Algebraic Number Theory *

Zhiyuan Bai

Compiled on March 15, 2023

This document serves as a set of revision materials for the Cambridge Mathematical Tripos Part III course *Algebraic Number Theory* in Lent 2023. However, despite its primary focus, readers should note that it is NOT a verbatim recall of the lectures, since the author might have made further amendments in the content. Therefore, there should always be provisions for errors and typos while this material is being used.

Contents

*Based on the lectures under the same name taught by Dr. H. Wiersema in Lent 2023.

1 Statements of Class Field Theory

1.1 Flashbacks to Number Fields

For a number field K, we write $\mathcal{O}_K$ for its ring of integers. Let L/K be a finite extension of number fields.
Take any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, then $\mathfrak{p}\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$, therefore factorises $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ for distinct primes $\mathfrak{P}_i$ of $\mathcal{O}_L$. We say a prime $\mathfrak{P}$ of $\mathcal{O}_L$ lies above $\mathfrak{p}$ if $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$. Equivalently, $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ (which in this case happens iff $\mathfrak{p} \subset \mathfrak{P}$).

Definition 1.1. $e_i = e_{\mathfrak{P}_i|\mathfrak{p}}$ is called the ramification index of $\mathfrak{P}_i$ over $\mathfrak{p}$. We say $\mathfrak{p}$ ramifies if some $e_{\mathfrak{P}|\mathfrak{p}}$ is strictly greater than 1.

For any prime $\mathfrak{P} \leq \mathcal{O}_L$, we write $k_{\mathfrak{P}} = \mathcal{O}_L/\mathfrak{P}$ to denote its residue field. If $\mathfrak{P}$ lies above $\mathfrak{p}$, we obtain an extension of residue fields $k_{\mathfrak{P}}/k_{\mathfrak{p}}$.

Definition 1.2. The degree $f_{\mathfrak{P}|\mathfrak{p}} = [k_{\mathfrak{P}} : k_{\mathfrak{p}}]$ is called the inertial degree of $\mathfrak{P}$ over $\mathfrak{p}$.

Theorem 1.1. *If $\mathfrak{p} \leq \mathcal{O}_K$ is a prime with the factorisation $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, then*

$$[L : K] = \sum_{i=1}^{g} e_{\mathfrak{P}_i|\mathfrak{p}} f_{\mathfrak{P}_i|\mathfrak{p}}$$

In the case where L/K is Galois, things are a lot nicer.

Theorem 1.2. *Suppose in addition that L/K is Galois, then:*
(i) $\mathrm{Gal}(L/K)$ acts transitively on primes of $\mathcal{O}_L$ lying above $\mathfrak{p}$, i.e. suppose $\mathfrak{P}, \mathfrak{P}'$ both lie above $\mathfrak{p}$, then there is some $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma\mathfrak{P} = \mathfrak{P}'$.
(ii) All primes above $\mathfrak{p}$ have the same ramification index and inertial degree. In particular, $[L : K] = efg$, where e is the common ramification index and f the common inertial degree.

Definition 1.3. Suppose $\mathfrak{P}$ lies above $\mathfrak{p}$. The decomposition group of $\mathfrak{P}$ over $\mathfrak{p}$ is $D_{\mathfrak{P}|\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma\mathfrak{P} = \mathfrak{P}\}$. The inertial group of $\mathfrak{P}$ over $\mathfrak{p}$ is $I_{\mathfrak{P}|\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(L/K) : \forall \alpha \in \mathcal{O}_L, \sigma\alpha \equiv \alpha \pmod{\mathfrak{P}}\}$.

Note that we have $I_{\mathfrak{P}|\mathfrak{p}} \subset D_{\mathfrak{P}|\mathfrak{p}}$.
The extension of residue fields $k_{\mathfrak{P}}/k_{\mathfrak{p}}$ is an extension of finite fields, therefore is Galois and its Galois group is cyclic with canonical generator given by the Frobenius. Each $\sigma \in D_{\mathfrak{P}|\mathfrak{p}}$ naturally descends to an element $\tilde{\sigma} \in \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$.

Proposition 1.3. *(i) $D_{\mathfrak{P}|\mathfrak{p}} \to \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}}), \sigma \mapsto \tilde{\sigma}$ is surjective with kernel $I_{\mathfrak{P}|\mathfrak{p}}$.*
(ii) $\#I_{\mathfrak{P}|\mathfrak{p}} = e_{\mathfrak{P}|\mathfrak{p}}, \#D_{\mathfrak{P}|\mathfrak{p}} = e_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}|\mathfrak{p}}$.

1.2 The Artin Symbol

Lemma 1.4. *Let L/K be Galois and $\mathfrak{p} \subset \mathcal{O}_K$ a prime unramified in $\mathcal{O}_L$. Suppose $\mathfrak{P} \leq \mathcal{O}_L$ lies above $\mathfrak{p}$, then there exists a unique element $\sigma \in \mathrm{Gal}(L/K)$ such that for all $\alpha \in \mathcal{O}_L$, we have $\sigma\alpha \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}}$ where $N(\mathfrak{p}) = \#k_{\mathfrak{p}}$.*

Proof. Note that such a σ must reside in $D_{\mathfrak{P}|\mathfrak{p}}$. Since $\mathfrak{p}$ is unramified, the map $\sigma \mapsto \tilde{\sigma}$ must be an isomorphism by the preceding proposition. So we are able, forced, to choose σ to be the automorphism corresponding to the Frobenius. □

Definition 1.4. Such a σ is known as the Artin symbol, denoted by $(L/K, \mathfrak{P})$.

Corollary 1.5. *Suppose we are in the setting of the preceding lemma, then:*
(i) For any $\sigma \in \mathrm{Gal}(L/K)$, we have $(L/K, \sigma\mathfrak{P}) = \sigma(L/K, \mathfrak{P})\sigma^{-1}$.
(ii) $(L/K, \mathfrak{P})$ has order $f_{\mathfrak{P}|\mathfrak{p}}$.
(iii) $\mathfrak{p}$ splits completely in L if and only if $(L/K, \mathfrak{P}) = 1$.

Proof. (i) Exercise.
(ii) This follows from the isomorphism $D_{\mathfrak{P}|\mathfrak{p}} \cong \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$.
(iii) $\mathfrak{p}$ splits completely in L iff $e = f = 1$. But $e = 1$ and (ii) tells us that $(L/K, \mathfrak{P}) = 1 \iff f = 1$. □

Definition 1.5. We say L/K is abelian if it is Galois with abelian Galois group.

If L/K is an abelian extension of number fields, then $(L/K, \mathfrak{P})$ depends only on the underlying prime $\mathfrak{p}$. This follows from part (i) of the preceding corollary. In this case, we write $(L/K, \mathfrak{p})$ to denote $(L/K, \mathfrak{P})$.

Example 1.1. Suppose $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{d})$ where $d \neq 0, 1$ is a square-free integer. Recall that L/K has discriminant $D = d$ or $4d$ (depending on the residue of d modulo 4). Recall also that $\mathfrak{p} = (p)$ ramifies in L iff $p \mid D$.
Identify $\mathrm{Gal}(L/K)$ with $\{\pm 1\}$. If (p) is unramified, then $(L/K, (p)) = (D/p)$, where $(-/-)$ is the Kronecker symbol.

1.3 The Artin Map

Recall the following:

Definition 1.6. A fractional ideal $\mathfrak{a}$ of K is an $\mathcal{O}_K$-submodule of K such that there is some nonzero $x \in \mathcal{O}_K$ such that $x\mathfrak{a} \leq \mathcal{O}_K$. Equivalently, it is somethihng of the form αI for some $\alpha \in K, I \leq \mathcal{O}_K$.

The set of fractional ideals form a group under ideal multiplication, which we'll denote by I_K. We write $P_K \leq I_K$ to be the subgroup of principal fractional ideals, i.e. something of the form $\alpha\mathcal{O}_K, \alpha \in K$. $\mathrm{Cl}(K) = I_K/P_K$ is the ideal class group of K.

Remark. For any $\mathfrak{a} \in I_K$, we have a unique prime factorisation $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ where $e_i \in \mathbb{Z}$ and $\mathfrak{p}_i$ are distinct primes of $\mathcal{O}_K$.

We will extend the Artin symbol to any fractional ideals using unique factorisation.

Definition 1.7. Suppose L/K is abelian and unramified, in the sense that every prime of $\mathcal{O}_K$ is unramified, then we define the Artin map to be the homomorphism $(L/K, -) : I_K \to \mathrm{Gal}(L/K)$ by setting $(L/K, \mathfrak{a}) = \prod_i (L/K, \mathfrak{p}_i)^{e_i}$ where $\mathfrak{a} = \prod_i \mathfrak{p}_i^{e_i}$.

If L/K is ramified, we can still define the Artin symbol for unramified primes, but not for all primes. So we need to do a little bit more work in order for it to work.

Definition 1.8. For a number field K, a modulus of K is a formal product $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}, n_{\mathfrak{p}} \geq 0$, where the product is taken over all primes $\mathfrak{p}$ of K (finite and infinite), such that:
1. $n_{\mathfrak{p}} = 0$ for all but finitely many $\mathfrak{p}$.
2. $n_{\mathfrak{p}} = 0$ if $\mathfrak{p}$ is a complex infinite prime.
3. $n_{\mathfrak{p}} \leq 1$ if $\mathfrak{p}$ is a real infinite prime.

When $n_{\mathfrak{p}} = 0$ for all $\mathfrak{p}$, we write $\mathfrak{m} = 1$.

Example 1.2. If K is a purely imaginary field (e.g. an imaginary quadratic field), then a modulus is just an ideal of $\mathcal{O}_K$.

Definition 1.9. Let $\mathfrak{m}$ be a modulus, then we define $I_K(\mathfrak{m})$ to be the group of all fractional ideals relatively prime to (the finite part of) $\mathfrak{m}$.

Example 1.3. 1. When $\mathfrak{m} = 1$, we have $I_K(\mathfrak{m}) = I_K$.
2. If $K = \mathbb{Q}$ and $\mathfrak{m} = (m)$ for some integer m, then $I_{\mathbb{Q}}(\mathfrak{m}) = \{(a/b)\mathbb{Z} : \gcd(a, m) = \gcd(b, m) = 1\}$.

Let L/K be abelian and suppose $\mathfrak{m}$ is a modulus of K which is divisible by all ramified primes of K, then for each prime $\mathfrak{p} \in I_K(\mathfrak{m})$, we can define the Artin symbol $(L/K, \mathfrak{p}) \in \mathrm{Gal}(L/K)$.

Definition 1.10. The Artin map for L/K and $\mathfrak{m}$ is the homomorphism $\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$ defined by extending the Artin symbol multiplicatively.

Example 1.4. Let m be a positive integer, ζ_m a primitive m-th root of unity. Let $K = \mathbb{Q}, L = \mathbb{Q}(\zeta_m)$. We know that $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ by identifying $\sigma \in \mathrm{Gal}(L/K)$ with $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ where $\sigma\zeta_m = \zeta_m^a$. Moreover, if a prime ramifies in L then it divides m.
Now consider the modulus $\mathfrak{m} = (m) \cdot \infty$. Then $\mathfrak{m}$ is divisible by all ramified primes, hence we can define $\Phi_{\mathfrak{m}} : I_{\mathbb{Q}}(\mathfrak{m}) \to \mathrm{Gal}(L/K)$. Let $(a/b)\mathbb{Z} \in I_{\mathbb{Q}}(\mathfrak{m})$, then indeed $\Phi_{\mathfrak{m}}((a/b)\mathbb{Z}) = [a][b]^{-1} \in (\mathbb{Z}/m\mathbb{Z})^\times$. In particular, the Artin map is surjective.

1.4 Generalised Ideal Class Group

Suppose $\mathfrak{m}$ is a modulus of a number field K.

Definition 1.11. Let $P_K(\mathfrak{m})$ be the subgroup of $I_K(\mathfrak{m})$ consisting of all principal fractional ideals (α) where $\alpha \in K$ is such that:
1. $v_{\mathfrak{p}}(\alpha - 1) \geq v_{\mathfrak{p}}(\mathfrak{m})$ for any finite $\mathfrak{p} \mid \mathfrak{m}$.
2. $\sigma\alpha > 0$ for every real infinite prime (given by the embedding σ) dividing $\mathfrak{m}$.

Example 1.5. 1. For $\mathfrak{m} = 1$, $P_K(\mathfrak{m}) = P_K$.
2. Let $K = \mathbb{Q}$, $\mathfrak{m} = (m)$. An ideal $\alpha\mathbb{Z}$ is generated by α or $-\alpha$. So if $(\alpha) \in P_{\mathbb{Q}}(\mathfrak{m})$ then we must have either $v_p(\alpha - 1) \geq v_p(m)$ for all $p \mid m$ or $v_p(-\alpha - 1) \geq v_p(m)$ for all $p \mid m$. This means that $P_Q(\mathfrak{m}) = \{(a/b)\mathbb{Z} \in I_{\mathbb{Q}}(\mathfrak{m}) : a \equiv b \pmod{m}\}$.
3. Again take $K = \mathbb{Q}$ but now consider the modulus $\mathfrak{m}' = (m) \cdot \infty$ just to torture you. So now $P_{\mathbb{Q}}(\mathfrak{m}') = \{(a/b)\mathbb{Z} \in I_{\mathbb{Q}}(\mathfrak{m}) : a \equiv b \pmod{m}, a/b > 0\}$.

Remark. 1. For $K = \mathbb{Q}$, $\ker \Phi_{(m)\cdot\infty} = P_{\mathbb{Q}}((m)\cdot\infty)$.
2. $P_K(\mathfrak{m})$ is sometimes called the a ray or a ray group.

Proposition 1.6. $[I_K(\mathfrak{m}) : P_K(\mathfrak{m})] < \infty$.

Proof. Omitted and a special case is on example sheet. □

Definition 1.12. A subgroup $H \leq I_K(\mathfrak{m})$ is a congruence subgroup for $\mathfrak{m}$ if $P_k(\mathfrak{m}) \leq H \leq I_K(\mathfrak{m})$.

Definition 1.13. For a congruence subgroup H for $\mathfrak{m}$. The quotient $I_k(\mathfrak{m})/H$ is a generalised ideal class group.
If $H = P_k(\mathfrak{m})$, we call this quotient the ray class group.

Example 1.6. When $\mathfrak{m} = 1$, the ray class group is just the ideal class group.

Proposition 1.7. *Write $P_{\mathfrak{m}} \leq I_K(\mathfrak{m})$ to denote the subgroup of principal fractional ideals in $I_K(\mathfrak{m})$. Then we have an exact sequence*

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

Remark. This shows that $h_K \mid h_K(\mathfrak{m})$ where $h_K = \#\,\mathrm{Cl}(K)$ is the class number of K and $h_K(\mathfrak{m}) = \#(I_K(\mathfrak{m})/P_K(\mathfrak{m}))$.

