(\frac{1}{2}\right)^{-1}\mathrm{Res}_{s=1} Z(s) = 1$$

by Theorem 2.19. Now from the functional equation from Theorem 2.18,

$$\zeta(1-s) \overset{(\dagger)}{=} \pi^{\frac{1}{2}-s} \frac{\Gamma\left(\frac{s}{2}\right)}{\Gamma\left(\frac{1-s}{2}\right)} \zeta(s).$$

By Proposition 2.12, we have

$$\begin{aligned} \Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{1+s}{2}\right) &= \frac{2\sqrt{\pi}}{2^s}\Gamma(s), \\ \Gamma\left(\frac{1-s}{2}\right)\Gamma\left(\frac{1+s}{2}\right) &= \frac{\pi}{\sin\left(\frac{\pi s}{2}\right)}, \\ \Longrightarrow \frac{\Gamma\left(\frac{s}{2}\right)}{\Gamma\left(\frac{1-s}{2}\right)} &= \frac{2}{2^s\sqrt{\pi}} \sin\left(\frac{\pi s}{2}\right)\Gamma(s). \end{aligned}$$

Insert this into (†) to get our result, i.e.

$$\zeta(1-s) = 2(2\pi)^{-s}\Gamma(s)\sin\left(\frac{\pi(1-s)}{2}\right)\zeta(s).$$

□

What about the zeroes of $\zeta(s)$? We have that

- $\zeta(s) \neq 0$ for $\mathrm{Re}(s) > 1$.
- For $\mathrm{Re}(s) < 0$, we have trivial zeroes at $s = -2, -4, -6, \ldots$.
- Any other zeroes have to lie in the critical strip $0 \leq \mathrm{Re}(s) \leq 1$.

The Riemann hypothesis says that all the nontrivial zeroes of $\zeta(s)$ lie on the line $\mathrm{Re}(s) = \frac{1}{2}$.

2.3 The Dedekind zeta function

12 Feb 2024, Lecture 11

Let K be a number field.

Definition 2.21. The **Dedekind zeta function** of K is the series

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$$

for $\mathfrak{a}$ varying over integral ideals of K, and $N(\mathfrak{a})$ the absolute norm.

Proposition 2.22. The series $\zeta_K(s)$ converges absolutely and uniformly in the domain $\{\mathrm{Re}(s) > 1 + \delta\}$ for every $\delta > 0$ and one has

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^s}$$

for $\mathfrak{p}$ running through the prime ideals of K.

Proof. Exercise. This is similar to the same proof for $\zeta(s)$. □

We can also complete $\zeta_K(s)$. Let $Z_\infty(s) = \left|d_{K/\mathbb{Q}}\right|^{5/2} \pi^{-ns/2}\Gamma_k\left(\frac{s}{2}\right)$ for n the degree of K, the "Euler factor at infinity".

Definition 2.23. The **completed zeta function** of the number field K is

$$Z_K(s) = Z_\infty(s)\zeta_K(s).$$

Proposition 2.24. The completed zeta function $Z_K(s)$ admits an analytic continuation to $\mathbb{C} \setminus \{0, 1\}$ and satisfies $Z_K(s) = Z_K(1-s)$. It has simple poles at $s = 0$ and $s = 1$ with residues $-\frac{2^r h_K R}{\omega}$ and $\frac{2^r h_K R}{\omega}$, where r is the number of infinite primes, h_K is the class number, ω is the number of roots of unity in K, and R is the regulator.

Corollary 2.25. (i) The Dedekind zeta function $\zeta_K(s)$ admits an analytic continuation to $\Gamma \setminus \{1\}$.

(ii) At $s = 1$, we have a simple pole with residue

$$\mathrm{Res}_{s=1}\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h_K R}{\omega \left|d_K\right|^{1/2}}$$

for r_1 the number of real infinite primes and r_2 the number of complex infinite primes.

(iii) We have the functional equation $\zeta_K(1-s) = A(s)\zeta_K(s)$.

Remark. The formula for $\mathrm{Res}_{s=1}\zeta_K(s)$ is known as the analytic class number formula. Let $\kappa = \frac{2^{r_1}(2\pi)^{r_2} R}{\omega |d_K|^{1/2}}$, then $\mathrm{Res}_{s=1}\zeta_K(s) = \kappa h_K$.

Let $K = \mathbb{Q}(\sqrt{N})$ for $N \neq 0, 1$ squarefree. We get

$$\begin{aligned}\zeta_K(s) &= \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p}^s)}\right)^{-1} \\ &= \prod_{\mathfrak{p} \text{ splits}} \left(1 - \frac{1}{\mathfrak{p}^s}\right)^{-2} \prod_{\mathfrak{p} \text{ inert}} \left(1 - \frac{1}{\mathfrak{p}^{2s}}\right)^{-1} \prod_{\mathfrak{p} \text{ ramifies}} \left(1 - \frac{1}{\mathfrak{p}^s}\right)^{-1}.\end{aligned}$$

From this we see that $\zeta(s)$ divides $\zeta_K(s)$, and we have

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{\mathfrak{p}} \left(1 - \frac{\chi_K(\mathfrak{p})}{p^s}\right)^{-1},$$

where

$$\chi_K(\mathfrak{p}) = \begin{cases} 1 & \mathfrak{p} \text{ splits} \\ -1 & \mathfrak{p} \text{ inert} \\ 0 & \mathfrak{p} \text{ ramifies} \end{cases}$$

is an (extended) Dirichlet character.

Definition 2.26. A **Dirichlet chracter** mod m is a homomorphism

$$\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times.$$

It is called **primitive** if it doesn't arise as the composite $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/m'\mathbb{Z})^\times \xrightarrow{\chi'} \mathbb{C}^\times$ for a Dirichlet character χ' mod m' for a proper divisor $m' \mid m$.

If χ is a Dirichlet character mod $\mathfrak{f}$ and χ is primitive, then $\mathfrak{f}$ is called the **conductor** of χ.

Remark. The conductor is the greatest common divisor of all $m' \mid m$ such that a Dirichlet character mod m is induced from a character mod m'.

A Dirichlet character mod m can be extended to all of $\mathbb{Z}$ as follows:

$$\chi(n) = \begin{cases} \chi(n \bmod m) & (n,m) = 1 \\ 0 & (n,m) \neq 1. \end{cases}$$

Example 2.1.

$$\chi_K(\mathfrak{p}) = \begin{cases} 1 & \mathfrak{p} \text{ splits} \\ -1 & \mathfrak{p} \text{ inert} \\ 0 & \mathfrak{p} \text{ ramifies} \end{cases}$$

is a Dirichlet character mod $d_K/\mathbb{Q}$.

Definition 2.27. The **principal character** mod m is the trivial character χ_0 mod m,

$$\chi_0(n) = \begin{cases} 1 & (n,m) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Suppose χ_1, χ_2 are two Dirichlet characters mod m. Then define $\chi_1\chi_2$ by $\chi_1\chi_2(n) = \chi_1(n)\chi_2(n)$. This turns the collection of all characters of $(\mathbb{Z}/m\mathbb{Z})^\times$ into an abelian group. Write $\widehat{(\mathbb{Z}/m\mathbb{Z})^\times}$ with identity χ_0 and the inverse of any χ equal to $n \mapsto \chi(n)^{-1}$.