To prove this, recall that for any ideal $I \leq \mathcal{O}_K$, every ideal class in $\mathrm{Cl}(K)$ can be represented by an ideal coprime to I.

Sketch of proof. Let $\mathfrak{a} \in I_K(\mathfrak{m})$. Consideer $h : I_K(\mathfrak{m}) \to \mathrm{Cl}(K)$ via $h(\mathfrak{a}) = [\mathfrak{a}]$. This is a group homomorphism with kernel $P_{\mathfrak{m}}$, surjective by the fact we just recalled. Hence the exact sequence

$$1 \longrightarrow P_{\mathfrak{m}} \longrightarrow I_K(\mathfrak{m}) \longrightarrow \mathrm{Cl}(K) \longrightarrow 1$$

But $\ker h \supset P_K(\mathfrak{m})$, so we get the exact sequence as claimed. □

Example 1.7. Let $K = \mathbb{Q}$ and m an integer. Then $I_{\mathbb{Q}}((m))/P_{\mathbb{Q}}((m)) \cong (\mathbb{Z}/m\mathbb{Z})^\times/\{\pm 1\}$ and $I_{\mathbb{Q}}(\mathfrak{m})/P_{\mathbb{Q}}(\mathfrak{m}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ where $\mathfrak{m} = (m)\cdot\infty$.
We've seen the surjection $\Phi_{\mathfrak{m}} : I_{\mathbb{Q}}(\mathfrak{m}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. Since $\ker \Phi_{\mathfrak{m}} = P_{\mathbb{Q}}(\mathfrak{m})$, $\Phi_{\mathfrak{m}}$ descends to an isomorphism $I_{\mathbb{Q}}(\mathfrak{m})/P_{\mathbb{Q}}(\mathfrak{m}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$.

Class field theory is the idea of generalising this phenomenon, by establishing a general isomorphism between certain generalised class groups and Galois groups of abelian extensions via the Artin map.

Proposition 1.8. *Let $M/L/K$ be a tower of abelian extensions. Suppose a modulus $\mathfrak{m}$ contains all primes of $\mathcal{O}_K$ that ramify in M, then the diagram*

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

Remark. Recall that an infinite prime ramifies if it is a real infinite prime and it is the restriction of a complex infinite prime in the bigger field.

1.5 The Conductor

Lemma 1.9. *Let L/K be an abelian extension and a $\mathfrak{m}$ be a modulus containing all ramified primes of K, and $\mathfrak{n}$ is another modulus with $\mathfrak{m} \mid \mathfrak{n}$. If $P_K(\mathfrak{m}) \subset \ker \Phi_\mathfrak{m}$, then $P_K(\mathfrak{n}) \subset \ker \Phi_\mathfrak{n}$.*

Proof. Since $\mathfrak{m} \mid \mathfrak{n}$, we have $P_K(\mathfrak{n}) \subset P_K(\mathfrak{m})$ and $\Phi_\mathfrak{n} = \Phi_\mathfrak{m}|_{I_K(\mathfrak{m})}$. So $\ker \Phi_n = \ker(\Phi_\mathfrak{m}|_{I_K(\mathfrak{n})})$.
If $(\alpha) \in P_K(\mathfrak{n}) \subset P_K(\mathfrak{m}) \subset \ker \Phi_\mathfrak{m}$, then since $P_K(\mathfrak{n}) \subset I_K(\mathfrak{n})$, we have $(\alpha) \in \ker(\Phi_\mathfrak{m}) \cap I_K(\mathfrak{n}) = \ker \Phi_\mathfrak{n}$. □

This means that if $\ker \Phi_\mathfrak{m}$ is a congruence subgroup for $\mathfrak{m}$, so is $\ker \Phi_\mathfrak{n}$ for any $\mathfrak{n}$ divisible by $\mathfrak{m}$. So there is a "best" modulus.

Theorem 1.10 (The Conductor Theorem)**.** *Let L/K be an abelian extension, then there is a modulus $\mathfrak{f}(L/K)$ such that:*
(i) A prime of K (finite or infinite) ramifies in L if and only if it divides $\mathfrak{f}(L/K)$.
(ii) If $\mathfrak{m}$ is a modulus divisible by all primes of K that ramifies in L, then $\ker \Phi_\mathfrak{m}$ is a congruence subgroup for $\mathfrak{m}$ if and only if $\mathfrak{f}(L/K) \mid \mathfrak{m}$.

It's clear that $\mathfrak{f}(L/K)$ is uniquely determined.

Definition 1.14. $\mathfrak{f}(L/K)$ is the conductor of L/K.

Example 1.8. 1. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{d})$ where $d \neq 0, 1$ is square-free. Then

$$\mathfrak{f}(L/K) = \begin{cases} |D| & \text{if } d > 0 \\ |D| \cdot \infty & \text{if } d < 0 \end{cases}$$

where D is the discriminant of L over K.
2. Let $K = \mathbb{Q}$ still and $L = \mathbb{Q}(\zeta_m)$. Then

$$\mathfrak{f}(L/K) = \begin{cases} 1 & \text{if } m \leq 2 \\ (m/2) \cdot \infty & \text{if } v_2(n) = 1 \\ (m) \cdot \infty & \text{otherwise} \end{cases}$$

Remark. The conductor is not always the simple product of ramified primes. We sometimes need a higher multiplicity for some of them. In example sheet, you'll find a cubic extension ramified only at 3, but where neither $\mathfrak{m} = (3)$ nor $\mathfrak{m} = (3) \cdot \infty$ has $\ker \Phi_{L/K,\mathfrak{m}}$ a congruence subgroup (so $\mathfrak{f}(L/\mathbb{Q})$ divides neither of them).

1.6 Artin Reciprocity

For each abelian extension L/K, $\mathrm{Gal}(L/K)$ turns out to be a generalised ideal class group.

Theorem 1.11 (Artin Reciprocity)**.** *Let L/K be abelian and let $\mathfrak{m}$ be a modulus divisible by $\mathfrak{f}(L/K)$. Then the Artin map $\Phi_\mathfrak{m} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$ is surjective. Its kernel is a congruence subgroup, so we have an isomorphism between a generalised class group and $\mathrm{Gal}(L/K)$ induced by $\Phi_\mathfrak{m}$.*

We'll later show Theorem 1.11 using density theorems. Let's first try to understand this kernel.

Definition 1.15. The norm map of L/K is $N_{L/K} : I_L \to I_K$ defined by

$$\prod_i \mathfrak{P}_i^{e_i} \mapsto \prod_i (\mathfrak{P}_i \cap \mathcal{O}_K)^{f_{\mathfrak{P}_i|\mathfrak{P}_i\cap\mathcal{O}_K} e_i}.$$

In particular, for any $\mathfrak{P}$ lying above $\mathfrak{p}$, we have $N_{L/K}\mathfrak{P} = \mathfrak{p}^{f_{\mathfrak{P}|\mathfrak{p}}}$.

Definition 1.16. Let L/K be an abelian extension of which $\mathfrak{m}$ is a modulus divisible by $\mathfrak{f}(L/K)$. The norm group (or Takagi group) associated to $\mathfrak{m}$ is the congruence subgroup $T_{L/K}(\mathfrak{m}) = N_{L/K}(I_L(\mathfrak{m}))P_K(\mathfrak{m})$. where $I_L(\mathfrak{m}) \leq I_L$ consists of fractional ideals in L coprime to $\mathfrak{m}\mathcal{O}_L$.

Theorem 1.12 (Artin Reciprocity, Continued)**.** $\ker \Phi_{\mathfrak{m}} = T_{L/K}(\mathfrak{m})$.

Artin reciprocity gives us information about decomposition of primes.

Theorem 1.13 (Decomposition Theorem)**.** *Let L/K be abelian of degree n and suppose $\mathfrak{p} \leq \mathcal{O}_K$ is unramified in L. Let $\mathfrak{m}$ be a modulus divisible by $\mathfrak{f}(L/K)$ but not by $\mathfrak{p}$. Write $H = \ker \Phi_{\mathfrak{m}}$.*
Suppose f is the smallest positive integer such that $\mathfrak{p}^f \in H$. Then $\mathfrak{p}$ decomposes in L into a product $\mathfrak{P}_1 \cdots \mathfrak{P}_g$ of $g = n/f$ distinct primes, all of inertia degree f over $\mathfrak{p}$.

Proof. Suppose $\mathfrak{p}$ decomposes as $\mathfrak{P}_1 \cdots \mathfrak{P}_g$. Their common inertia degree is the order of $(L/K, \mathfrak{p})$ in $\mathrm{Gal}(L/K)$, hence (via the isomorphism $I_K(\mathfrak{m})/H \cong \mathrm{Gal}(L/K)$) the order of $\mathfrak{p}$ mod H in $I_K(\mathfrak{m})/H$, which is f. On the other hand, $n = fg$ by Theorem 1.1. □

1.7 The Existence Theorem

Every generalised ideal class group is the Galois group of some abelian extension.

Theorem 1.14 (Existence Theorem)**.** *Let $\mathfrak{m}$ be a modulus of K and H any congruence subgroup for $\mathfrak{m}$. Then there is a unique abelian extension L/K with the property that all its ramified (finite or infinite) primes divide $\mathfrak{m}$, $H = N_{L/K}(I_L(\mathfrak{m}))P_K(\mathfrak{m})$, and $I_K(\mathfrak{m})/H \cong \mathrm{Gal}(L/K)$ via $\Phi_{\mathfrak{m}}$.*

Definition 1.17. Let $\mathfrak{m}$ be any modulus and H the congruence subgroup $P_K(\mathfrak{m})$. Then the ray class field is the unique abelian extension $K_{\mathfrak{m}}/K$ such that $P_K(\mathfrak{m}) = \ker \Phi_{K_{\mathfrak{m}}/K,\mathfrak{m}}$ given by the preceding theorem. In particular, $\mathrm{Gal}(K_{\mathfrak{m}}/K) \cong I_K(\mathfrak{m})/P_K(\mathfrak{m})$.

Example 1.9. Let m be a positive integer not congruent to 2 modulo 4. For $K = \mathbb{Q}$, we have $K_{(m)\cdot\infty} = \mathbb{Q}(\zeta_m)$ and $K_{(m)} = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$.

Corollary 1.15. *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 ramified in either L or M such that $P_K(\mathfrak{m}) \leq \ker \Phi_{M/K,\mathfrak{m}} \leq \ker \Phi_{L/K,\mathfrak{m}}$.*

Sketch of proof. Suppose first that $L \subset M$. Then by Theorem 1.11, there exists moduli $\mathfrak{m}_1, \mathfrak{m}_2$ such that $P_K(\mathfrak{m}_1) \leq \ker \Phi_{L/K,\mathfrak{m}_1}$ and $P_K(\mathfrak{m}_2) \leq \ker \Phi_{M/K,\mathfrak{m}_2}$. Lemma 1.9 shows that we can find some $\mathfrak{m}$ dividing both $\mathfrak{m}_1, \mathfrak{m}_2$ such that $P_K(\mathfrak{m}) \leq \ker \Phi_{L/K,\mathfrak{m}}$ and $P_K(\mathfrak{m}) \leq \ker \Phi_{M/K,\mathfrak{m}}$. But $\Phi_{L/K,\mathfrak{m}} = \mathrm{res} \circ \Phi_{M/K,\mathfrak{m}}$, hence the result.

Conversely, suppose we have the inclusion $P_K(\mathfrak{m}) \leq \ker \Phi_{M/K,\mathfrak{m}} \leq \ker \Phi_{L/K,\mathfrak{m}}$, then under $\Phi_{M/K,\mathfrak{m}} : I_K(\mathfrak{m}) \to \mathrm{Gal}(M/K)$, the subgroup $\ker \Phi_{L/K,\mathfrak{m}} \leq I_K(\mathfrak{m})$ maps to a subgroup $H \leq \mathrm{Gal}(M/K)$. H corresponds to an intermediate field $K \subset \tilde{L} \subset M$.
The first part of the proof applied to $\tilde{L} \subset M$ shows that $\ker \Phi_{\tilde{L}/K,\mathfrak{m}} = \Phi_{L/K,\mathfrak{m}}$, so $L = \tilde{L}$ by the uniqueness part of 1.14. □

Remark. This implies that every abelian extension is contained in a ray class field. Indeed, if L/K is abelian and $\mathfrak{f}(L/K) \mid \mathfrak{m}$, then $H = \ker \Phi_{L/K,\mathfrak{m}}$ is a congruence subgroup $H \geq P_K(\mathfrak{m})$. So by the preceding corollary, $L \subset K_{\mathfrak{m}}$.

Theorem 1.16 (Classification Theorem)**.** *Let K be a number field. Then there is an order-reversing bijection between the system of abelian extensions of K and the system of generalised ideal class groups of K.*

Theorem 1.17 (Kronecker-Weber)**.** *Let $L/\mathbb{Q}$ be an abelian extension, then there is some positive integer m such that $L \subset \mathbb{Q}(\zeta_m)$.*

Proof. By Theorem 1.11, there is a modulus $\mathfrak{m}$ such that $\ker \Phi_{L/\mathbb{Q},\mathfrak{m}} \supset P_{\mathbb{Q}}(\mathfrak{m})$. Lemma 1.9, we may assume that $\mathfrak{m} = (m) \cdot \infty$ for some $m \in \mathbb{Z}_{>0}$. But then $P_{\mathbb{Q}}(\mathfrak{m}) = \ker \Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},\mathfrak{m}}$, so we are done by Corollary 1.15. □

1.8 Hilbert Class Field

Let K be a number field. Setting $\mathfrak{m} = 1$ in Theorem 1.14 gives us an unramified abelian extension and has Galois group isomorphic to the ideal class group of K.

Definition 1.18. This unramified abelian extension is known as the Hilbert class group of K.

Example 1.10. The Hilbert class field of $\mathbb{Q}$ is itself.

Theorem 1.18. *The Hilbert class field of K is the maximal unramified abelian extension of K.*

Remark. In view of Theorem 1.10, when we say L/K is unramified we mean $\mathfrak{f}(L/K) = 1$ (i.e. taking into account the infinite primes).

Proof. Write F for the Hilbert class field of K. Suppose M/K is another unramified abelian extension. Then $\mathfrak{f}(M/K) = 1$ and $P_K(1) \leq \ker \Phi_{M/K,1}$. So $P_K(1) = P_K = \ker \Phi_{F/K,1} \subset \Phi_{M/K,1}$ and we are done by Corollary 1.15. □

Theorem 1.16 applied to unramified abelian extensions now reads:

Corollary 1.19. *Suppose M/K corresponds to $H \leq \mathrm{Cl}(K)$, then the Artin map gives an isomorphism $\mathrm{Cl}(K)/H \to \mathrm{Gal}(M/K)$.*

Example 1.11. Let $K = \mathbb{Q}(\sqrt{-5})$, then we'll show that its Hilbert class field F is $\mathbb{Q}(\sqrt{-5}, i)$. It's not hard to compute $h_K = 2$, so we must have $\#\,\mathrm{Gal}(F/K) = 2$, i.e. F is an(y) unramified quadratic extension of $\mathbb{Q}(\sqrt{-5})$.
The only prime that ramifies in $\mathbb{Q}(i)/\mathbb{Q}$ is 2 and the only prime that ramifies in $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ is 5. Therefore the only primes that can ramify in $\mathbb{Q}(\sqrt{-5}, i)/\mathbb{Q}$, the composite of $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{5})$, are 2 and 5. But $2, 5$ both already ramify in $\mathbb{Q}(\sqrt{-5})$, and also $\mathbb{Q}(\sqrt{-5})$ has no real infinite prime. So $\mathbb{Q}(\sqrt{-5}, i)/\mathbb{Q}(\sqrt{-5})$ must be unramified.

Let's characterise the primes which split in the Hilbert class field.

Corollary 1.20. *Let F be the Hilbert class field of K. A prime ideal $\mathfrak{p} \leq \mathcal{O}_K$ splits completely in F if and only if $\mathfrak{p}$ is principal.*

Proof. We know $\mathfrak{p}$ splits completely in F iff $(L/K, \mathfrak{p}) = 1$ (note that $\mathfrak{p}$ must be unramified in F since F is unramified). But the Artin map induces an isomorphism $\mathrm{Cl}(K) \cong \mathrm{Gal}(F/K)$. □

Theorem 1.21 (Principal Ideal Theorem)**.** *In the Hilbert class field, every ideal of K becomes principal.*

Example 1.12. Let $K = \mathbb{Q}(\sqrt{-5})$ which has Hilbert class field $F = \mathbb{Q}(\sqrt{5}, i)$. Then $\mathrm{Cl}(K) = \{[\mathcal{O}_K], [(2, 1+\sqrt{-5})]\}$. And in fact $(2, 1+\sqrt{-5})\mathcal{O}_F$ is principal, and is generated by $1 + i$.

1.9 Reciprocity Theorems

Let K be a number field containing a primitive n-th root of unity ζ. Let $\mathfrak{p} \leq \mathcal{O}_K$ be a prime ideal in $\mathcal{O}_K$. Then for $\alpha \in \mathcal{O}_K$ prime to $\mathfrak{p}$, we have $\alpha^{N(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}}$.
Suppose that $\mathfrak{p}$ is prime to n. Then $n \mid N(\mathfrak{p}) - 1$, so $x = \alpha^{(N(\mathfrak{p})-1)/n}$ is a solution to the congruence $x^n \equiv 1 \pmod{\mathfrak{p}}$, i.e. $\alpha^{(N(\mathfrak{p})-1)/n} \equiv 1, \zeta, \zeta^2, \ldots, \zeta^{n-1} \pmod{\mathfrak{p}}$. Since the n-th roots of unity are distinct modulo $\mathfrak{p}$, $\alpha^{(N(\mathfrak{p})-1)/n}$ is congruent to a unique n-th root of unity modulo $\mathfrak{p}$. We write $(\alpha/\mathfrak{p})_n$ for this root of unity.
More generally, if $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ is an ideal of $\mathcal{O}_K$ which α is prime to, then we set

$$\left(\frac{\alpha}{\mathfrak{a}}\right)_n = \prod_{j=1}^{n} \left(\frac{\alpha}{\mathfrak{p}_j}\right)_n$$

Thus if $\mathfrak{m}$ is a modulus of K such that every prime containing $n\alpha$ divides $\mathfrak{m}$, then $(\alpha/-)_n$ becomes a homomorphism $I_K(\mathfrak{m}) \to \mu_n$, where $\mu_n = \mu_n(K)$ is the group of n-th roots of unity in K.

Definition 1.19. $(-/-)_n$ is known as the n-th power Legendre symbol.

Remark. This extends the Legendre symbol in the study of quadratic residues.

Recall that if K has a primitive n-th root of unity, then for any $\alpha \in K$, $L = K(\sqrt[n]{\alpha})$ is Galois over K and for any $\sigma \in \mathrm{Gal}(L/K)$ we have $\sigma\sqrt[n]{\alpha} = \xi\sqrt[n]{\alpha}$ for some $\xi \in \mu_n(K)$. We therefore get an injective homomorphism $\mathrm{Gal}(L/K) \to \mu_n(K)$.

Theorem 1.22 (Weak Reciprocity)**.** *Let K be a number field containing a primitive n-th root of unity and suppose $L = K(\sqrt[n]{\alpha})$ for some nonzero $\alpha \in \mathcal{O}_K$. Assume $\mathfrak{m}$ is a modulus divisible by all primes containing $n\alpha$ and suppose $\ker \Phi_{L/K,\mathfrak{m}}$ is a congruence subgroup for $\mathfrak{m}$, then there is a commutative diagram*

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

Furthermore, if G is the image of $\mathrm{Gal}(L/K)$ in μ_n, then $(\alpha/-)_n$ induces a surjective homomorphism $(\alpha/-)_n : I_K(\mathfrak{m})/P_K(\mathfrak{m}) \to \mu_n$.

Proof. We have $(L/K, \mathfrak{p})(\sqrt[n]{\alpha}) = (\alpha/\mathfrak{p})_n \sqrt[n]{\alpha}$ pretty much by definition. This gives the commutativity of the diagram. The last part follows from Theorem 1.11. □

Remark. There is something called the "strong reciprocity", which gives the Legendre symbol in terms of the n-th power Hilbert symbol, which we are not gonna define.

Theorem 1.23 (Quadratic Reciprocity)**.** *Let p, q be distinct odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

Proof. This is equivalent to say $(p^*/q) = (q/p)$ where $p^* = (-1)^{(p-1)/2}p$. Recall that $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is a generalised ideal class group for $\mathfrak{m} = (p) \cdot \infty$. So the same holds for any subfield of $\mathbb{Q}(\zeta_p)$.
Since $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is cyclic of order $p-1$, there is a unique subfield $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_p)$ quadratic over $\mathbb{Q}$, and by what we've said $\mathrm{Gal}(K/\mathbb{Q})$ is a generalised ideal class group to $(p) \cdot \infty$.
Indeed, $K = \mathbb{Q}(\sqrt{p^*})$. (p) is the only finite prime of $\mathbb{Q}$ ramified in K. So $\ker \Phi_{K/\mathbb{Q},(p)\cdot\infty}$ is a congruence subgroup for $(p)\cdot\infty$. Bythe preceding theorem, we have a surjection $I_{\mathbb{Q}}((p)\cdot\infty)/P_{\mathbb{Q}}((p)\cdot\infty) \to \{\pm 1\}$ induced by $(p^*/-)$. Consider the map $(\mathbb{Z}/p\mathbb{Z})^\times \to I_{\mathbb{Q}}((p)\cdot\infty)/P_{\mathbb{Q}}((p)\cdot\infty), [a] \mapsto [a\mathbb{Z}]$ which induces an isomorphism. We therefore get a surjective homomorphism $(p^*/-) : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$. But $(-/p)$ also gives a surjective homomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$ and $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, so they must be the same, i.e. $(p^*/q) = (q/p)$. □

2 ζ-Functions and L-Series

I don't have to tell you that many arithemtic information are contained in the behaviour of all kinds of ζ-functions and L-functions.

2.1 Dirichlet Series

Definition 2.1. A Dirichlet series is a series of the form $f(s) = \sum_n a_n n^{-s}$ for $a_n, s \in \mathbb{C}$.

We often write $s = \sigma + it, \sigma, t \in \mathbb{R}$.
Suppose $\{a_n\}_{n\geq 1}$ is any sequence of complex numbers. We'll write $A(N) = \sum_{n=1}^{N} a_n$ and $A(M, N) = \sum_{n=M}^{N} a_n$.

Theorem 2.1. *If a Dirichlet series $f(s) = \sum_n a_n n^{-s}$ converges for some $s = s_0 = \sigma_0 + it_0$, then it converges for any $s = \sigma + it$ such that $\sigma > \sigma_0$, uniformly on any compact subset of $\{\sigma > \sigma_0\}$.*

Proof. We'll prove that the series converges uniformly on every region of the form $\{|\arg(s - s_0)| \leq \pi/2 - \epsilon < \pi/2\}$ for $\epsilon > 0$. Since

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

We may assume WLOG that $s_0 = 0$.
Now our assumption means that $A(N)$ converges as $N \to \infty$, and for each $\epsilon > 0$ we have some N_0 such that $|A(M,N)| \leq \epsilon$ for all $N > M \geq N_0$. Now for each $N > M \geq N_0$, we have

$$\begin{aligned}\sum_{n=M}^{N} \frac{a_n}{n^s} &= \sum_{n=M}^{N} (A(M,n) - A(M,n-1))n^{-s} \\ &= A(M,N)N^{-s} + \sum_{n=M}^{N-1} A(M,n)(n^{-s} - (n+1)^{-s})\end{aligned}$$

Now we have the estimate

$$|n^{-s} - (n+1)^{-s}| = \left| s \int_n^{n+1} \frac{\mathrm{d}x}{x^{s+1}} \right| \leq |s| \int_n^{n+1} \frac{\mathrm{d}x}{x^{s+1}} = \frac{|s|}{\sigma}(n^{-\sigma} - (n+1)^{-\sigma})$$

But $|s|/\sigma$ is bounded in the region $\{-\pi/2 < \arg s < \pi/2\}$. Say $|s|/\sigma < C$ for s in this region, then we get the estimate

$$\begin{aligned}\left| \sum_{n=M}^{N} \frac{a_n}{n^s} \right| &= |A(M,N)||N^{-s}| + \sum_{n=M}^{N-1} |A(M,n)||n^{-s} - (n+1)^{-s}| \\ &\leq \epsilon N^{-\sigma} + C\epsilon M^{-\sigma} < (C+1)N_0^{-\sigma}\epsilon\end{aligned}$$

for $-\pi/2 < \arg s < \pi/2$. □

Definition 2.2. The smallest $\sigma_0 \in \mathbb{R}$ such that a Dirichlet series f converges in the region $\{\sigma > \sigma_0\}$ is called the abscissa of convergence for f.

Remark. 1. We see from the preceding theorem that f would converge in the region $\{\sigma > \sigma_0\}$ but diverges in the region $\{\sigma < \sigma_0\}$. 2. If the f converges for $s_1 = \sigma_1 + it_1$, then we must have an estimate $a_n = O(n^{\sigma_1})$, and f converges absolutely and uniformly on compact subsets of $\{\sigma \geq \sigma_1 + 1 + \delta\}$ for any $\delta > 0$.

Theorem 2.2. *Suppose there exists a number C and $\sigma_1 \geq 0$ such that $|A(N)| \leq CN^{\sigma_1}$ for all N. Then the abscissa of convergence for f is at most σ_1.*

Proof. Exercise. □

2.2 Riemann ζ-Function

The Dirichlet series associated with $a_n = 1$ is known as the Riemann ζ-function $\zeta(s) = \sum_n n^{-s}$. Theorem 2.2 shows that $\zeta(s)$ converges for $\sigma > 1$.
We'll show that $\zeta(s)$ has a meromorphic continuation to $\{\sigma > 0\}$ with a pole at $s = 1$. Once we know this, we must have $\mathrm{Res}_{s=1}\,\zeta(s) = 1$ since for any $\sigma > 1$,

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

So $s = 1$ is a simple pole with residue 1.
To formulate the continuation, we use the following trick: Consider $\zeta_2(s) = \sum_{n \geq 1}(-1)^{n+1}n^{-s} = (1 - 2^{1-s})\zeta(s)$. Theorem 2.2 shows that $\zeta_2(s)$ converges for $\sigma > 0$. But we are done: $\zeta(s) = \zeta_2(s)/(1 - 2^{1-s})$ extends ζ to $\{\sigma > 0\}$ with

only possible poles at $s = 1 + 2\pi ik/\log 2$ for $k \in \mathbb{Z}$.
We similarly define $\zeta_3(s) = \sum_{n\geq 0}(1/(3n+1)^s + 1/(3n+2)^s - 2/(3n+3)^s)$ which converges in $\{\sigma > 0\}$ and has $\zeta(s) = \zeta_3(s)/(1-3^{1-s})$. This shows that the poles of ζ on $\{\sigma > 0\}$ are at $s = 1 + 2\pi ik/\log 3$ for $k \in \mathbb{Z}$, so essentially the only pole is at $s = 1$.

Proposition 2.3. *For $\sigma > 1$, we have $\zeta(s) = \prod_{p\ prime}(1 - p^{-s})^{-1}$.*

Recall that an infinite product $\prod_n a_n$ of nonzero complex numbers is said to converge if the sequence $\sum_{n=1}^N a_n$ has a nonzero limit as $N \to \infty$. Equivalently, the series $\sum_n \log a_n$ converges. The product converges absolutely if this series does.

Proof. Write $E(s) = \prod_{p \text{ prime}}(1 - p^{-s})^{-1}$. Then

$$\log E(s) = \sum_{p \text{ prime}} \sum_{n=1}^{\infty} \frac{1}{np^{ns}}$$

which converges absolutely if $\sigma \geq 1+\delta$ for some $\delta > 0$, as $|p^{ns}| = p^{n\sigma} \geq p^{n(1+\delta)}$. On the other hand, we have $(1 - p^{-s})^{-1} = 1 + p^{-s} + p^{-2s} + \cdots$, so if $p_1, \ldots, p_r$ are primes at most N then

$$\prod_{p\leq N \text{ prime}} \frac{1}{1-p^{-s}} = \sum_{e_1,\ldots,e_r=0}^{\infty} \frac{1}{(p_1^{e_1}\cdots p_r^{e_r})^s} = \sum_n{}' \frac{1}{n^s}$$

where $\sum_n'$ sums over all n such that $p \mid n$ for some $p \leq N$ prime. In particular, $\sum_n'$ summed over all $n \leq N$, so

$$\prod_{p\leq N \text{ prime}} \frac{1}{1-p^{-s}} = \sum_{n\leq N} \frac{1}{n^s} + \sum_{n>N}{}' \frac{1}{n^s}$$

Therefore

$$\left| \prod_{p\leq N \text{ prime}} \frac{1}{1-p^{-s}} - \zeta(s) \right| \leq \left| \sum_{n>N, p\nmid n} \frac{1}{n^s} \right| \leq \sum_{n>N} \frac{1}{n^{1+\delta}}$$

which goes to 0 as $N \to \infty$. □

Definition 2.3. The gamma function is the absolutely convergent integral

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

defined for $\sigma > 0$.