Let A be any abelian group. Let $\widehat{A}$ be the group of homomorphisms $\chi : A \to \mathbb{C}^\times$. This is the **character group** or **dual group** of A.

Proposition 2.28. If A is a finite abelian group, then $A \cong \widehat{A}$.

Proof. Use induction on the order of A. Assume A is cyclic with order m and generator y. Then $y^m = 1$, so $\chi(y)$ is an m^{th} root of unity for every χ and every character is determined by $\chi(y)$. Let ζ be a primitive m^{th} root of unity. Then for each $r = 0, 1, \ldots, m-1$, the function $\chi_r(y^s) = (\zeta^r)^j$ is a character, these are all distinct and $\chi_r = \chi_1^r$, so $\widehat{A}$ is the cyclic group generated by χ_1. But $\chi_1^r(y) = 1 \iff \zeta^r = 1$, so χ_1 must have order m, so $\widehat{A}$ is cyclic of order m, so $\widehat{A} \cong A$.

Now suppose $A = A_1 \times A_2$ with A_1, A_2 cyclic and such that $A_i \neq 1$. We will to show that $\widehat{A} \cong \widehat{A_1} \times \widehat{A_2}$. For this, define $\widehat{A} \to \widehat{A_1} \times \widehat{A_2}$ by $\chi \mapsto (\chi|_{A_1}, \chi|_{A_2})$ which has inverse $\widehat{A_1} \times \widehat{A_2} \to \widehat{A}$ by $(\chi_1, \chi_2) \mapsto \chi$ via $(a_1, a_2) \mapsto \chi_1(a_1)\chi_2(a_2)$. It follows by induction that $\widehat{A_i} \cong A_i$, so we're done. □

Recall that $(\mathbb{Z}/m\mathbb{Z})^\times$ has order $\phi(m)$, hence so does $\widehat{(\mathbb{Z}/m\mathbb{Z})^\times}$.

Example 2.2. Let $m = 4$, so $\phi(m) = 2$. We have two characters mod 4: these are χ_0 mod 4 and χ_1 given by $\chi_1(n) = \begin{cases} 1 & n \equiv 1 \pmod 4 \\ -1 & n \equiv 3 \pmod 4 \\ 0 & 2 \mid n. \end{cases}$

Corollary 2.29. If A is a finite abelian group, then $A \cong \widehat{\widehat{A}}$ via the correspondence sending

$$A \to \widehat{\widehat{A}}$$
$$a \mapsto \tilde{a} : \widehat{A} \to \mathbb{C}^\times \text{ defined by } \chi \mapsto \chi(a).$$

Proof. Left as an exercise. □

Proposition 2.30 (Orthogonality relations)**.** Let A be a finite abelian group and $a \in A$.

(i) If $\chi \in \widehat{A}$, $\sum_{a \in A} \chi(a) = \begin{cases} 0 & \chi \neq \chi_0 \\ |A| & \chi = \chi_0. \end{cases}$

(ii) $\sum_{\chi \in \widehat{A}} \chi(a) = \begin{cases} 0 & \text{if } a \neq 1 \\ |A| & \text{if } a = 1. \end{cases}$

14 Feb 2024, Lecture 12

Proof. (i) Let $\chi \in \widehat{A}$, $\chi \neq \chi_0$. Let $b \in A$ be such that $\chi(b) \neq 1$. Then

$$\sum_{a \in A} \chi(a) = \sum_{a \in A} \chi(ab) = \chi(b) \sum_{a \in A} \chi(a),$$

so $\sum_{a \in A} \chi(a) = 0$. The second part of (i) is immediate.

(ii) Note by Proposition 2.28 that $\sum_{\chi\in\widehat{A}}\chi(a)=\sum_{\chi\in\widehat{A}}\tilde{a}(\chi)$, and now use (i). □

Proposition 2.31. Let χ be a Dirichlet character mod m. If $\chi\neq\chi_0$, then $\left|\sum_{n\leq x}\chi(n)\right|\leq m$.

Proof. Exercise. □

2.4 Dirichlet L-series

Definition 2.32. Let χ be a Dirichlet character. Then the **Dirichlet L-series** is

$$L(\chi,s)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}.$$

Proposition 2.33. For $\mathrm{Re}(s)>1$, the series $L(\chi,s)$ converges absolutely and we get an Euler product

$$L(\chi,s)=\prod_p\left(1-\frac{\chi(p)}{p^s}\right)^{-1}.$$

If χ is nontrivial, then $L(\chi,s)$ extends to a analytic function for $\mathrm{Re}(s)>0$.

Proof. The first part is an exercise. The second part follows from Theorem 2.6 and Proposition 2.31. □

We can write

$$L(\chi,s)=\prod_{p\nmid m}\left(1-\frac{\chi(p)}{p^s}\right)^{-1},$$

so for $\chi=\chi_0$,

$$L(\chi_0,s)=\zeta(s)\cdot\prod_{p\mid m}\left(1-\frac{1}{p^s}\right).$$

Write $\zeta_K(s)$ as a product of L-functions. Let $K=\mathbb{Q}(\zeta_m)$.

Proposition 2.34. Let $K=\mathbb{Q}(\zeta_m)$ and let $m=\prod_p p^{v_p}$ be the prime factorization. For every prime p, let f_p be the smallest positive integer such that

$$p^{f_p}\equiv 1\left(\mathrm{mod}\ \frac{m}{p^{v_p}}\right).$$

Then $p\mathcal{O}_K = (\mathfrak{p}_1, \ldots, \mathfrak{p}_r)^{\phi(p^{v_p})}$ with $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ distinct prime ideals, all of degree f_p. In particular, if $p \nmid m$, then the order of $[p]$ in $(\mathbb{Z}/m\mathbb{Z})^\times$ if f_p.

Proof. Omitted, can be found in Neukirch's book. □

Proposition 2.35. Let $K = \mathbb{Q}(\zeta_m)$. Then

$$\zeta_K(s) = \prod_{\mathfrak{p}|m}(1 - N(\mathfrak{p})^{-s})^{-1} \prod_{\chi \in \widehat{(\mathbb{Z}/m\mathbb{Z})^\times}} L(\chi, s)$$

Since $(\mathbb{Z}/m\mathbb{Z})^\times \cong \mathrm{Gal}(K/\mathbb{Q})$, $\chi \in (\mathbb{Z}/m\mathbb{Z})^\times$ can also be viewed as a character of $\mathrm{Gal}(K/\mathbb{Q})$.

Proof. Let $p\mathcal{O}_K = (\mathfrak{p}_1, \ldots, \mathfrak{p}_r)^e$, and let $f = f_{\mathfrak{p}_i|p}$, so $N(\mathfrak{p}_i) = p^f$. Since we have $\zeta_K(s) = \prod_{\mathfrak{p}}(1 - N(\mathfrak{p})^{-s})^{-1}$, $\zeta_K(s)$ contains

$$\prod_{\mathfrak{p}|p}(1 - N(p)^{-s})^{-1} = (1 - p^{-fs})^{-r}.$$

For fixed p, $\prod_\chi L(\chi, s)$ gives the factor $\prod_\chi \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$, which is 1 if $p \mid m$. Assume $p \nmid m$, then $e = 1$ and f is the order of $[p]$ in $(\mathbb{Z}/m\mathbb{Z})^\times$ by Proposition 2.33. Write G_p for the subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$ generated by $[p]$. Since $efr = |(\mathbb{Z}/m\mathbb{Z})^\times| = \phi(m)$, this gives that $r = \frac{\phi(m)}{f}$ is the index of G_p in $(\mathbb{Z}/m\mathbb{Z})^\times$.