Proposition 2.4. *(i) $\Gamma(s)$ is analytic and admits a meromorphic continuation to $\mathbb{C}$.*
(ii) $\Gamma(s)$ is nowhere zero, and only has simple poles at $s = -n$ for $n = 0, 1, \ldots$, with residues $(-1)^n/n!$.
(iii) $\Gamma(s)$ satisfies the functional equations $\Gamma(s + 1) = s\Gamma(s)$, $\Gamma(s)\Gamma(1 - s) = \pi/\sin(\pi s)$ and $\Gamma(s)\Gamma(s + 1/2) = 2^{1-2s}\sqrt{\pi}\Gamma(2s)$.
(iv) $\Gamma(n) = n!$ for $n \in \mathbb{N}$, $\Gamma(1/2) = \sqrt{\pi}$.

Yeah we are not gonna prove this. Consult literally any book on analytic number theory.
Now for $\sigma > 1$,

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

So

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

Definition 2.4. The completed ζ-function is $Z(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$.

Our calculation before then yields:

Proposition 2.5. *We have*

$$Z(s) = \frac{1}{2}\int_0^\infty (\theta(iy) - 1) y^{s/2} \frac{\mathrm{d}y}{y}$$

where $\theta(z) = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 z}$ *is the Jacobi* θ*-series.*

So let's try to understand θ.

Proposition 2.6. *The series* $\theta(z)$ *is analytic on* $\mathfrak{h} = \{z \in \mathbb{Z} : \operatorname{Im} z > 0\}$ *and satisfies* $\theta(-1/z) = \sqrt{z/i}\theta(z)$ *where* $\sqrt{z/i} = \exp((1/2)\log(z/i))$ *with the principal branch of* log *taken.*

Definition 2.5. Let $f : \mathbb{R}_+ \to \mathbb{C}$ be continuous. The Mellin transform of f is

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

provided that $f(\infty) = \lim_{x\to\infty} f(x)$ exists and is finite, and that the integral exists.

Theorem 2.7 (Mellin Principle)**.** *Let* $f, g : \mathbb{R}_+ \to \mathbb{C}$ *be continuous and* $f(y) = a_0 + O(e^{-c_0 y^\alpha}), g(y) = b_0 + O(e^{-c_0 y^\alpha})$ *as* $y \to \infty$*, for some* a_0, b_0 *and* $c_0 > 0, \alpha > 0$*. If* $f(1/y) = Cy^k g(y)$ *for some* $k > 0$ *and* $C \in \mathbb{C}^\times$*, then:*
(i) $M(f,s)$ *and* $M(g,s)$ *converge absolutely and uniformly on any compact subset of* $\{\sigma > k\}$*. Therefore they are holomorphic on* $\{s \in \mathbb{C} : \sigma > k\}$ *and admit holomorphic continuation to* $\mathbb{C} \setminus \{0, k\}$*.*
(ii) $M(f,s)$ *and* $M(g,s)$ *have simple poles at* $s = 0, k$ *where* $\operatorname{Res}_{s=0} M(f,s) = -a_0$*,* $\operatorname{Res}_{s=0} M(g,s) = b_0$*,* $\operatorname{Res}_{s=k} M(f,s) = Cb_0$*,* $\operatorname{Res}_{s=0} M(g,s) = C^{-1}a_0$*.*
(iii) We have $M(f,s) = CM(f, k-s)$*.*

Ain't gonna prove this either.

Theorem 2.8. $Z(s)$ *adimts an analytic continuation to* $\mathbb{C} \setminus \{0,1\}$*, has simple poles at* $s = 0, 1$ *with residues* $-1, 1$ *respectively, and satisfies the functional equation* $Z(s) = Z(1-s)$*.*

Proof. $Z(2s) = M(f,s)$ where $f(y) = (1/2)\theta(iy)$.
We have

$$\theta(iy) = 1 + 2e^{-\pi y}\left(1 + \sum_{n=2}^\infty e^{-\pi(n^2-1)y}\right)$$

and therefore $f(y) = 1/2 + O(e^{-\pi y})$. Also $f(1/y) = y^{1/2} f(y)$ by Proposition 2.6, so we conclude using the preceding theorem. □

Corollary 2.9. *$\zeta(s)$ admits an analytic continuation to $\mathbb{C} \setminus \{1\}$, has a simple pole at $s = 1$ with residue 1, and satisfies the functional equation $\zeta(1-s) = 2(2\pi)^{-s}\Gamma(s)\cos(\pi s/2)\zeta(s)$.*

Proof. Recall that $Z(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$, so our desired continuation would be $\zeta(s) = \Gamma(s/2)^{-1}\pi^{s/2}Z(s)$. Both $Z(s)$ and $\Gamma(s/2)$ has a simple zero at $s = 0$, so ζ is holomorphic at $s = 0$. At $s = 1$, $Z(s)$ has a simple pole with residue 1, so the same is true for $\zeta(s)$ since $\Gamma(1/2) = \sqrt{\pi}$. ζ is holomorphic elsewhere since Γ is nonvanishing.
Now $Z(s) = Z(1-s)$, so $\zeta(1-s) = \pi^{1/2-s}\Gamma(s/2)\Gamma((1-s)/2)^{-1}\zeta(s)$. But we know that $\Gamma(s/2)\Gamma((1+s)/2) = 2^{1-s}\sqrt{\pi}\Gamma(s)$ and $\Gamma((1-s)/2)\Gamma((1+s)/2) = \pi/\cos(\pi s/2)$. So we have the result. □

What about the zeros of ζ? We know that ζ is nonvanishing at $\sigma > 1$ due to Proposition 2.3. For $\sigma < 0$, ζ vanishes at $-2, -4, -6, \ldots$ by the functional equation. They are known as the "trivial zeros". All the other zeros must line in the "critical strip" $\{0 \le \sigma \le 1\}$, they are called the "nontrivial zeros".

Proposition 2.10 (Riemann Hypothesis)**.** *The nontrivial zeros of ζ all have real part $1/2$.*

Proof. Suppose $\zeta(s) = 0$ with $0 \le \sigma \le 1$. It's known that $\sigma \ne 0, 1 \ldots$.
Wait, you didn't really expect a proof, did you? □

2.3 Dedekind ζ-Function

Definition 2.6. Let K be a number field. Its (Dedekind) ζ-function is the series $\zeta_K(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}$, where the sum is taken over ideals $0 \ne \mathfrak{a} \le \mathcal{O}_K$ and $N(\mathfrak{a}) = \#(\mathcal{O}_K/\mathfrak{a})$.

Proposition 2.11. *The series $\zeta_K(s)$ converges absolutely and uniformly in $\{\sigma \ge 1 + \delta\}$ for any $\delta > 0$, and we have an Euler product*

$$\zeta_K(s) = \prod_{\mathfrak{p} \le \mathcal{O}_K \text{ prime}} \frac{1}{1 - N(\mathfrak{p})^{-s}}$$

Proof. Similar to the case of ζ, but now using the multiplicativity of N and unique factorisation. □

We'll see that ζ_K too has an analytic continuation to $\mathbb{C}\setminus\{1\}$ and satisfies the functional equation relating its values at s and $1 - s$. We'll do this by splitting up ζ_K using ideal classes.

Definition 2.7. For an ideal class $\mathscr{C} \in \mathrm{Cl}(K)$, the partial ζ-function is defined as $\zeta(\mathscr{C}, s) = \zeta_K(\mathscr{C}, s) = \sum_{\mathfrak{a} \in \mathscr{C}, \mathfrak{a} \le \mathcal{O}_K} N(\mathfrak{a})^{-s}$.

Then $\zeta_K(s) = \prod_{\mathscr{C} \in \mathrm{Cl}(K)} \zeta(\mathscr{C}, s)$.

Definition 2.8. Let $Z_\infty(s) = |d_K|^{s/2}\pi^{-ns}\Gamma_K(s/2)$ where $n = [K : \mathbb{Q}]$ and Γ_K is a version of the Γ-function. The completed partial ζ-function is $Z(\mathscr{C}, s) = Z_\infty(s)\zeta(\mathscr{C}, s)$.

Theorem 2.12. *The completed partial ζ-function admits an analytic continuation to $\mathbb{C} \setminus \{0,1\}$ and satisifes the functional equation $Z(\mathscr{C}, s) = Z(\mathscr{C}', 1-s)$ where $\mathscr{C}\mathscr{C}' = [\partial]$ is the class of the different ideal.*
Further more, it has simple poles at $s = 0, 1$ with residues $-2^r R/w, 2^r R/w$ respectively, where r is the number of infinite primes, w the number of roots of unity, and R the regulator, respectively of K.

Remark. We will not prove this. But the idea is basically Theorem 2.7.

Definition 2.9. Let $Z_K(s) = Z_\infty(s)\zeta_K(s) = \sum_{\mathscr{C} \in \mathrm{Cl}(K)} Z(\mathscr{C}, s)$ is the completed ζ-function of K.

Corollary 2.13. *$Z_K(s)$ admits an analytic continuation to $\mathbb{C} \setminus \{0,1\}$, satisfies the functional equation $Z_K(s) = Z_K(1-s)$, has simple poles at $s = 0, 1$ with residues $-2^r hR/w$ and $-2^r hR/w$ where $h = h_K = \#\,\mathrm{Cl}(K)$.*

For a number field K, let r_1 be the number of real places and r_2 the number of complex places of it. After analysing $Z_\infty(s)$, one might find

Corollary 2.14. *ζ_K has an analytic continuation to $\mathbb{C} \setminus \{1\}$ and has a simple pole at $s = 1$ with residue*

$$\kappa = \frac{2^{r_1}(2\pi)^{r_2}}{w|d_K|^{1/2}} hR$$

Furthermore, $\zeta_K(1-s) = A(s)\zeta_K(s)$ for some factor $A(s)$ which we're not gonna define.

Remark. The formula for κ is known as the analytic class number formula.

2.4 Dirichlet Characters

We'll work towards finding explicit formulae for the class numbers for some quadratic fields. Let $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 0, 1$ is square-free. If a prime p of $\mathbb{Q}$ splits, then $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ for $\mathfrak{p}_1 \neq \mathfrak{p}_2$ and $N(\mathfrak{p}_i) = p$; If it is inert, then $p\mathcal{O}_K$ is a prime with norm p^2; If it ramifies, then $p\mathcal{O}_K = \mathfrak{p}^2$ for $N(\mathfrak{p}) = p$. So

$$\zeta_K(s) = \prod_{p \text{ split}} \left(1 - \frac{1}{p^s}\right)^{-2} \prod_{p \text{ inert}} \left(1 - \frac{1}{p^{2s}}\right)^{-1} \prod_{p \text{ ramified}} \left(1 - \frac{1}{p^s}\right)^{-1}$$

But each of these products contain a factor of $(1 - p^{-s})^{-1}$. More precisely,

$$\zeta_K(s) = \zeta(s) \prod_{p \text{ prime}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

where

$$\chi(p) = \begin{cases} 1 & \text{if } p \text{ splits} \\ -1 & \text{if } p \text{ is inert} \\ 0 & \text{if } p \text{ ramifies} \end{cases}$$

This is an example of a Dirichlet character. And we'll see that the second factor in this decomposition turns out to be the Euler product of a certain Dirichlet series $L(s, \chi)$.

Definition 2.10. Let m be a natural number. A Dirichlet character modulo m is a homomorphism $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$.

Example 2.1. Let χ be as before, then it (or rather, its restriction) agrees with a Dirichlet character modulo d_K.

Definition 2.11. A Dirichlet character χ modulo m is primitive if it does not factor as $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/m'\mathbb{Z})^\times \to \mathbb{C}^\times$ for some other Dirichlet character $(\mathbb{Z}/m'\mathbb{Z})^\times \to \mathbb{C}^\times$ where $m' \mid m$.

Definition 2.12. If χ is a primitive Dirichlet character modulo m, then this m is called the conductor of χ.

Equivalently: Suppose χ is a Dirichlet character modulo m_0. Then the conductor m of χ is the greatest common divisor of all $m' \mid m_0$ such that χ factors through a Dirichlet character modulo m'.
We can, and always, extend a Dirichlet character χ to a (multiplicative) function $\mathbb{Z} \to \mathbb{C}$ by setting $\chi(n) = \chi(n \bmod m)$ if $\gcd(n, m) = 1$, and $\chi(n) = 0$ otherwise.

Example 2.2. χ as before is such an extension.

Definition 2.13. Write χ_0 for the trivial character (or the principal character) modulo m, which is $\chi_0(n) = 1_{\gcd(m,n)=1}$. For $m = 1$, we just write 1 for χ_0.

Example 2.3. Take $m = 4$. Then there are Dirichlet characters modulo 4 given by χ_0 and

$$\chi_1(n) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod 4 \\ -1 & \text{if } n \equiv 3 \pmod 4 \end{cases}$$

Remark. Suppose we have two Dirichlet characters χ_1, χ_2 modulo m. We can take their product $(\chi_1\chi_2)(n) = \chi_1(n)\chi_2(n)$, which is still a Dirichlet character modulo m. This turns the collection of all Dirichlet characters modulo m into an abelian group with identity χ_0, which we shall denote as $(\mathbb{Z}/m\mathbb{Z})^\times$.
In general, for any finite abelian group A, a character of it is a group homomorphism $A \to \mathbb{C}^\times$. We denote the abelian group of all characters of A by $\widehat{A}$, which is known as the character group (or dual group) of A.

Proposition 2.15. *If A is any finite abelian group, then $\widehat{A} \cong A$.*

Remark. The isomorphism is not canonical, in general.

Proof. Induction on $\#A$. When A is cyclic (say with order m and generator y), $\chi(y)^m = \chi(y^m) = \chi(1) = 1$, so $\chi(y) \in \mu_m(\mathbb{C})$. Conversely, the data of a character of A is essentially the same as the data of a choice $\chi(y) \in \mu_m(\mathbb{C})$. So indeed $\widehat{A} = \{y \mapsto \zeta : \zeta \in \mu_m(\mathbb{C})\} \cong \mu_m(\mathbb{C}) \cong A$.
Suppose A is not cyclic. Then we can write $A = A_1 \times A_2$ where A_1, A_2 are nontrivial. We have homomorphisms $\widehat{A} \to \widehat{A_1} \times \widehat{A_2}, \chi \mapsto (\chi|_{A_1}, \chi|_{A_2})$ and $\widehat{A_1} \times \widehat{A_2} \to \widehat{A}, (\chi_1, \chi_2) \mapsto ((m, n) \mapsto \chi_1(m)\chi_2(n))$, which are mutual inverses. Hence $\widehat{A} \cong \widehat{A_1} \times \widehat{A_2}$, so we are done by induction hypothesis. □

Recall that $(\mathbb{Z}/m\mathbb{Z})^\times$ has order $\phi(m)$ where ϕ is the Euler totient function. So there are exactly $\phi(m)$ Dirichlet characters modulo m. Indeed, $\chi(4) = 2$ so our previous example listed all the Dirichlet characters modulo 4.

Corollary 2.16. *If A is a finite abelian group, then $A \cong \widehat{\widehat{A}}$ canonically via $m \mapsto (\chi \mapsto \chi(m))$.*

Proof. This is an injective map between finite groups of equal size. □

Proposition 2.17 (Orthogonality of Characters)**.** *Let $\chi_1, \chi_2 \in \widehat{A}$ and $a, b \in A$. Then:*
(i)

$$\sum_{a \in A} \chi_1(a)\chi_2(a) = \begin{cases} 0 & \text{if } \chi_1 \neq \chi_2^{-1} \\ |A| & \text{if } \chi_1 = \chi_2^{-1} \end{cases}$$

(ii)

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

Proof. (ii) follows from (i) by the preceding corollary. For (i), we observe that whenever $\chi \in \widehat{A}$ is not equal to χ_0, we can take $b \in A$ such that $\chi(b) \neq 1$. Then

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

And so $\sum_{a \in A} \chi(a) = 0$. Taking $\chi = \chi_1\chi_2$ gives the result. □

2.5 Dirichlet L-Series

Definition 2.14. Let χ be a Dirichlet character modulo m, extended as a function $\mathbb{Z} \to \mathbb{C}$. The Dirichlet L-series associated to χ is $L(\chi, s) = \sum_{n \geq 1} \chi(n) n^{-s}$.

Proposition 2.18. *$L(\chi, s)$ is absolutely convergent on $\{\sigma > 1\}$. Moreover, we have an Euler product*

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

Proof. Exercise. □

Note that we have

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

In particular, $L(\chi_0, s) = \zeta(s) \prod_{p|m}(1 - p^{-s})$.
We can relate these Dirichlet L-series to Dedekind ζ-functions. Let's see how this works in cyclotomic fields first.

Proposition 2.19. *Let $K = \mathbb{Q}(\zeta_m)$, then*

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

Proof. Let p be a (rational) prime and write its decomposition as $p\mathcal{O}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^e$ for $\mathfrak{p}_i$ distinct. Let $f = f_{\mathfrak{p}_1|p}$ be the common inertia degree.
Then $\zeta_K(s)$ contains the factor

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

On the other hand, the product of these Dirichlet L-series contains the factor $\prod_\chi (1 - \chi(p)p^{-s})^{-1}$. This is 1 if $p \mid m$. For $p \nmid m$, note that f is the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$ and $e = 1$. Since $efr = \#(\mathbb{Z}/m\mathbb{Z})^\times = \phi(m)$, $r = \phi(m)/f$ is the index of the subgroup G_p generated by p in $(\mathbb{Z}/m\mathbb{Z})^\times$.
We have an isomorphism $\widehat{G_p} \to \mu_f, \chi \mapsto \chi(f)$ and an exact sequence

$$1 \longrightarrow \widehat{G/G_p} \longrightarrow \hat{G} \longrightarrow \mu_f \longrightarrow 0$$

So we have $r = \#\widehat{G/G_p} = [G : G_p]$ elements in the preimage of $\chi(p)$. Therefore

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

The result follows from taking the product of both sides over all primes. □

Consequently,

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

Since both ζ and ζ_K have simple poles at $s = 1$,

Proposition 2.20. *For every nontrivial Dirichlet character χ has $L(\chi, 1) \neq 0$.*

Theorem 2.21 (Dirichlet)**.** *For any $a \in (\mathbb{Z}/m\mathbb{Z})^\times$, the arithmetic progression of a modulo m contains infinitely many prime numbers.*

Proof. Let χ be a Dirichlet character modulo m. Then on $\{\sigma > 1\}$, we have

$$\begin{aligned}\log L(\chi, s) &= -\sum_{p \text{ prime}} \log(1 - \chi(p)p^{-s}) = \sum_{p \text{ prime}} \sum_{n=1}^{\infty} \frac{\chi(p^n)}{np^n} \\ &= g_\chi(s) + \sum_{p \text{ prime}} \frac{\chi(p)}{p^s}\end{aligned}$$

For some $g_\chi(s)$ holomorphic on $\{\sigma > 1/2\}$. Let's multiply this by $\chi(a^{-1})$ and sum over all characters modulo m. Then we get, for some g holomorphic on $\{\sigma > 1/2\}$,

$$\begin{aligned}\sum_\chi \chi(a^{-1}) \log L(\chi, s) &= g(s) + \sum_\chi \sum_{p \text{ prime}} \frac{\chi(a^{-1}p)}{p^s} \\ &= g(s) + \sum_{b=1}^{m} \sum_\chi \chi(a^{-1}b) \sum_{p \equiv b \pmod m} \frac{1}{p^s} \\ &= g(s) + \sum_{p \equiv a \pmod m} \frac{\phi(m)}{p^s}\end{aligned}$$

Now let $s > 1$ be real. As $s \to 1$, $\log(\chi, s)$ stays bounded for $\chi \neq \chi_0$ since $L(\chi, 1) \neq 0$. But

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

which goes to infinity as $s \to 1$. By our previous computation, this can only happen if we have

$$\lim_{s \to 1} \sum_{p \equiv a \pmod{m}} \frac{\phi(m)}{p^s} = \infty$$

which forces the sum to be infinite. □

2.6 Analytic Class Number Formula, (sort-of) Explained

Now for any number field K and any $s \in \{\sigma > 1\}$, we can write $\zeta_K(s) = \sum_{n \geq 1} j_n n^{-s}$ where $j(n)$ is the number of integral ideals $\mathfrak{a} \leq \mathcal{O}_K$ with $N(\mathfrak{a}) = n$. We may write

$$\zeta_K(s) = h_K \kappa \zeta(s) + \sum_{n=1}^{\infty} \frac{j_n - h_K \kappa}{n^s}$$

The series $\sum_{n \geq 1}(j_n - h_K\kappa)n^{-s}$ converges for $\sigma = 1$ (in fact on $\{\sigma > 1 - [K : \mathbb{Q}]^{-1}\}$). Then $h_K \kappa = \rho$ where $\rho = \lim_{s \to 1} \zeta_K(s)/\zeta(s)$. So let's study this limit by factoring ζ_K more generally.

Suppose $K/\mathbb{Q}$ is abelian. Then $K \subset \mathbb{Q}(\zeta_m)$ for some m. We'll always identify $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ with $(\mathbb{Z}/m\mathbb{Z})^\times$. Let $G = \mathrm{Gal}(K/\mathbb{Q})$ which is a quotient of $(\mathbb{Z}/m\mathbb{Z})^\times$. Taking duals, we can consider $\hat{G}$ as a subgroup of $\widehat{(\mathbb{Z}/m\mathbb{Z})^\times}$.

Adapting the proof of Proposition 2.19 shows that, for $p \nmid m$,

$$\prod_{\chi \in \widehat{G}} \left(1 - \frac{\chi(p)}{p^s}\right) = \left(1 - \frac{1}{p^{fs}}\right)^r = \prod_{\mathfrak{p}|p} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)$$

where f, r are what you think they are.

So for $\sigma > 1$, we have

$$\prod_{\chi \in \widehat{G}} L(\chi, s) = \prod_{p \nmid m} \left(1 - \frac{1}{p^{fs}}\right)^{-r} = \prod_{p \nmid m} \prod_{\mathfrak{p}|p} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}$$

We therefore have a similar factorisation

$$\begin{aligned}\zeta_K(s) &= \prod_{\mathfrak{p}|m} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} \prod_{\chi \in \widehat{G}} L(\chi, s) \\ &= \left(\prod_{p|m} \left(1 - \frac{1}{N(\mathfrak{p})}\right)^{-1}\right) \left(\prod_{p|m} \left(1 - \frac{1}{p^s}\right)\right) \left(\prod_{\chi \neq \chi_0} L(\chi, s)\right) \zeta(s)\end{aligned}$$

Consequently,

Theorem 2.22. *We have*

$$\rho = \prod_{p|m} \left[\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^{f_p}}\right)^{-r_p}\right] \prod_{\chi \in \widehat{G}, \chi \neq \chi_0} L(\chi, 1)$$

Okay, now let's try to compute $L(\chi, 1)$.

Definition 2.15. Let ζ be a primitive m-th root of unity. Then for $k \geq 0$, then k-th Gauss sum is $\tau_k(\chi) = \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(a)\zeta^{ak}$.

Theorem 2.23. *Let χ be a nontrivial Dirichlet character modulo m, then*

$$L(\chi, 1) = -\frac{1}{m} \sum_{k=1}^{m-1} \tau_k(\chi) \log(1 - \zeta^{-k})$$

Proof. For $\sigma > 1$, we have

$$\begin{aligned} L(\chi, s) &= \sum_{n \geq 1} \frac{\chi(n)}{n^s} = \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(a) \sum_{n \geq 1, n \equiv a \pmod m} \frac{1}{n^s} \\ &= \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(a) \sum_{n \geq 1} \frac{1}{n^s} \left(\frac{1}{m} \sum_{k=0}^{m-1} \zeta^{(a-n)k} \right) = \frac{1}{m} \sum_{k=0}^{m-1} \tau_k(\chi) \sum_{n \geq 1} \frac{\zeta^{-nk}}{n^s} \end{aligned}$$

Note that $\tau_0(\chi) = \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(a) = 0$. The Dirichlet series $\sum_{n \geq 1} \zeta^{-nk} n^{-s}$ converges to an analytic function on the half-plane $\sigma > 0$, therefore is continuous at $s = 1$. Its value at $s = 1$ is $-\log(1 - \zeta^{-k})$, so the result follows. □

Lemma 2.24. *Let χ be a primitive character modulo m, then $|\tau_1(\chi)|^2 = m$ and*

$$\tau_k(\chi) = \begin{cases} \overline{\chi(k)}\tau_1(\chi) & \text{if } \gcd(k, m) = 1 \\ 0 & \text{otherwise} \end{cases}$$

Proof. Omitted. □

Definition 2.16. We say χ is even if $\chi(-1) = 1$, and odd if $\chi(-1) = -1$.

Lemma 2.25. *For $0 < k < m$, we have $\log(1 - \zeta^k) = \log 2 + \log \sin(k\pi/m) + (k/m - 1/2)\pi i$.*

Proof. Also omitted. Deal with it. □

Ok now let's compute.

$$\begin{aligned} L(\chi, 1) &= -\frac{1}{m} \sum_{k=1}^{m-1} \tau_k(\chi) \log(1 - \zeta^{-k}) = -\frac{\tau_1(\chi)}{m} \sum_{k \in (\mathbb{Z}/m\mathbb{Z})^\times} \overline{\chi(k)} \log(1 - \zeta^{-k}) \\ &= -\frac{\chi(-1)\tau_1(\chi)}{m} \sum_{k \in (\mathbb{Z}/m\mathbb{Z})^\times} \overline{\chi(k)} \log(1 - \zeta^{k}) \\ &= -\frac{\chi(-1)\tau_1(\chi)}{m} \sum_{k \in (\mathbb{Z}/m\mathbb{Z})^\times} \overline{\chi(k)} \left(\log \sin \frac{k\pi}{m} + \frac{k\pi i}{m} \right) \\ &= \begin{cases} -\tau_1(\chi) m^{-1} \sum_{k \in (\mathbb{Z}/m\mathbb{Z})^\times} \overline{\chi(k)} \log \sin(k\pi/m) & \text{for even } \chi \\ \pi i \tau_1(\chi) m^{-2} \sum_{k \in (\mathbb{Z}/m\mathbb{Z})^\times} \overline{\chi(k)} k & \text{for odd } \chi \end{cases} \end{aligned}$$

Note that for odd χ we have

$$\sum_{k \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(k)k = \frac{m}{\overline{\chi(2)} - 2} \sum_{k \in (\mathbb{Z}/m\mathbb{Z})^\times, k < m/2} \chi(k)$$

with $\chi(2) = 0$ if m is even. Therefore

Theorem 2.26. *Let χ be a primitive character modulo $m \geq 3$, then*

$$|L(\chi,1)| = \begin{cases} 2m^{-1/2}\left|\sum_{k\in(\mathbb{Z}/m\mathbb{Z})^\times, k<m/2} \chi(k)\log\sin(k\pi/m)\right| & \text{for even } \chi \\ \pi|2-\chi(2)|^{-1}m^{-1/2}\left|\sum_{k\in(\mathbb{Z}/m\mathbb{Z})^\times, k<m/2}\chi(k)\right| & \text{for odd } \chi \end{cases}$$

Let $K = \mathbb{Q}(\sqrt{d})$ with $d \neq 0, 1$ square-free. Let $m = |d_K|$, then $K \subset \mathbb{Q}(\zeta_m)$. We now know that $\rho = L(\chi, 1)$ where χ is the unique nontrivial Dirichlet character modulo m corresponding to a character of $\mathrm{Gal}(K/\mathbb{Q})$. For $p \nmid m$, we have

$$\chi(p) = \begin{cases} 1 & \text{if } p \text{ splits} \\ -1 & \text{if } p \text{ inert} \end{cases}$$

This is a primitive character modulo m, which is even if $d > 0$ and odd if $d < 0$.

Theorem 2.27. *In the quadratic case sketched above, we have for $d > 0$,*

$$h_K = \frac{1}{\log\epsilon}\left|\sum_{k\in(\mathbb{Z}/m\mathbb{Z})^\times, k<m/2}\chi(k)\log\sin\frac{k\pi}{m}\right|$$

where ϵ is the fundamental unit; and for $d < 0$ and $d \neq -1, -3$,

$$h_K = \frac{1}{2-\chi(2)}\left|\sum_{k\in(\mathbb{Z}/m\mathbb{Z})^\times, k<m/2}\chi(k)\right|$$

Example 2.4. Let $d = -2$, then $h_K = (1/2)|\chi(1) + \chi(3)| = 1$.

3 Density

3.1 Dirichlet Density

Let K be a number field.

Definition 3.1. Let S be a set of prime ideals. The Dirichlet density of S is

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

provided that it exists.

This provides a way to measure the ratio of the set of primes in S to the set of all primes.

Lemma 3.1. *(i) $d(\mathcal{P}) = 1$ where $\mathcal{P}$ is the set of all primes of K.*
(ii) If $S \subset T$ and $d(S), d(T)$ both exist, then $d(S) \leq d(T)$.
(iii) If $d(S)$ exists, then $0 \leq d(S) \leq 1$.
(iv) If S, T are disjoint and $d(S), d(T)$ both exist, then $d(S \sqcup T) = d(S) + d(T)$.
(v) If S is finite, then $d(S) = 0$.
(vi) If $d(S)$ exists and S, T differ by finitely many elements, then $d(T) = d(S)$.