There is an isomorphism between $\widehat{G_p}$ and μ_f, the group of f^{th} roots of unity by $\widehat{G_p} \to \mu_f$, $\chi \mapsto \chi(p)$. Let $G = (\mathbb{Z}/m\mathbb{Z})^\times$, then this gives us an exact sequence

$$1 \to \widehat{G/G_p} \to \widehat{G} \to \mu_j \to 1.$$

This means we have $r = \left|\widehat{G/G_p}\right| = [G : G_p]$ elements in the preimage of $\chi(p)$. Then

$$\prod_\chi \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \prod_{\zeta \in \mu_f} \left(1 - \frac{\zeta}{p^s}\right)^{-r} = (1 - p^{-fs})^{-r},$$

so $\prod_\chi L(\chi, s)$ and $\zeta_K(s)$ both contain these terms. Take the product over all primes $p \nmid m$ to get the result. □

Since $L(\chi_0, s) = \zeta(s)\prod_{p|m}\left(1 - \frac{1}{p^s}\right)$, we have

$$\zeta_K(s) = \prod_{\mathfrak{p}|m}(1 - N(\mathfrak{p})^{-s}) \left(\zeta(s)\prod_{p|m}\left(1 - \frac{1}{p^s}\right)\right) \prod_{\chi \neq \chi_0} L(\chi, s).$$

Since $\zeta_K(s)$ and $\zeta(s)$ have poles at $s = 1$, we have:

Proposition 2.36. Every nontrivial Dirichlet character χ satisfies $L(\chi, 1) \neq 0$.

Theorem 2.37 (Dirichlet's Prime Number Theorem)**.** Every arithmetic progression of the form $a \pm km, k \in \mathbb{Z}$ with $(a, m) = 1$, i.e. every class a mod m contains infinitely many prime numbers.

Proof. Note $L(\chi, s) \neq 0$ for $\mathrm{Re}(s) > 1$ and we have

$$\begin{aligned} L(\chi, s) &= \prod_p (1 - \chi(p)p^{-s})^{-1} \\ \implies \log L(\chi, s) &= -\sum_p \log(1 - \chi(p)p^{-s}) \\ &= \sum_p \sum_{n \geq 1} \frac{\chi(p)^n p^{-ns}}{n}. \end{aligned}$$

This converges absolutely for $\mathrm{Re}(s) > 1$ since

$$\begin{aligned} \left| \frac{\chi(p)^n}{np^{ns}} \right| &\leq \frac{1}{p^{ns}} = \frac{1}{p^{n\mathrm{Re}(s)}} \\ \implies \sum_p \sum_{n \geq 1} \frac{1}{p^{n\mathrm{Re}(s)}} &\leq \sum_{m \geq 1} \frac{1}{m^{\mathrm{Re}(s)}}, \end{aligned}$$

which converges for $\mathrm{Re}(s) > 1$. Hence

$$\log L(\chi, s) = \sum_p \frac{\chi(p)}{p^s} + \sum_p \sum_{n \geq 2} \frac{\chi(p)^n}{np^{ns}},$$

where the latter sum is absolutely convergent for $\mathrm{Re}(s) > \frac{1}{2}$ and takes a finite value at $s = 1$. Write

$$g_\chi(s) = \sum_p \sum_{n \geq 2} \frac{\chi(p)^n}{np^{ns}}.$$

Let $(a, m) = 1$. Then

$$\begin{aligned}
&\sum_{\chi \in \widehat{(\mathbb{Z}/m\mathbb{Z})^\times}} \chi(a)^{-1} \log L(\chi, s) \\
=&\sum_{\chi} \chi(a^{-1}) \left(\sum_p \frac{\chi(p)}{p^s} + g_\chi(s) \right) \\
=&\sum_p \frac{1}{p^s} \sum_\chi \chi(a^{-1})\chi(p) + \sum_\chi \chi(a)^{-1} g_\chi(s) \\
=&\sum_p \frac{1}{p^s} \sum_\chi \chi(pa^{-1}) + \sum_\chi \chi(a^{-1}) g_\chi(s).
\end{aligned}$$

By orthogonality,

$$\sum_\chi \chi(pa^{-1}) = \begin{cases} \phi(m) & p \equiv a \pmod m \\ 0 & \text{otherwise.} \end{cases}$$

This gives

$$\begin{aligned}
&\sum_\chi \chi(a)^{-1} \log L(\chi, s) \\
=&\phi(m) \sum_{p \equiv a \bmod m} p^{-s} + \left(\text{smth. that conv. for } \mathrm{Re}(s) > \frac{1}{2} \right).
\end{aligned}$$

Let $s \to 1$, then the RHS is

$$\lim_{s \to 1} \phi(m) \sum_{p \equiv a \bmod m} p^{-s} + (\text{finite constant})$$

finite since the theorem is false?? wtf does this mean? TODO: check it

Since $L(\chi_0, s) = \zeta(s) \prod_{p|m} (1 - p^{-s})$, so $\log L(\chi_0, s) \to \infty$ as $s \to 1$ (since $\zeta(s)$ has a pole at $s = 1$). We know $L(\chi, 1)$ is defined for $\chi \neq \chi_0$ and $L(\chi, 1) \neq 0$, so $\log L(\chi, 1)$ will be finite for $\chi \neq \chi_0$, so $\sum_\chi \chi(a)^{-1} \log L(\chi, s) \to \infty$ as $s \to 1^+$, so the same is true for the RHS. □

16 Feb 2024, Lecture 13

Lecture start summary: Let $K/\mathbb{Q}$ be abelian. Then $K \subset \mathbb{Q}(\zeta_m)$ for some m. Let $G = \mathrm{Gal}(K/\mathbb{Q})$ and consider its image in $(\mathbb{Z}/m\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. We can consider characters of G as Dirichlet characters mod m, and view $\widehat{G}$ as a subgroup of $\widehat{(\mathbb{Z}/m\mathbb{Z})^\times}$.

Proposition 2.38. For K as above, we have

$$\zeta_K(s) = \prod_{\mathfrak{p}|m}(1 - N(\mathfrak{p})^{-s})^{-1} \prod_{\chi \in \widehat{G}} L(\chi, s)$$

for $\mathrm{Re}(s) > 1$.

Proof. Similar to Proposition 2.35, left as an exercise. □

Corollary 2.39. We have

$$h_K = \left(\prod_{\mathfrak{p}|m} \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{p^{f_p}}\right) \right)^{-r_p} \prod_{\chi \neq \chi_0} L(\chi, 1)/K.$$

Proof. Follows from the analytic class number formula and

$$L(\chi, s) = \zeta(s) \prod_{p|m} \left(1 - \frac{1}{p^s}\right)$$

and the fact that $\zeta(s)$ has a simple pole at $s = 1$ with residue 1. □

There exist explicit formulae for $L(\chi, 1)$ that we can use to compute h_K (see e.g. Marcus). In Ex. Sheet 2, there is an exercise making this explicit in the quadratic case. If $K = \mathbb{Q}(\sqrt{N})$, for $N \neq 0, 1$ squarefree, let $m = \left|d_{K/\mathbb{Q}}\right|$, then $K \subset \mathbb{Q}(\zeta_m)$.