Proof. Exercise. □

For $\sigma > 1$, we have seen that $\zeta_K(s) = \prod_{\mathfrak{p}}(1-N(\mathfrak{p})^{-s})^{-1}$. Taking logarithms, we get

$$\log \zeta_K(s) = \sum_{\mathfrak{p}} \sum_{n=1}^{\infty} \frac{1}{nN(\mathfrak{p})^{ns}} = \sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s} + \sum_{\mathfrak{p}} \sum_{n=2}^{\infty} \frac{1}{nN(\mathfrak{p})^{ns}}$$

The second term is analytic at $s = 1$.

Definition 3.2. Let f, g be functions defined for $\sigma > 1$. We write $f(s) \sim g(s)$ if $f(s) - g(s)$ has a finite limit as $s \to 1^+$.

So $\log \zeta_K(s) \sim \sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}$. Since $\zeta_K(s)$ has a simple pole at $s = 1$, we can write $\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s} \sim \log(1/(s-1))$. This allows us to write

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

Definition 3.3. A prime $\mathfrak{p}$ of K has degree 1 if its residue class degree is 1. Equivalently, $N(\mathfrak{p})$ is prime.

Lemma 3.2. *Let S be the set of degree 1 primes, then $d(S) = 1$.*

In particular, S is infinite.

Proof.

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

For $\mathfrak{p} \notin S$, $N(\mathfrak{p}) = p^f \geq p^2$ where $(p) = \mathfrak{p} \cap \mathbb{Z}$. There are at most $[K : \mathbb{Q}]$ primes of K lying above any prime of $\mathbb{Q}$, so

$$\left| \sum_{\mathfrak{p} \notin S} \frac{1}{N(\mathfrak{p})^s} \right| \leq [K : \mathbb{Q}] \sum_{p} \frac{1}{p^{2\sigma}}$$

which is bounded as $s \to 1^+$. □

3.2 Frobenius Density Theorem

We will prove the Frobenius density theorem and use it to prove Theorem 1.11. Suppose L/K is a Galois extension. Write $G = \mathrm{Gal}(L/K)$.

Definition 3.4. Let $\sigma \in G$ an element of order n. The division of σ is the set of all elements of G which are conjugate to σ^m for some m coprime to n.

Lemma 3.3. *Let $\sigma \in G$ and write $H = \langle \sigma \rangle$. The number $t = t_\sigma$ of elements in the division of σ is $t = \phi(n)[G : N_G(H)]$.*

Recall that for any finite group G and any $g \in G$, the number of elements in the conjugacy class of g equals $[G : C_G(g)]$.

Proof. For $\gcd(m,n)=1$, we have $C_G(\sigma)=C_G(\sigma^m)$. So σ^m has $[G:C_G(g)]$ conjugates. As m ranges over all integers between 1 and n relatively prime to n, we count $\phi(n)[G:C_G(\sigma)]$ conjugates. They are not all distinct: In fact, an element is counted q times if it is conjugate to q distinct powers $\sigma^m, m \in (\mathbb{Z}/n\mathbb{Z})^\times$. But the number of distinct powers of σ conjugate to σ is exactly the number of distinct automorphisms of H induced by conjugation by elements of G. This is just $[N_G(H):C_G(\sigma)]$. So we conclude the proof. □

Theorem 3.4 (Frobenius Density Theorem)**.** *Fix $\sigma \in G$. Let $S = S_\sigma$ be the set of primes in K such that there is a prime $\mathfrak{P}$ of L lying above it with $(L/K, \mathfrak{P})$ living in the division of σ. Then $d(S_\sigma) = t_\sigma/\#G = t_\sigma/[L:K]$.*

Before proving this, let's first use it to establish Theorem 1.11. We can in fact do something slightly more general.

Theorem 3.5. *Suppose L/K is abelian and $\mathfrak{m}$ is a modulus of K divisible by every ramified prime of K. Then $\Phi_\mathfrak{m} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$ is surjective.*

Proof. Let $\sigma \in \mathrm{Gal}(L/K)$. Since $\mathrm{Gal}(L/K)$ is abelian, the division of σ is simply the set of generators for $\langle\sigma\rangle$.
By the preceding theorem, one can find infinitely many primes $\mathfrak{P}$ in L such that $(L/K, \mathfrak{P})$ generates $\langle\sigma\rangle$. Choose one of them such that its underlying prime in K is not contained in $\mathfrak{m}$. Then $\Phi_\mathfrak{m}(\mathfrak{P}) = \sigma'$ is a generator of $\langle\sigma\rangle$, so σ is also in the image of $\Phi_\mathfrak{m}$. □

Lemma 3.6. *Let S be any set of primes in K whose density exists, then $d(S) = d(S \cap \{\text{degree 1 primes}\})$.*

Proof. We have $\sum_{\mathfrak{p}\in S \text{ degree } 1} N(\mathfrak{p})^{-s} \sim 0$ by the proof of Lemma 3.2 □

Proof of Theorem 3.4. Induction on the order n of σ. Suppose first that $n=1$. Then S_σ is the set of primes that split completely in L. Let S_L be the set of primes in L lying above some prime in S_σ. Each prime $\mathfrak{p}$ in S has exactly $[L:K] = \#G$ primes in S_L above it, and any such prime has norm $\mathfrak{p}$. So we have

$$\sum_{\mathfrak{P}\in S_L} N_{L/\mathbb{Q}}(\mathfrak{P})^{-1} = \sum_{\mathfrak{P}\in S_L} N_{K/\mathbb{Q}}(N_{L/K}(\mathfrak{P}))^{-1} = (\#G)\sum_{\mathfrak{p}\in S_\sigma} N_{K/\mathbb{Q}}(\mathfrak{p})^{-1}$$

Let S_L^1 be the set of primes of L with degree 1 over $\mathbb{Q}$. Then $S_L^1 \subset S_L$ and so $d(S_L) = 1$. So we arrive at $(\#G)\sum_{\mathfrak{p}\in S_\sigma} N_{K/\mathbb{Q}}(\mathfrak{p})^{-1} \sim -\log(s-1)$ and therefore $d(S_\sigma) = (\#G)^{-1}$.
For general n, we do the following: For each divisor d of n, we write t_d for the number of elements in the division of σ^d. Write $S_d = S_{\sigma^d}$, in particular $S_1 = S_\sigma$. By the induction hypothesis, $d(S_d) = t_d/\#G$ for all $d > 1$.
Write $E = L^H$. The primes $\mathfrak{p}$ of K with at least one degree 1 prime in E lying above it are exactly those lying under a prime $\mathfrak{P}$ of L with $(L/K, \mathfrak{P})$ conjugate to some power of σ, i.e. those living in S_d for some divisor $d \mid n$.
Next let S_E be the primes of E having inertia degree 1 over K. For each $\mathfrak{p} \in S_d$, let $n(\mathfrak{p})$ be the number of primes in S_E lying above $\mathfrak{p}$. So $\mathfrak{p} \in S_d$ is the norm of

exactly $n(\mathfrak{p})$ distinct primes in S_E. Since S_E contains all degree 1 primes of E over $\mathbb{Q}$, we have $d(S_E) = 1$. So

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

Galois theory tells us that, for any prime $\mathfrak{p} \in S_d$, $n(\mathfrak{p})$ is the number of distinct cosets $H\tau_1$ such that $H\tau_i\sigma^d = H\tau_i$, or equivalently, $\tau_i\sigma^d\tau_i^{-1} \in H$. But H is cyclic, so in fact $\tau_i \in N_G(\langle\sigma^d\rangle)$. Hence $n(\mathfrak{p}) = [N_G(\langle\sigma^d\rangle) : H]$.
By the induction hypothesis, we obtain

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

But $t_d = \phi(n/d)[G : N_G(\langle\sigma^d\rangle)]$, so this is in fact

$$\begin{aligned} \left(-1 + \sum_{d|n, d \neq 1} \frac{1}{n} \phi\left(\frac{n}{d}\right) \right) \log(s-1) &= \left(-1 - \frac{\phi(n)}{n} + \frac{1}{n} \sum_{e|n} \phi(e) \right) \log(s-1) \\ &= -\frac{\phi(n)}{n} \log(s-1) \end{aligned}$$

Therefore

$$\sum_{\mathfrak{p} \in S_1} N(\mathfrak{p})^s \sim \frac{-\phi(n)}{n[N_G(H) : H]} \log(s-1) = \frac{-t}{\#G} \log(s-1)$$

which is what we wanted. □

Corollary 3.7. *Suppose $G = \mathrm{Gal}(L/K)$ is cyclic of order n, and let $d \mid n$. Write S_d for the set of prime ideals in $\mathcal{O}_K$ having exactly d primes lying above it in $\mathcal{O}_L$. Then S_d has Dirichlet density $\phi(n/d)/n$. In particular, there are infinitely many primes in K which are inert in L.*

Proof. We are allowed to ignore the primes which ramify in L since there are only finitely many of them. A prime $\mathfrak{p}$ of $\mathcal{O}_K$ has d factors in L if and only if $\sigma = (L/K, \mathfrak{p})$ has order n/d. The number of element in G with order n/d is $\phi(n/d)$ since G is cyclic. By Theorem 3.4, $d(S_d) = \phi(n/d)/\#G = \phi(n/d)/n$. □

Theorem 3.8. *Let K be a number field with a modulus $\mathfrak{m}$. Let H be a congruence subgroup for $\mathfrak{m}$. Let S be the set of prime ideals in H. If S has a Dirichlet density, then this density is at most $1/[I_K(\mathfrak{m}) : H]$.*

Remark. We are not going to prove this due to time constraints, but the technique is basically to look at characters of the group $I_K(\mathfrak{m})/H$.

Theorem 3.9 (First Fundamental Inequality of Class Field Theory)**.** *Let L/K be a Galois extension of number fields and suppose $\mathfrak{m}$ is a modulus of K. Let $L = I_L(\mathfrak{m})$ be the subgroup of I_L generated by all primes $\mathfrak{P}$ of L with $\mathfrak{P} \cap \mathcal{O}_K \in I_K(\mathfrak{m})$. Then*

$$[I_K(\mathfrak{m}) : N_{L/K}(I_L(\mathfrak{m}))P_K(\mathfrak{m})] \leq [L : K]$$

Proof. Let $H = N_{L/K}(I_L(\mathfrak{m}))P_K(\mathfrak{m})$. With finitely many exceptions, the primes of K split completely in L are in $N_{L/K}(I_K(\mathfrak{m}))$. The density of this set is $1/[L:K]$ by Theorem 3.4. So we are done by the preceding theorem. □

Remark. The other direction is known as the second fundamental inequality.

3.3 Chebotarev Density Theorem

We can refine Theorem 3.4 to get something stronger.

Theorem 3.10 (Chebotarev)**.** *Let L/K be Galois and $G = \mathrm{Gal}(L/K)$. Fix $\sigma \in G$ and suppose σ has c many conjugates in G. Then the set of primes $\mathfrak{p}$ of K unramified in L with $(L/K, \mathfrak{p}) = \sigma$ has density $c/[L:K]$.*

Remark. We don't need L/K to be abelian. In the non-abelian case, we write $(L/K, \mathfrak{p})$ to denote the conjugacy class of $(L/K, \mathfrak{P})$ for any $\mathfrak{P} \mid \mathfrak{p}$.

Corollary 3.11. *Let L/K be abelian and suppose $\mathfrak{m}$ is a modulus of K divisible by all primes of K that ramify in L. For $\sigma \in G$, the set S of primes $\mathfrak{p} \nmid \mathfrak{m}$ such that $(L/K, \mathfrak{p}) = \sigma$ has density $d(S) = 1/[L:K]$. In particular, S is infinite.*

Remark. One can also use this to show Theorem 1.11.

Proposition 3.12. *For any Galois extension L/K, there are infinitely many primes of K that split completely in L.*

Proof. Apply Theorem 3.10 to $1 \in G$. The primes $\mathfrak{p} \leq \mathcal{O}_K$ such that $(L/K, \mathfrak{p}) = 1$ has density $1/[L:K]$. And $(L/K, \mathfrak{p}) = 1$ iff $\mathfrak{p}$ splits completely in L. □

In fact, the primes that split completely in L characterises the extension L/K completely.

Definition 3.5. Suppose S, T are two sets, we write $S \dot{\subset} T$ if $S \subset T \cup \Sigma$ for some finite set Σ. We write $S \doteq T$ if $S \dot{\subset} T$ and $T \dot{\subset} S$.

Given any finite extension L/K, we denote by $S_{L/K}$ the set of primes $\mathfrak{p} \leq \mathcal{O}_K$ that split completely in L.

Theorem 3.13. *Suppose L, M are finite extensions of K, then:*
(i) If M is Galois over K, then $L \subset M$ iff $S_{M/K} \dot{\subset} S_{L/K}$.
(ii) If L is Galois over K, then $L \subset M$ iff $\tilde{S}_{M/K} \dot{\subset} S_{L/K}$, where $\tilde{S}_{M/K}$ is the set of primes in K unramified in M such that $f_{\mathfrak{P}|\mathfrak{p}} = 1$ for some $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_M$.

Proof. We first show (ii). The "only if" part is left as exercise. For the "if" part, let N be a Galois extension of K containing both L and M. To show $L \subset M$, it suffices to prove that $\mathrm{Gal}(N/M) \subset \mathrm{Gal}(N/L)$.
For $\sigma \in \mathrm{Gal}(N/M)$, let's show that $\sigma|_L$ is the identity. By Theorem 3.10, we can find a prime $\mathfrak{p}$ of K unramified in N such that $(N/K, \mathfrak{P}) = \sigma$ for some $\mathfrak{P} \leq \mathcal{O}_N$ lying above $\mathfrak{p}$.
We claim $\mathfrak{p} \in \tilde{S}_{M/K}$. Indeed, let $\mathfrak{P}_M = \mathfrak{P} \cap \mathcal{O}_M$. Then for any $\alpha \in \mathcal{O}_M$ we have $\alpha \equiv \sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}_M}$, where the first congruence is due to σ being the identity on M. Consequently, $\mathcal{O}_M/\mathfrak{P}_M \cong \mathcal{O}_K/\mathfrak{p}$. Hence $f_{\mathfrak{P}_M|\mathfrak{p}} = 1$.
By Theorem 3.10, one of these choices for $\mathfrak{p}$ lives in $S_{L/K}$. Hence $1 = (L/K, \mathfrak{p}) = (N/K, \mathfrak{P})_L = \sigma|_L$.