Next we will prove a fundamental inequality and a more general version of Dirichlet's prime number theorem.

Notation. Write $f(s) \sim g(s)$ to mean that two functions which have a singularity at $s = 1$ differ by a function that is analytic at $s = 1$. So $\zeta(s) \sim \frac{1}{s-1}$, which is because

$$\log -\zeta(s) = \sum_p \sum_{n \geq 1} \frac{1}{np^{ns}} = \sum_p \frac{1}{p^s} + \sum_p \sum_{n \geq 2} \frac{1}{np^{ns}}$$

and the second term converges uniformly and absolutely for $\mathrm{Re}(s) > \frac{1}{2}$, so only $\sum_p p^{-s}$ contributes to the singularity at $s = 1$, so $\log \zeta(s) \sim \sum_p p^{-s} \sim \log \frac{1}{s-1}$.

Similarly, since $\log \zeta_K(s) = \sum_{\mathfrak{p}} \sum_{n \geq 1} \frac{1}{nN(\mathfrak{p})^s}$, we have

$$\log \zeta_K(s) \sim \sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s} \sim \sum_{\deg \mathfrak{p} = 1} \frac{1}{N(\mathfrak{p})^s},$$

where a degree one prime is a prime whose residue field degree over $\mathbb{Q}$ is 1, or equivalently a prime ideal whose absolute norm is a prime number. Note

$$\zeta_K(s) = \sum_{C \in \mathrm{Cl}(K)} \zeta(C, s)$$

for $\zeta(C, s)$ the **partial zeta function**, i.e.

$$\zeta_K(s) = \sum_{\mathfrak{a} \in C} \frac{1}{N(\mathfrak{a})^s}.$$

Proposition 2.40. Let $[K : \mathbb{Q}] = n$ and let $C \in \mathrm{Cl}(K)$ be an ideal class. Then $\zeta(C, s)$ is analytic for $\mathrm{Re}(s) > 1 - \frac{1}{n}$, except for a simple pole at $s = 1$ with residue κ.

This is what is needed for the analytic class number formula. We skip the proof, since it needs estimates for the number of ideals in a given ideal class, see e.g. Lang.

More generally, let $\mathfrak{m}$ be a modulus of K and

$$\zeta_K(\mathfrak{m}, s) = \sum_{(\mathfrak{a}, \mathfrak{m}) = 1} \frac{1}{N(\mathfrak{a})^s},$$

then

$$\zeta_K(\mathfrak{m}, s) = \prod_{\mathfrak{p} \nmid \mathfrak{m}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}$$

and

$$\zeta_K(\mathfrak{m}, s) = \sum_{C \in I_K(\mathfrak{m})/P_K(\mathfrak{m})} \zeta(C, s)$$

is as before, but with C a class in $I_K(\mathfrak{m})/P_K(\mathfrak{m})$.

Proposition 2.41. Let $\mathfrak{m}$ be a modulus of K, C a class in $I_K(\mathfrak{m})/P_K(\mathfrak{m})$. Then $\zeta(C, s)$ is analytic for $\mathrm{Re}(s) > 1 - \frac{1}{n}$. except for a simple pole at $s = 1$ with residue $\rho_{\mathfrak{m}}$ depending only on $\mathfrak{m}$ and not on C.

Consequently, $\zeta_K(\mathfrak{m}, s)$ is analytic for $\mathrm{Re}(s) > 1 - \frac{1}{n}$, except for a simple pole at $s = 1$ with residue $\rho_{\mathfrak{m}} h_{\mathfrak{m}}(K)$.

Note the product for $\zeta_K(\mathfrak{m}, s)$ differs from $\zeta_K(s)$ by the factors corresponding to $p \mid \mathfrak{m}$, so only at finitely many primes. This finite product does not affect the singularity at $s = 1$, so

$$\log \zeta_K(s) \sim \log \zeta_K(\mathfrak{m}, s).$$

Definition 2.42. We define a **generalized Dirichlet character** (also known as a **Weber character**) af modulus $\mathfrak{m}$ to be a group homomorphism

$$\chi : I_K(\mathfrak{m})/P_K(\mathfrak{m}) \to \mathbb{C}^\times.$$

The corresponding L-series $L_\mathfrak{m}(\chi, s)$ is

$$L_\mathfrak{m}(\chi, s) = \sum_{\mathfrak{a}\subset\mathcal{O}_K,(\mathfrak{a},\mathfrak{m})=1} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s}$$

are called **Weber L-functions**. We can write

$$L_\mathfrak{m}(\chi, s) = \sum_{C\in I_K(\mathfrak{m})/P_K(\mathfrak{m})} \chi(C)\zeta(C, s).$$

Proposition 2.43. The Dirichlet series $L_\mathfrak{m}(\chi, s)$ is analytic for $\mathrm{Re}(s) > 1 - \frac{1}{n}$. If $\chi \neq \chi_0$, then

$$L_\mathfrak{m}(\chi, s) = \prod_{\mathfrak{p}\nmid m} \left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^{-1}.$$

Proof. Lang. □

Note $L_\mathfrak{m}(\chi_0, s) = \prod_{\mathfrak{p}\nmid\mathfrak{m}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = \zeta_K(\mathfrak{m}, s)$, so by Proposition 2.41, this is analytic for $\mathrm{Re}(s) > 1 - \frac{1}{n}$, except for a simple pole at $s = 1$.

Let L/K be Galois. Recall that we had the norm for the Takagi group $T_{L/K}(\mathfrak{m}) = P_K(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))$, which will be the kernel of $\Phi_\mathfrak{m}$ for suitable $\mathfrak{m}$. We call $[I_K(\mathfrak{m}) : T_{L/K}(\mathfrak{m})]$ the **norm index**.

Theorem 2.44 (Universal Norm Index Inequality)**.** Let L/K be Galois and let $\mathfrak{m}$ be divisible by all primes of K that ramify in L. Then

$$[I_K(\mathfrak{m}) : T_{L/K}(\mathfrak{m})] \leq [L : K].$$

Proof. Let $\chi \neq \chi_0$ be a character of $I_K(\mathfrak{m})/T_{L/K}(\mathfrak{m})$. We can also view this as a character of $I_K(\mathfrak{m})/P_K(\mathfrak{m})$. Let $m(\chi)$ be the order of the zero at $s = 1$ of $L_\mathfrak{m}(\chi, s)$. By Proposition 2.43, $m(\chi) \geq 0$ (as the series is analytic). Write

$$L_\mathfrak{m}(\chi, s) = (s - 1)^{m(\chi)} g(\chi, s),$$

so

$$\log L_\mathfrak{m}(\chi, s) \sim m(\chi)\log(s - 1) = -m(\chi)\log\frac{1}{s - 1}.$$

Let $\mathrm{Re}(s) > 1$ and let χ be any character of $I_K(\mathfrak{m})/T_{L/K}(\mathfrak{m})$. By the Euler

product,

$$\log L_{\mathfrak{m}}(\chi, s) = \sum_{\mathfrak{p}\nmid\mathfrak{m}} \sum_{n\geq 1} \frac{\chi(\mathfrak{p})^n}{nN(\mathfrak{p})^{ns}} = \sum_{\mathfrak{p}\nmid\mathfrak{m}} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s} + \sum_{\mathfrak{p}\nmid\mathfrak{m}} \sum_{n\geq 2} \frac{\chi(\mathfrak{p})}{nN(\mathfrak{p})^{ns}} \sim \sum_{\mathfrak{p}\nmid\mathfrak{m}} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}.$$

Write $h = [I_K(\mathfrak{m}) : T_{L/K}(\mathfrak{m})]$. Since χ is trivial on $T_{L/K}(\mathfrak{m})$, we get

$$\sum_{\chi} \chi(\mathfrak{p}) = \begin{cases} h & \mathfrak{p} \in T_{L/K}(\mathfrak{m}) \\ 0 & \mathfrak{p} \notin T_{L/K}(\mathfrak{m}) \end{cases}$$

by the orthogonality relation. Let $s \to 1$ from above, and take the sum over all characters to get

$$\sum_{\chi} \log L_{\mathfrak{m}}(\chi, s) \sim h \sum_{\mathfrak{p}\in T_{L/K}(\mathfrak{m})} \frac{1}{N(\mathfrak{p})^s}.$$

If $\chi = \chi_0$, we get $L_{\mathfrak{m}}(\chi, s) = \zeta_K(\mathfrak{m}, s)$, so $\log L(\chi, s) \sim \log \zeta_K(s) \sim \log \frac{1}{s-1}$ as $s \to 1$. Thus

Feb 19 2024, Lecture 14

$$\begin{aligned} \sum_{\chi} \log L_{\mathfrak{m}}(\chi, s) &\sim \log \zeta_K(s) + \sum_{\chi\neq\chi_0} \log L_{\mathfrak{m}}(\chi, s) \\ &\sim \log \frac{1}{s-1} - \sum_{\chi\neq 1} m(\chi) \log\left(\frac{1}{s-1}\right) = \left(1 - \sum_{\chi\neq 1} m(\chi)\right) \log \frac{1}{s-1}. \end{aligned}$$

If $\mathfrak{p}$ splits completely in L, then $\mathcal{P} \in \mathcal{O}_L$ with $\mathcal{P} \mid \mathfrak{p}$, then $f_{\mathcal{P}|\mathfrak{p}} = 1$, so $N_{L/K}(\mathcal{P}) = \mathfrak{p}$. So then (if $\mathfrak{p} \nmid \mathfrak{m}$), then $\mathfrak{p} \in T_{L/K}(\mathfrak{m}) = P_K(\mathfrak{m})N_{L/K}(I_L(\mathfrak{m}))$. Then there are $[L : K]$ primes of L above $\mathfrak{p}$, so

$$h \sum_{\mathfrak{p}\in T_{L/K}(\mathfrak{m})} \frac{1}{N(\mathfrak{p})^s} = h \left(\sum_{\substack{\mathfrak{p}\in T_{L/K}(\mathfrak{m}) \\ \text{splits completely}}} N(\mathfrak{p})^{-s} + \sum_{\substack{\mathfrak{p}\in T_{L/K}(\mathfrak{m}) \\ f_{\mathcal{P}|\mathfrak{p}}>1}} N(\mathfrak{p})^{-s} \right)$$

since $\mathfrak{m}$ is divisible by all ramified primes. The second series does not contribute to the singularity, as $N(\mathfrak{p}) \geq p^2$.

If $\mathcal{P} \subset \mathcal{O}_L$ is a degree one prime and if for $\mathfrak{p} \subset \mathcal{O}_K$ we have $\mathcal{P} \mid \mathfrak{p}$, then $f_{\mathcal{P}|\mathfrak{p}} = 1$. If $\mathfrak{p}$ is unramified in L, then $\mathfrak{p}$ splits completely with $[L : K]$ primes above it.

Write $\gtrsim$ to mean that the RHS is less than or equal to the LHS plus some

constant in a neighborhood of $s = 1$. We get

$$h \sum_{\mathfrak{p} \in T_{L/K}(\mathfrak{m})} \frac{1}{N(\mathfrak{p})^s} \gtrsim h \sum_{\mathfrak{p} \text{ splits comp.}} \frac{1}{N(\mathfrak{p})^s} \gtrsim \frac{h}{[L:K]} \sum_{\deg(\mathcal{P})=1} \frac{1}{N(\mathcal{P})^s} \gtrsim \frac{h}{[L:K]} \log \frac{1}{s-1}.$$

Hence

$$\left(1 - \sum_{\chi \neq 1} m(\chi)\right) \log \frac{1}{s-1} \gtrsim \frac{h}{[L:K]} \log \frac{1}{s-1},$$

which means that $m(\chi) = 0 \ \forall \chi \neq 1$ and $h \leq [L:K]$. □

The fact that $L_{\mathfrak{m}}(\chi, s) \neq 0$ for $\chi \neq \chi_0$ is important for the generalization of the Prime Number Theorem.

3 Density results

3.1 Dirichlet density

To motivate the definition, reconsider the proof of Dirichlet's Prime Number Theorem. For some m with $(a, m) = 1$, we had

$$\sum_{\chi \in \widehat{(\mathbb{Z}/m\mathbb{Z})^\times}} \chi(a)^{-1} \log L(\chi, s) = \phi(m) \sum_{p \equiv a \bmod m} p^{-s} + \left(\text{abs. conv. part for } \operatorname{Re}(s) > \frac{1}{2}\right),$$

so

$$\sum_{\chi} \chi(a)^{-1} \log L(\chi, s) \sim \phi(m) \sum_{p \equiv a \bmod m} \frac{1}{p^s} \sim \log L(\chi_0, s) \sim \log \zeta(s)$$

as $L(\chi, s) = \prod_{p|m}(1 - p^{-s})\zeta(s)$, so

$$\sum_{p \equiv a \bmod m} \frac{1}{p^s} \sim \phi(m) \log \zeta(s).$$

Let $s \to 1^+$, which diverges, which finished the proof, and

$$\lim_{s \to 1^+} \frac{\sum_{p \equiv a \bmod m} p^{-s}}{\log \frac{1}{s-1}} = \frac{1}{\phi(m)}.$$

Why did we just do this? Let S be any set of primes. If

$$\lim_{s\to 1^+} \frac{\sum_{p\in S} p^{-s}}{\log \frac{1}{s-1}}$$

exists, then we say this set S has Dirichlet density $\delta = \delta(S)$. If S is finite, we say $\delta(S) = 0$. So we can "rephrase" Dirichlet's Prime Number Theorem by saying

$$\delta(S) = \frac{1}{\phi(m)},$$

where $S = \{p \in \mathbb{Z} \mid p \text{ prime}, p \equiv a \pmod{m}\}$.

Proposition 3.1. Let $K/\mathbb{Q}$ be Galois. Let

$$\mathcal{S}_K = \{p \in \mathbb{Z} \mid p \text{ prime}, p \text{ splits completely in } K/\mathbb{Q}\}.$$

Then $\delta(\mathcal{S}_K) = \frac{1}{[K:\mathbb{Q}]}$.