Let's now show (i). Let L' be the Galois closure of L over K, then $L \subset M$ iff $L' \subset M$. Also, a prime splits completely in L if and only if it splits completely in L'. As M is Galois over K, $\tilde{S}_{M/K} = S_{M/K}$, so we are done by (ii). □

Corollary 3.14. *Let L and M be Galois extensions of K. Then:*
(i) $L \subset M$ iff $S_{M/K} \dot{\subset} S_{L/K}$.
(ii) $L = M$ iff $S_{M/K} \doteq S_{L/K}$.

Theorem 3.15. *Let L/K be abelian and let $\mathfrak{m}$ be a modulus divisible by $\mathfrak{f}_{L/K}$, then* $\ker \Phi_{\mathfrak{m}} \subset T_{L/K}(\mathfrak{m}) = N_{L/K}(I_L(\mathfrak{m}))P_K(\mathfrak{m})$.

Proof. Since $\mathfrak{f}_{L/K} \mid \mathfrak{m}$, we know that $P_K(\mathfrak{m}) \subset \ker \Phi_{\mathfrak{m}} \subset I_K(\mathfrak{m})$. For any $\mathfrak{a} \in I_K(\mathfrak{m})$, the corresponding $(L/K, \mathfrak{a})$ only depends on the class of $\mathfrak{a}$ modulo $P_K(\mathfrak{m})$. By Theorem 3.10, for any $\sigma \in \mathrm{Gal}(K_{\mathfrak{m}}/K)$ there are infinitely many primes $\mathfrak{p}$ in $\mathcal{O}_K$ such that $(K_{\mathfrak{m}}/K, \mathfrak{p}) = \sigma$. So we can always choose $\mathfrak{p}$ such that it does not divide $\mathfrak{m}$.
Since $I_K(\mathfrak{m})/P_K(\mathfrak{m}) \cong \mathrm{Gal}(K_{\mathfrak{m}}/K)$, every $\mathfrak{a} \in I_K(\mathfrak{m})$ is equivalent to a prime $\mathfrak{p}$ modulo $P_K(\mathfrak{m})$.
Suppose $\mathfrak{p}$ is a prime of $\mathcal{O}_K$ residing in $\ker \Phi_{\mathfrak{m}}$. Then $(L/K, \mathfrak{p}) = 1$, in particular $\mathfrak{p}$ splits completely with inertia degrees 1.
For any $\mathfrak{P} \mid \mathfrak{p}$, we have $N_{L/K}\mathfrak{P} = \mathfrak{p}$, so $\mathfrak{p} \in N_{L/K}(I_L(\mathfrak{m})) \subset T_{L/K}(\mathfrak{m})$. □

4 Idèles and Adèles

4.1 Restricted Product Topology

Before you ask, idèle is an abbreviation of "ideal element" and adèle an abbreviation of "additive idèle".
Let K be a number field. Recall that any absolute value on K is equivalent to either $|\cdot|_{\mathfrak{p}}$ for some (finite) prime $\mathfrak{p} \leq \mathcal{O}_K$, or $|\cdot|_\sigma$ for some embedding $K \hookrightarrow \mathbb{R}, \mathbb{C}$ ("infinite primes").
Let $\mathfrak{p}$ be a prime of K, finite or infinite. Let $K_{\mathfrak{p}}$ be the completion of K at $\mathfrak{p}$ (i.e. with respect to $|\cdot|_{\mathfrak{p}}$). This is either a p-adic field for some prime p, $\mathbb{R}$, or $\mathbb{C}$.
For a non-Archimedean valued field F, the valuation ring of F is $\mathcal{O}_F = \{x \in F : |x|_F \leq 1\}$. This is an open subring of F whose units are $\mathcal{O}_F^\times = \{x \in F : |x| = 1\}$, and $\mathfrak{m}_F = \mathcal{O}_F \setminus \mathcal{O}_F^\times$ is the unique maximal ideal of $\mathcal{O}_F$.
The idea of idèles is to study a number field K using local fields associated to it. It is certainly useful, then, to embed K in these $K_{\mathfrak{p}}$ simultaneously. But $\prod_{\mathfrak{p}} K_{\mathfrak{p}}$ is not exactly nice topologically (it's not locally compact, for example). So we need to adjust it somehow, by introducing the restricted product topology.

Definition 4.1. Let $\{X_i\}_{i \in I}$ be a family of topological spaces indexed by some $i \in I$. Let $\{U_i\}_{i \in I}$ of open sets $U_i \subset X_i$. The restricted product of $\{X_i\}_{i \in I}$ with respect to $\{U_i\}_{i \in I}$ is

$$\underline{\prod}(X_i, U_i) = \{(x_i) : x_i \in U_i \text{ for all but finitely many } i \in I\} \subset \prod X_i$$

with a basis for its topology given by $\prod_i V_i$ for $V_i \subset X_i$ open for all $i \in I$ and $V_i = U_i$ for all but finitely many $i \in I$.

This is in general not the same as the subspace topology this inherits from the product topology. It has more open sets that that.
When $U_i = X_i$, the restricted product is just the product.

Proposition 4.1. *Let $\{X_i\}_{i\in I}$ be a family of locally compact topological spaces and $U_i \subset X_i$ is a family of open subsets, all but finitely many of which are compact. Then $\underline{\prod}(X_i, U_i)$ is locally compact.*

Proof. Allegedly this is not a topology course. □

4.2 The Ring of Adèles and the Group of Idèles

Definition 4.2. An adèle of K is a family $\alpha = (\alpha_\mathfrak{p})$ of elements with $\alpha_\mathfrak{p} \in K_\mathfrak{p}$, where $\mathfrak{p}$ runs through all primes of K, finite or infinite, and $\alpha_\mathfrak{p}$ is integral in $K_\mathfrak{p}$ for all but finitely many $\mathfrak{p}$.
The ring of adèles $\mathbb{A}_K$ of K is the topological ring

$$\mathbb{A}_K = \left\{(\alpha_\mathfrak{p}) \in \prod_\mathfrak{p} K_\mathfrak{p} : \alpha_\mathfrak{p} \in \mathcal{O}_{K_\mathfrak{p}} \text{ for all but finitely many } \mathfrak{p}\right\} = \underline{\prod}(K_\mathfrak{p}, \mathcal{O}_{K_\mathfrak{p}})$$

where, if $\mathfrak{p}$ is infinite, we set $\mathcal{O}_{K_\mathfrak{p}} = K_\mathfrak{p}$.

This is a subset of $\prod_\mathfrak{p} K_\mathfrak{p}$, but not a topological subspace since we are putting on $\mathbb{A}_K$ the restricted product topology.
Notationally, for $\alpha \in \mathbb{A}_K$, we write $\alpha_\mathfrak{p}$ for its projection to $K_\mathfrak{p}$. $\mathbb{A}_K$ is made into a ring by componentwise addition and multiplication.

Example 4.1. Let $K = \mathbb{Q}$. Then

$$\begin{aligned}\mathbb{A}_\mathbb{Q} &= \mathbb{R} \times \left\{(\alpha_p) \in \prod_{p \text{ prime}} \mathbb{Q}_p : \alpha_p \in \mathbb{Z}_p \text{ for almost all } p\right\} \\ &= \bigcup_{S \text{ finite set of primes}} \mathbb{R} \times \prod_{p\in S} \mathbb{Q}_p \times \prod_{p\notin S} \mathbb{Z}_p\end{aligned}$$

as rings.

Proposition 4.2. *$\mathbb{A}_K$ is locally compact and Hausdorff.*

Proof. We know it's locally compact from Proposition 4.1. It is Hausdorff since $\prod_\mathfrak{p} K_\mathfrak{p}$ is Hausdorff and $\mathbb{A}_\mathbb{Q}$ has even more open sets than the subspace topology. □

Definition 4.3. Let S be a finite set of primes in S. The ring of S-adèles is

$$\mathbb{A}_{K,S} = \prod_{\mathfrak{p}\in S} K_\mathfrak{p} \times \prod_{\mathfrak{p}\notin S} \mathcal{O}_{K_\mathfrak{p}} \subset \mathbb{A}_K$$

So $\mathbb{A}_K$ is the union of all $\mathbb{A}_{K,S}$.
The canonical embeddings $K \hookrightarrow K_\mathfrak{p}$ induces a canonical embedding $K \hookrightarrow \mathbb{A}_K$ (since every element of K lives in $\mathcal{O}_{K_\mathfrak{p}}$ for all but finitely many $\mathfrak{p}$). Its image is known as the subring of principal adèles.
We want to set the group of idèles in K to be the unit group $\mathbb{A}_K^\times \subset \mathbb{A}_K$. As a subspace of $\mathbb{A}_K$, this is not a topological group, so we put a different topology on it by giving it the restricted product topology by identifying it as $\underline{\prod}(K_\mathfrak{p}^\times, \mathcal{O}_\mathfrak{p}^\times)$. Now it is a topological group.

Definition 4.4. The group $\mathbb{I}_K$ of idèles is the topological group $\underline{\prod}(K_\mathfrak{p}^\times, \mathcal{O}_\mathfrak{p}^\times)$ under componentwise multiplication.

Proposition 4.3. *$\mathbb{I}_K$ is locally compact and Hausdorff.*

Proof. Mutatis mutandis. □

We similarly have an embedding $K^\times \to \mathbb{I}_K$. Elements of its image are called principal idèles.

Definition 4.5. For any finite set S of primes, the group of S-idèles is the subgroup

$$\mathbb{I}_{K,S} = \prod_{\mathfrak{p}\in S} K_\mathfrak{p}^\times \times \prod_{\mathfrak{p}\notin S} \mathcal{O}_{K_\mathfrak{p}}^\times \subset \mathbb{I}_K$$

So $\mathbb{I}_K$ is the union of all $\mathbb{I}_{K,S}$.

4.3 The Idèle Class Group

Let K be a number field.

Definition 4.6. The idèle class group C_K of K is the quotient $\mathbb{I}_K/K^\times$, where $K^\times$ is viewed as the subgroup of $\mathbb{I}_K$ consisting of principal idèles.

We have a surjective homomorphism $\mathbb{I}_K \to I_K$ sending each idèle α to

$$(\alpha) = \prod_{\mathfrak{p} \text{ finite prime}} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})}$$

This is continuous for the discrete topology on I_K, and its kernel $\mathbb{I}_{K,S_\infty}$ where S_∞ is the set of infinite primes in K.
Note that $\mathbb{I}_{K,S_\infty}K^\times$ is the preimage of P_K under this map, so we obtain a surjective homomomrphism $C_K \to \mathrm{Cl}(K)$ with kernel $\mathbb{I}_{K,S_\infty}K^\times$ and

Proposition 4.4. $\mathbb{I}_K/(\mathbb{I}_{K,S_\infty}K^\times) \cong \mathrm{Cl}(K)$.

Sadly (or not), C_K is usually infinite. However, since $\mathrm{Cl}(K)$ is finite, we can enlarge S_∞ to a set S which contains enough primes to obtain $\mathbb{I}_K = \mathbb{I}_{K,S}K^\times$.

Proposition 4.5. *For a sufficiently large (finite) set S of primes in K, we have $\mathbb{I}_K = \mathbb{I}_{K,S}K^\times$.*

Proof. Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ be integral ideals representing the classes of I_K/P_K. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be all their prime factors. Then just take S to be any set of primes containing all the infinite primes and all these $\mathfrak{p}_i$.
To see such an S works, consider the isomorphism $\mathbb{I}_K/\mathbb{I}_{K,S_\infty} \cong I_K$. For $\alpha \in \mathbb{I}_K$, the corresponding ideal (α) belong to $\mathfrak{a}_i P_K$ for some i, i.e. $(a) = \mathfrak{a}_i(a)$ for some principal ideal (a). Then the idèle $\alpha' = \alpha a^{-1}$ is mapped to the ideal $\mathfrak{a}_i$.
Since the primes occuring in $\mathfrak{a}_i$ are in S, we have $v_\mathfrak{p}(\alpha'_\mathfrak{p}) = 0$ for all $\mathfrak{p} \notin S$, i.e. $\alpha' \in \mathbb{I}_{K,S}$. So $\alpha \in \mathbb{I}_{K,S}K^\times$. □

Proposition 4.6. *$K^\times$ is a discrete subgroup of $\mathbb{I}_K$.*

Recall the product formula: For any $\alpha \in K^\times$, we have $\prod_\mathfrak{p} |\alpha|_\mathfrak{p} = 1$.

Proof. It suffices to show that the identity $1 \in K^\times \subset \mathbb{I}_K$ has a neighbourhood containing no other elements of $K^\times$. We take the neighbourhood to be $U = \{\alpha \in \mathbb{I}_K : |\alpha_\mathfrak{p}|_\mathfrak{p} = 1 \text{ for finite } \mathfrak{p}, |\alpha_\mathfrak{p} - 1|_\mathfrak{p} < 1 \text{ for infinite } \mathfrak{p}\}$.
Suppose $x \in U \setminus \{1\}$ is a principal idèle, then $1 = \prod_\mathfrak{p} |x-1|_\mathfrak{p} < \prod_{\mathfrak{p} \text{ finite}} |x-1| \leq \prod_{\mathfrak{p} \text{ finite}} \max\{|\alpha_\mathfrak{p}|_\mathfrak{p}, 1\} = 1$, contradiction. □

Corollary 4.7. *$K^\times \subset \mathbb{I}_K$ is a closed subgroup, and the quotient topology on C_K is Hausdorff and locally compact.*

Definition 4.7. The idèle norm of $\alpha \in \mathbb{I}_K$ is the real number $|\alpha| = N(\alpha) = \prod_\mathfrak{p} |\alpha_\mathfrak{p}|_\mathfrak{p}$. This defines a homomorphism $\mathbb{I}_K \to \mathbb{R}_+$. We write $\mathbb{I}_K^0$ for its kernel, which contains $K^\times$ by the product formula. So we get a map $N : C_K \to \mathbb{R}_+$. Write C_K^0 for its kernel.

Proposition 4.8. *C_K^0 is compact.*

Proof. Omitted (meh). □

As we do with all the statement we don't prove, we are gonna dig so deep into its applications and make you wonder why the hell didn't we prove it.
Anyways,

Definition 4.8. Let S be a finite set of primes. The ring of S-integers is the subring $\mathcal{O}_{K,S} = \{x \in K : \forall \mathfrak{p} \notin S, x \in \mathcal{O}_{K_\mathfrak{p}}\}$.

Now suppose S contains all infinite primes.

Corollary 4.9. *The group $\mathcal{O}_{K,S}^\times$ of S-units is a finitely generated abelian group of rank $\#S - 1$.*

When $S = S_\infty$, we recover the usual Dirichlet unit theorem.