Proof. We have seen

$$\log \zeta_K(s) \sim \log\left(\frac{1}{s-1}\right) \sim \sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}$$

$$\sim \sum_{\substack{\mathfrak{p} \\ f_{\mathcal{P}|\mathfrak{p}}=1=e_{\mathcal{P}|\mathfrak{p}}}} p^{-s} + \sum_{\substack{\mathfrak{p} \\ f_{\mathcal{P}|\mathfrak{p}}>1}} p^{-f_{\mathcal{P}|\mathfrak{p}}s} + \sum_{\substack{\mathfrak{p} \\ f_{\mathcal{P}|\mathfrak{p}}>1 \\ e_{\mathcal{P}|\mathfrak{p}}>1}} p^{-s}$$

$$\sim \sum_{p\in\mathcal{S}_K} [K:\mathbb{Q}] p^{-s}.$$

So

$$\log\left(\frac{1}{s-1}\right) = [K:\mathbb{Q}] \sum_{p\in\mathcal{S}_K} p^{-s} + g(s)$$

for $g(s)$ bounded as $s \to 1^+$, so

$$\delta(\mathcal{S}_K) = \lim_{s\to 1^+} \frac{\sum_{p\in\mathcal{S}_K} p^{-s}}{\log\left(\frac{1}{s-1}\right)} = \lim_{s\to 1^+} \left(\frac{[K:\mathbb{Q}]\sum_{p\in\mathcal{S}_K} p^{-s} + g(s)}{\sum_{p\in\mathcal{S}_K} p^{-s}}\right)^{-1} = \frac{1}{[K:\mathbb{Q}]}.$$

□

Definition 3.2. Let K be a number field. Let S be a set of prime ideals in

$\mathcal{O}_K$. If the limit

$$\lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in S} N(\mathfrak{p})^{-s}}{\log\left(\frac{1}{s-1}\right)}$$

exists, then we say this set S has **Dirichlet density** $\delta = \delta(S)$.

Note that since $\log\left(\frac{1}{s-1}\right) \sim \sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s}$, we can also write

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

Lemma 3.3. Let $\mathcal{P}_K$ be the set of all prime ideals of K. Let S, T be subsets of $\mathcal{P}_K$. Then

(i) $\delta(\mathcal{P}_K) = 1$.

(ii) If $S \subset T$ and $\delta(S), \delta(T)$ exist, then $\delta(S) \leq \delta(T)$.

(iii) If $\delta(S)$ exists, then $0 \leq \delta(S) \leq 1$.

(iv) If S and T are disjoint and $\delta(S), \delta(T)$ exist, then $\delta(S \cup T) = \delta(S) + \delta(T)$.

(v) If S is finite, then $\delta(S) = 0$.

(vi) If $\delta(S)$ exists and T differs from S by only finitely many elements, then $\delta(T) = \delta(S)$.

Proof. Exercises. Note that it might be simpler to prove this in some order different than the one listed above. □

Lemma 3.4. Let L/K be Galois and let

$$\mathcal{S}_{L/K} = \{\mathfrak{p} \in \mathcal{O}_K \mid \mathfrak{p} \text{ splits completely in } L\}.$$

Then $\delta(\mathcal{S}_{L/K}) = \frac{1}{[L:K]}$.

Proof. Left as an exericse. □

Lemma 3.5. Let $\mathcal{S}_1$ be the set of prime ideals of degree one. Then $\delta(\mathcal{S}_1) = 1$, and if $\mathcal{S}$ is a set of prime ideals of K and $\delta(\mathcal{S})$ exists, then $\delta(\mathcal{S}) = \delta(\mathcal{S} \cup \mathcal{S}_1)$.

Proof. Similarly to before we write

$$\log P_K(\mathcal{S}) = \sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s} = \sum_{\mathfrak{p}\in\mathcal{S}_1} \frac{1}{N(\mathfrak{p})^s} + \sum_{\mathfrak{p}\notin\mathcal{S}_1} \frac{1}{N(\mathfrak{p})^s} \sim \sum_{\mathfrak{p}\in\mathcal{S}_1} \frac{1}{N(\mathfrak{p})^s},$$

since $N(\mathfrak{p}) = p^f = p^2$ for all $\mathfrak{p} \notin \mathcal{S}_1$. Hence from the definition we get $\delta(\mathcal{S}_1) = 1$, and $\sum_{\substack{\mathfrak{p}\in\mathcal{S}\\ \mathfrak{p}\notin\mathcal{S}_1}} N(\mathfrak{p})^{-s} = 0$, so

$$\sum_{\mathfrak{p}\in\mathcal{S}} N(\mathfrak{p})^{-s} \sim \sum_{\mathfrak{p}\in\mathcal{S}\cup\mathcal{S}_1} N(\mathfrak{p})^{-s}. \qquad \square$$

21 Feb 2024, Lecture 15

By the Existence Theorem (Theorem 1.26), for a number field K and a modulus $\mathfrak{m}$ of K, and any congruence subgroup $P_K(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m})$, we can find an abelian extension L/K such that $H = T_{L/K}(\mathfrak{m})$. In particular, we can find this for $P_K(\mathfrak{m})$. Hence we obtain

Theorem 3.6. Let $\mathfrak{m}$ be a modulus of K and χ a nontrivial character of $I_K(\mathfrak{m})/P_K(\mathfrak{m})$. Then $L(\chi, 1) \neq 0$.

Corollary 3.7 (Generalized version of Dirichlet's Prime Number Theorem)**.** Let $h_K(\mathfrak{m}) = |I_K(\mathfrak{m})/P_K(\mathfrak{m})|$ and let C_0 be an ideal class in $I_K(\mathfrak{m})/P_K(\mathfrak{m})$. Let S be the set of prime ideals in C_0, then

$$\delta(S) = \frac{1}{h_K(\mathfrak{m})}.$$

Proof. For $\mathrm{Re}(s) > 1$, we have

$$\begin{aligned}\log L_{\mathfrak{m}}(\chi, s) &\sim \sum_{\mathfrak{p}\nmid\mathfrak{m}} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s} \\ &\sim \sum_{C\in I_K(\mathfrak{m})/P_K(\mathfrak{m})} \chi(C) \sum_{\mathfrak{p}\in C} \frac{1}{N(\mathfrak{p})^s}.\end{aligned}$$

Multiply this by $\chi(C_0^{-1})$ and sum over all χ to get

$$\log \zeta_K(s) \sim \sum_C \sum_\chi \chi(CC_0^{-1}) \sum_{\mathfrak{p}\in C} \frac{1}{N(\mathfrak{p})^s}.$$

By the orthogonality relation, the sum over χ is zero unless $CC_0^{-1} = 1$, hence

$$\log \frac{1}{s-1} \sim h_K(\mathfrak{m}) \sum_{\mathfrak{p}\in C_0} \frac{1}{N(\mathfrak{p})^s}. \qquad \square$$

Hence any ideal class contains infinitely many prime ideals, and they are equidistributed.

3.2 Frobenius density theorems

Let $K \subset E \subset L$ with L/K Galois but E/K not necessarily Galois. Let $G = \mathrm{Gal}(L/K)$ and let H be the elements of G fixing E elementwise. Consider a coset decomposition $G = H_{\sigma_1} \cup \ldots \cup H_{\sigma_k}$. Any $\sigma \in G$ permutes these cosets by right multiplication $H_{\sigma_i} \mapsto H_{\sigma_i \sigma}$. A sequence

$$H_{\sigma_i}, H_{\sigma_i \sigma}, H_{\sigma_i \sigma^2}, \ldots, H_{\sigma_i \sigma^{t-1}}$$

is a cycle of length t, if these are t distinct cosets and $H_{\sigma_i} = H_{\sigma_i \sigma^t}$. The collection of all cosets of H is partitioned into disjoint cycles of σ.

Proposition 3.8. Let $K \subset E \subset L$ with L/K Galois. Let $\mathcal{P} \subset \mathcal{O}_L, \mathfrak{p} = \mathcal{P} \cap \mathcal{O}_K$ for $\mathfrak{p}$ unramified in L. Let $\sigma = \left(\frac{L/K}{\mathfrak{P}}\right)$. Suppose σ has cycles of length $t_1, \ldots, t_s$ (when acting on the cosets of $H = \mathrm{Gal}(L/E)$). Then $\mathfrak{p}\mathcal{O}_E$ factors as a product of s distinct prime ideals of E, with degrees $t_1, \ldots, t_s$. As a consequence, the number of prime ideals in E dividing $\mathfrak{p}$ equals the number of cosets H_{σ_i} for which $\sigma_i D_{\mathcal{P}|\mathfrak{p}} \sigma_i^{-1} \subset H$.

Proof. Can be found in Janusz, chapter 3. □

Definition 3.9. Let L/K be Galois, $G = \mathrm{Gal}(L/K)$ and let $\sigma \in G$ be an element of order n. Then the **division** of σ is the set of all elements of G which are conjugate to some σ^m for some m relatively prime to n.

Lemma 3.10. Let $\sigma \in G$, $H = \langle \sigma \rangle$ and let t be the number of elements in the division of σ. Then

$$t = \phi(n)[G : N_G(H)],$$

where ϕ is the Euler totient function and $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ is the normalizer of H in G.

Proof. Exercise. Use the fact that for any $g \in G$, the number of elements in its conjugacy class is $[G : C_G(g)]$, where $C_G(g) = \{a \in G \mid ag = ga\}$ is the centralizer of g in G. □

Theorem 3.11 (Frobenius Density Theorem)**.** Let L/K be Galois and let $\sigma \in G = \mathrm{Gal}(L/K)$. Suppose σ has t elements in its division. Let S be the set of prime ideals $\mathfrak{p}$ of K such that there is $\mathcal{P} \subset \mathcal{O}_L$ with $\mathcal{P} \mid \mathfrak{p}$ with $\left(\frac{L/K}{\mathcal{P}}\right)$ in the division of σ, i.e.

$$S = \{\mathfrak{p} \in P_K \mid \exists \mathcal{P} \in \mathcal{P}_L \text{ with } \mathcal{P} \mid \mathfrak{p} \text{ and } \left(\frac{L/K}{\mathcal{P}}\right) \text{ conjugate to } \sigma^m \text{ with } m \text{ coprime to the order of } \sigma\}.$$

Then $\delta(S) = \frac{t}{|G|}$.

Proof. Induct on n, the order of σ. If $n = 1$, so $\sigma = 1$, then $S = S_{L/K}$ and the result follows from Lemma 3.4. Assume now that σ has order $n > 1$. Let t_d be the number of elements in the division of σ^d for $d \mid n$. Let S_d be the set of primes divisible by some prime of L whose Artin symbol belongs to the division of σ^d. Note that $S_1 = S$. By induction, we have $\delta(S_d) = \frac{t_d}{|G|}$ for $d \neq 1$. Let $H = \langle\sigma\rangle$ and let $E = L^H = \{x \in L \mid \sigma(x) = x \ \forall \sigma \in H\}$.

By Proposition 3.8, a prime $\mathfrak{p} \subset \mathcal{O}_K$ is divisible by at least one prime of E having relative degree one if $\mathfrak{p}$ is divisible by a prime $\mathcal{P} \subset \mathcal{O}_L$ such that $\left(\frac{L/K}{\mathcal{P}}\right)$ has a cycle of length one (when acting as permutations on the cosets H_γ of H in G). This occurs precisely when $\gamma\left(\frac{L/K}{\mathcal{P}}\right)\gamma^{-1} \in H$, which means that $\mathfrak{p} \in S_d$ for some d.

Let S_E be the primes of E with degree one over K. For each prime $\mathfrak{p} \in S_E$, let $n(\mathfrak{p})$ be the number of primes in S_E dividing $\mathfrak{p}$. Then $\mathfrak{p} \in S_d$ is the norm of exactly $n(\mathfrak{p})$ primes in S_E. Since S_E contains all the primes of E with degree one over $\mathbb{Q}$, we get $\delta(S_E) = 1$. Then

$$-\log(s-1) \sim \sum_{\mathfrak{p}_E \in S_E} \frac{1}{N_{K/\mathbb{Q}}(N_{E/K}(\mathfrak{p}_E))^s} \sim \sum_{d|n} \sum_{\mathfrak{p} \in S_d} \frac{n(\mathfrak{p})^s}{N(\mathfrak{p})^s}. \quad (\dagger)$$

By Proposition 3.8, for $\mathfrak{p} \in S_d$, $n(\mathfrak{p})$ is the number of distinct cosets $H\gamma$ such that $H\gamma\sigma^d = H\gamma$, or equivalently $\gamma\sigma^d\gamma^{-1} \in H$. But H is cyclic, so this can only happen if $\gamma\sigma^d\sigma^{-1} \in \langle\sigma^d\rangle$, so $\gamma \in N_G(\langle\sigma^d\rangle)$. Putting this all together, $n(\mathfrak{p}) = [N_G(\langle\sigma^d\rangle) : H]$ for $\mathfrak{p} \in S_d$.

Using (†) above and induction hypothesis for the sum over S_d for $d \neq 1$, we find

$$[N_G(H) : H] \sum_{\mathfrak{p} \in S_1} N(\mathfrak{p})^{-s} \sim \left(-1 + \sum_{d|n, d\neq 1} \frac{[N_G(\langle\sigma^d\rangle) : H]t_d}{|G|}\right) \log(s-1).$$

By Lemma 3.10, we have $t_d = \phi\left(\frac{n}{d}\right)[G : N_G(\langle\sigma^d\rangle)]$, so the expression in the brackets above is

23 Feb 2024, Lecture 16

$$\begin{aligned} &-1 + \sum_{d|n, d\neq 1} \phi\left(\frac{n}{d}\right) \frac{[G : N_G(\langle\sigma^d\rangle)][N_G(\langle\sigma^d\rangle) : H]}{|G|} \\ =&-1 + \sum_{d|n, d\neq 1} \phi\left(\frac{n}{d}\right) \frac{[G : H]}{|G|} \\ =&-1 + \sum_{d|n, d\neq 1} \frac{1}{n}\phi\left(\frac{n}{d}\right) = -1 - \frac{\phi(n)}{n} + \frac{1}{n}\sum_{d|n} \phi\left(\frac{n}{d}\right). \end{aligned}$$

We have $\sum_{d|n} \phi\left(\frac{n}{d}\right) = n$, so

$$\sum_{\mathfrak{p}\in S} \frac{1}{N(\mathfrak{p})^s} \sim \frac{-\phi(n)}{[N_G(H):H]} \log(s-1) = \frac{-t}{|G|} \log(s-1)$$

by Lemma 3.10. □

We are now in a position to prove the surjectivity of the Artin map.

Theorem 3.12 (Surjectivity of the Artin map)**.** Let L/K be abelian and let $\mathfrak{m}$ be a modulus divisible by all ramified prime ideals. Then the Artin map $\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$ is surjective.

Proof. Let $\sigma \in \mathrm{Gal}(L/K)$. Since this is abelian, the division of σ consists of elements which are all generators of the cyclic group $\langle\sigma\rangle$. By the Frobenius density theorem, there exist infinitely many prime ideals $\mathcal{P}$ of L whose Artin symbol $\left(\frac{L/K}{\mathcal{P}}\right)$ generates $\langle\sigma\rangle$.

Since only finitely many primes divide $\mathfrak{m}$, we can pick $\mathcal{P}$ with $\mathfrak{p} = \mathcal{P} \cap \mathcal{O}_K$ coprime to $\mathfrak{m}$. Then $\Phi_{\mathfrak{m}}(\mathfrak{p}) = \sigma'$, where σ' is some generator of $\langle\sigma\rangle$. Hence σ is in the image of $\Phi_{\mathfrak{m}}$. □

3.3 Chebotarov's density theorem

Theorem 3.13 (Chebotarov's density theorem)**.** Let L/K be Galois and let $\sigma \in \mathrm{Gal}(L/K)$. Suppose σ has c conjugates in $\mathrm{Gal}(L/K)$. Let

$$S = \{\mathfrak{p} \subset \mathcal{O}_K \mid \left(\frac{L/K}{\mathcal{P}}\right) = \sigma \text{ for some } \mathcal{P} \mid \mathfrak{p}\}.$$

Then this set S has density

$$\delta(S) = \frac{c}{|\mathrm{Gal}(L/K)|}.$$

Note that the original proof of this does not use class field theory, but most proofs in modern textbooks do.

Notation. If L/K is not abelian, we can still write $\left(\frac{L/K}{\mathfrak{p}}\right)$ which refers to the conjugacy class of $\left(\frac{L/K}{\mathcal{P}}\right)$ for any $\mathcal{P} \mid \mathfrak{p}$.

Corollary 3.14. Let L/K be abelian, $\mathfrak{m}$ a modulus divisible by all primes that ramify in L, and $\sigma \in \mathrm{Gal}(L/K)$. If

$$S = \left\{\mathfrak{p} \subset \mathcal{O}_K \mid \mathfrak{p} \nmid \mathfrak{m}, \left(\frac{L/K}{\mathcal{P}}\right) = \sigma\right\},$$

then $\delta(S) = \frac{1}{[L:K]}$.

Chebotarov gives an alternative proof for Lemma 3.4.

Alternate proof of Lemma 3.4. Let $\sigma = 1$. Then the set of primes with $\left(\frac{L/K}{\mathcal{P}}\right)$ has density $\frac{1}{[L:K]}$. But $\left(\frac{L/K}{\mathcal{P}}\right)$ if and only if $\mathfrak{p}$ splits completely. □

We next show that the primes that split completely characterize the extension L/K.

Notation. Given two sets S, T, we say $S \dot{\subset} T$ if $S \subset T \cup \Sigma$ for some finite set Σ. Write $S \doteq T$ if $S \dot{\subset} T$ and $T \dot{\subset} S$.

Theorem 3.15. Let L and M be Galois extensions of K. Then

(i) $L \subset M$ if and only if $S_{M/K} \dot{\subset} S_{L/K}$.

(ii) $L = M$ if and only if $S_{M/K} \doteq S_{L/K}$.

Proposition 3.16. Let L and M be finite extensions of K.

(i) If M/K is Galois, then $L \subset M \iff S_{M/K} \dot{\subset} S_{L/K}$.

(ii) If L/K is Galois, then $L \subset M \iff \widetilde{S}_{M/K} \dot{\subset} S_{L/K}$, where

$$\widetilde{S}_{M/K} = \{\mathfrak{p} \subset \mathcal{O}_K \mid \mathfrak{p} \text{ unramified in } M, f_{\mathcal{P}|\mathfrak{p}} = 1 \text{ for some } \mathcal{P} \subset \mathcal{O}_M \text{ with } \mathcal{P} \mid \mathfrak{p}\}.$$

Lemma 3.17. Let L/K is a finite extension with Galois closure M/K. Then

$$\delta(S_{L/K}) = \delta(S_{M/K}) = \frac{1}{[L:K]}.$$

Proof. Note that a prime $\mathfrak{p}$ of K splits completely in L if and only if it splits completely in all of the conjugates of L in M, i.e. $\sigma(L)$ for $\sigma \in \mathrm{Gal}(M/K)$. But the Galois closure M is the compositum of the conjugates of L. Hence $\mathfrak{p}$ splits completely in L if and only if it does so in M. □

Proof of Proposition 3.16. We first prove (ii). The direction $\implies$, i.e. if $L \subset M$, then $\widetilde{S}_{M/K} \dot{\subset} S_{L/K}$, is left as an exercise.

Now assume $\widetilde{S}_{M/K} \dot{\subset} S_{L/K}$. Let N be a Galois extension of K containing both L and M. To prove $L \subset M$, by Galois theory it suffices to show that $\mathrm{Gal}(N/M) \subset \mathrm{Gal}(N/L)$. In other words, for any $\sigma \in \mathrm{Gal}(N/M)$, we need to show $\sigma|_L = 1$. By Chebotarov, we can find a prime $\mathfrak{p} \subset \mathcal{O}_K$ unramified in N such that $\left(\frac{N/K}{\mathfrak{p}}\right)$ is the conjugacy class of σ. In particular, there is $\mathcal{P} \subset \mathcal{O}_N$

such that $\mathcal{P} \mid \mathfrak{p}$ and $\left(\frac{N/K}{\mathcal{P}}\right) = \sigma$. We show $\mathfrak{p} \in \widetilde{S}_{M/K}$. Let $\mathcal{P}_M = \mathcal{P}\mathbb{N}\mathcal{O}_M$. Then for $\alpha \in \mathcal{O}_M$ we have

$$\alpha \equiv \sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathcal{P}_M},$$

where the left equality uses $\sigma|_M = 1$ and the right uses the definition of the Artin symbol. It follows that $\mathcal{O}_M/\mathcal{P}_M \cong \mathcal{O}_K/\mathcal{P}$, so $f_{\mathcal{P}_M|\mathfrak{p}} = 1$ and hence $\mathfrak{p} \in \widetilde{S}_{M/K}$. By Chebotarov, we can find infinitely many such $\mathfrak{p}$, so we can assume $\mathfrak{p} \in S_{L/K}$. Since we assumed $\widetilde{S}_{M/K} \mathrel{\dot\subset} S_{L/K}$, we have $\left(\frac{L/K}{\mathfrak{p}}\right) = 1$. We also have $\left(\frac{L/K}{\mathfrak{p}}\right) = \left(\frac{N/K}{\mathcal{P}}\right)|_L$ and since $\sigma = \left(\frac{L/K}{\mathcal{P}}\right)$, this implies $\sigma|_L = 1$.

For the first part, direction $\Longleftarrow$, suppose $S_{M/K} \mathrel{\dot\subset} S_{L/K}$. By the proof of the previous lemma (Lemma 3.17), we have $S_{L/K} = S_{L'/K}$ for L' the Galois closure of L over K. Since M/K is Galois, we have $\widetilde{S}_{M/K} = S_{M/K}$ (exercise!). Hence $S_{M/K} \mathrel{\dot\subset} S_{L/K} \implies \widetilde{S}_{M/K} \mathrel{\dot\subset} S_{L'/K}$, but by the second part of this proposition we have $L' \subset M$, $L \subset M$.

The direction $\Longrightarrow$ is left as an exercise. □