Sketch of proof. Consider the map $\lambda_S : \mathbb{I}_K \to \prod_{\mathfrak{p} \in S} \mathbb{R}, \alpha \mapsto (\log |\alpha_\mathfrak{p}|_\mathfrak{p})_{\mathfrak{p} \in S}$ Using the product formula, one can show that $\lambda_S(\mathcal{O}_{K,S}^\times) \subset H = \{(\alpha_\mathfrak{p})_{\mathfrak{p} \in S} : \sum_{\mathfrak{p} \in S} \alpha_\mathfrak{p} = 0\}$. Due to the compactness of C_K^0, $\ker \lambda_S \cap \mathcal{O}_{K,S}^\times$ is finite and $\lambda_S(\mathcal{O}_{K,S}^\times)$ is a lattice on the hyperplane H. □

For each $\mathfrak{p}$, consider the homomorphism $n_\mathfrak{p} : K_\mathfrak{p}^\times \to \mathbb{I}_K$ with

$$(n_\mathfrak{p}(x))_\mathfrak{q} = \begin{cases} 1 & \text{if } \mathfrak{q} \neq \mathfrak{p} \\ x & \text{if } \mathfrak{q} = \mathfrak{p} \end{cases}$$

Write $\bar{n}_\mathfrak{p}$ for the same map but now with target C_K.

Proposition 4.10. *$C_K \cong C_K^0 \times \mathbb{R}_+$.*

Proof. It suffices to show that the group extension

$$1 \longrightarrow C_K^0 \longrightarrow C_K \xrightarrow{N} \mathbb{R}_+ \longrightarrow 0$$

has a splitting, i.e. a section $\mathbb{R}_+ \to C_K$ of N.
Choose an infinite prime $\mathfrak{p}$ and consider the embedding $\bar{n}_\mathfrak{p} : K_\mathfrak{p}^\times \to C_K$. As $\mathfrak{p}$ is infinite, $K_\mathfrak{p}^\times$ contains a copy of $\mathbb{R}_+$.
If $\mathfrak{p}$ is real, then the restriction of $\bar{n}_\mathfrak{p}$ to $\mathbb{R}_+$ just works. If $\mathfrak{p}$ is complex, then $N(\bar{n}_\mathfrak{p}(x)) = x^2$ for any $x \in \mathbb{R}_+$, so $x \mapsto \bar{n}_\mathfrak{p}(\sqrt{x})$ is a splitting. □

Corollary 4.11. $\mathrm{Cl}(K)$ *is finite.*

Proof. We have a surjective map $\mathbb{I}_K \to I_K$ which, as one can show, is also surjective as a map $\mathbb{I}_K^0 \to I_K$. This is continuous for the discrete topology on I_K.
As $K^\times$ gets mapped into P_K, $\mathrm{Cl}(K)$ is the continuous image of C_K^0, which is compact. Hence it is finite since it is also discrete. □

4.4 Idèles and Moduli

For a finite prime $\mathfrak{p}$, the units over $\mathfrak{p}$ are $\mathcal{O}_{K_\mathfrak{p}}^\times$. For an infinite prime $\mathfrak{p}$, let's be reminded that its group of units is just $\mathcal{O}_{K_\mathfrak{p}}^\times = K_\mathfrak{p}^\times$ since we have decreed $\mathcal{O}_{K_\mathfrak{p}} = K_\mathfrak{p}$.
Write

$$U_\mathfrak{p}^{r_\mathfrak{p}} = \begin{cases} \mathcal{O}_{K_\mathfrak{p}}^\times & \mathfrak{p} \text{ finite, } r_\mathfrak{p} = 0 \\ 1 + \mathfrak{p}^{r_\mathfrak{p}} & \mathfrak{p} \text{ finite, } r_\mathfrak{p} > 0 \\ \mathbb{R}^\times = K_\mathfrak{p}^\times & \mathfrak{p} \text{ real, } r_\mathfrak{p} = 0 \\ \mathbb{R}_+ \subset K_\mathfrak{p}^\times & \mathfrak{p} \text{ real, } r_\mathfrak{p} = 1 \\ \mathbb{C}^\times = K_\mathfrak{p}^\times & \mathfrak{p} \text{ complex} \end{cases}$$

We often abbreviate $U_\mathfrak{p}^0 = U_\mathfrak{p}$.
For $\alpha_\mathfrak{p} \in K_\mathfrak{p}^\times$, we write $\alpha_\mathfrak{p} \equiv 1 \pmod{\mathfrak{p}^{r_\mathfrak{p}}}$ if $\alpha_\mathfrak{p} \in U_\mathfrak{p}^{r_\mathfrak{p}}$. This is the ordinary congruence condition if $\mathfrak{p}$ is finite and $r_\mathfrak{p} > 0$. If $\mathfrak{p}$ is finite but $r_\mathfrak{p} = 0$, this means that $\alpha_\mathfrak{p} \in \mathcal{O}_{K_\mathfrak{p}}^\times$. If $\mathfrak{p}$ is real and $r_\mathfrak{p} = 1$, then this is the positivity condition $\alpha_\mathfrak{p} > 0$. For other values of $\mathfrak{p}$, this imposes no restrictions.
For any modulus $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{r_\mathfrak{p}}$ of K and idèle $\alpha \in \mathbb{I}_K$, we write $\alpha \equiv 1 \pmod{\mathfrak{m}}$ if $\alpha_\mathfrak{p} \equiv 1 \pmod{\mathfrak{p}^{r_\mathfrak{p}}}$ for all $\mathfrak{p}$.

Definition 4.9. $\mathbb{I}_K(\mathfrak{m}) = \{\alpha \in \mathbb{I}_K : \alpha \equiv 1 \pmod{\mathfrak{m}}\}$.

Then $\mathbb{I}_K(\mathfrak{m}) = \prod_\mathfrak{p} U_\mathfrak{p}^{r_\mathfrak{p}} \subset \mathbb{I}_K$ (as sets). If $\mathfrak{m} = 1$, then $\mathbb{I}_K(1) = \mathbb{I}_{K,S_\infty}$.

Definition 4.10. $C_K(\mathfrak{m}) = \mathbb{I}_K(\mathfrak{m})K^\times/K^\times \subset C_K$ is the congruence subgroup modulo $\mathfrak{m}$ of C_K. $C_K/C_K(\mathfrak{m})$ is called the ray class group modulo $\mathfrak{m}$.

We will show that in fact $C_K/C_K(\mathfrak{m}) \cong I_K(\mathfrak{m})/P_K(\mathfrak{m})$. When $\mathfrak{m} = 1$, this is clear: $C_K/C_K(1) = (\mathbb{I}_K/K^\times)/(\mathbb{I}_{K,S_\infty}K^\times/K^\times) \cong \mathbb{I}_K/\mathbb{I}_{K,S_\infty}K^\times \cong \mathrm{Cl}(K)$.

Proposition 4.12. *The closed subgroups of finite index of C_K are precisely those containing $C_K(\mathfrak{m})$ for some modulus $\mathfrak{m}$.*

Proof. Note first that $C_K(\mathfrak{m})$ is open in C_K since it is the image of $\mathbb{I}_K(\mathfrak{m})$ under the quotient map, and $\mathbb{I}_K(\mathfrak{m}) = \prod_\mathfrak{p} U_\mathfrak{p}^{r_\mathfrak{p}}$ is open in $\mathbb{I}_K$. Now, we claim that $C_K(\mathfrak{m})$ also has finite index. This would imply that $C_K(\mathfrak{m})$ is a closed subgroup of finite index, since C_K is a topological group. It also follows that any subgroup containing $C_K(\mathfrak{m})$ is closed of finite index, since any such subgroup is a union of cosets of $C_K(\mathfrak{m})$.
Let's show the claim. Note first that $\mathbb{I}_K(\mathfrak{m}) \subset \mathbb{I}_{K,S_\infty}$. We have seen that $[C_K : \mathbb{I}_{K,S_\infty}K^\times/K^\times] = [C_K : C_K(1)] = \#\,\mathrm{Cl}(K)$ is finite. So it suffices to show the finiteness of $[\mathbb{I}_{K,S_\infty}K^\times/K^\times : C_K(\mathfrak{m})] = [\mathbb{I}_{K,S_\infty}K^\times : \mathbb{I}_K(\mathfrak{m})K^\times]$. This of course is at most

$$[\mathbb{I}_{K,S_\infty} : \mathbb{I}_K(\mathfrak{m})] = \prod_{\mathfrak{p} \text{ finite}} [U_\mathfrak{p} : U_\mathfrak{p}^{r_\mathfrak{p}}] \prod_{\mathfrak{p} \text{ infinite}} [K_\mathfrak{p}^\times : U_\mathfrak{p}^{r_\mathfrak{p}}]$$

which is finite.
Now suppose $N \subset C_K$ is any closed subgroup with finite index. Then N is also open. Thus the preimage J of N in $\mathbb{I}_K$ is open and therefore it contains a subgroup of the form $W = \prod_{\mathfrak{p}\in S} W_\mathfrak{p} \times \prod_{\mathfrak{p}\notin S} U_\mathfrak{p}$ where S is a finite set of primes containing all infinite primes, and $W_\mathfrak{p}$ is an open neighbourhood of $1 \in K_\mathfrak{p}^\times$.
If $\mathfrak{p} \in S$ is finite, $W_\mathfrak{p}$ can be chosen to be $U_\mathfrak{p}^{r_\mathfrak{p}}$ for some $r_\mathfrak{p}$ since $\{U_\mathfrak{p}^r\}_r$ form a fundamental system of neighbourhoods of $1 \in K_\mathfrak{p}^\times$. If $\mathfrak{p} \in S$ is infinite, then the open set $W_\mathfrak{p}$ generates $K_\mathfrak{p}^\times$, or $\mathbb{R}_+$ if $\mathfrak{p}$ is real. Hence the subgroup of J generated by W has the form $\mathbb{I}_K(\mathfrak{m})$ for some $\mathfrak{m}$, therefore N contains $\mathbb{I}_K(\mathfrak{m})K^\times/K^\times$. □

4.5 Idèles meet Field Extensions

We study the behaviour of idèles (and idèle classes) when we pass through a finite extension L/K oif number fields.
If $\mathfrak{p}$ is a prime of K and $\mathfrak{P}$ is a prime of L lying above it, we write $\mathfrak{P} \mid \mathfrak{p}$. We can embed $\mathbb{I}_K$ into $\mathbb{I}_L$ by identifying each $\alpha \in \mathbb{I}_K$ with $\alpha' = (\alpha'_\mathfrak{P})$ where $\alpha'_\mathfrak{P} = \alpha_\mathfrak{p} \in K_\mathfrak{p} \subset L_\mathfrak{P}$ whenever $\mathfrak{P} \mid \mathfrak{p}$. From now on, we regard $\mathbb{I}_K$ as a subgroup of $\mathbb{I}_L$. Note that $\alpha = (\alpha_\mathfrak{P}) \in \mathbb{I}_L$ belongs to $\mathbb{I}_K$ if and only if:
(i) $\alpha_\mathfrak{P} \in K_\mathfrak{p}$ whenever $\mathfrak{P} \mid \mathfrak{p}$.
(ii) For any $\mathfrak{P}_1, \mathfrak{P}_2$ lying above the same prime $\mathfrak{p}$, we have $\alpha_{\mathfrak{P}_1} = \alpha_{\mathfrak{P}_2}$.
Now suppose L/K is Galois with $\mathrm{Gal}(L/K) = G$. Then $\mathbb{I}_L$ is a G-module. Indeed, any $\sigma \in G$ induces a canonical isomorphism $\sigma : L_{\sigma^{-1}\mathfrak{P}} \to L_\mathfrak{P}$, so G acts on $\mathbb{I}_L$ via $(\sigma\alpha)_\mathfrak{P} = \sigma(\alpha_{\sigma^{-1}\mathfrak{P}})$. Let $\mathbb{I}_L^G = \{\alpha \in \mathbb{I}_L : \sigma\alpha = \alpha\}$ be its group of invariants.

Proposition 4.13. $\mathbb{I}_L^G = \mathbb{I}_K$.

Proof. For $\sigma \in G$, the induced map $\sigma : L_\mathfrak{P} \to L_{\sigma\mathfrak{P}}$ is in fact a $K_\mathfrak{p}$-isomorphism, where $\mathfrak{p}$ lies under $\mathfrak{P}$. So any $\alpha \in \mathbb{I}_K$ is fixed by the G-action.
Conversely, suppose $\alpha \in \mathbb{I}_L$ is a G-invariant. Then $\sigma\alpha_{\sigma^{-1}\mathfrak{P}} = \alpha_\mathfrak{P}$ for all prime $\mathfrak{P}$ of L and all $\sigma \in G$. Recall that the decomposition group $D_{\mathfrak{P}|\mathfrak{p}}$ can be identified with $\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$. For any $\sigma \in D_{\mathfrak{P}|\mathfrak{p}}$, we have $\sigma^{-1}\mathfrak{P} = \mathfrak{P}$ by definition. As $\alpha_\mathfrak{P} = \sigma\alpha_\mathfrak{P}$ for $\sigma \in D_{\mathfrak{P}|\mathfrak{p}}$, we see that $\alpha_\mathfrak{P} \in K_\mathfrak{p}$.
Knowing this, suppose $\sigma \in G$ is any element, then $\alpha_\mathfrak{P} = \alpha_{\sigma^{-1}\mathfrak{P}}$. But $(\sigma^{-1}\mathfrak{P})_{\sigma\in G}$ is the set of all primes above $\mathfrak{p}$, so we conclude $\alpha \in \mathbb{I}_K$. □

Now back to the case where L/K is just any finite extension.

Proposition 4.14. *If L/K is a finite extension, then $L^\times \cap \mathbb{I}_K = K^\times$.*

In other words, any idèle of K which becomes principal in L is itself principal. This behaviour is of course different from ideals.

Proof. The inclusion $K^\times \subset L^\times \cap \mathbb{I}_K$ is immediate. Let Ω be the Galois closure of L/K. Then $\mathbb{I}_K \subset \mathbb{I}_L \subset \mathbb{I}_\Omega$. Take any $\alpha \in \Omega^\times \cap \mathbb{I}_K$, then $G = \mathrm{Gal}(\Omega/K)$ fixes α, and so $\alpha \in K^\times$. So $L^\times \cap \mathbb{I}_K \subset \Omega^\times \cap \mathbb{I}_K \subset K^\times$. □

Consequently, we obtain an injection $C_K = \mathbb{I}_K/K^\times \hookrightarrow \mathbb{I}_L/L^\times = C_L$. We view C_K from now on as a subgroup of C_L. Then $[\alpha] \in C_L$ lies in C_K if and only if it contains some $\alpha \in \mathbb{I}_K$.
Now if L/K is a Galois extension, then C_L is a G-module by setting $g[\alpha] = [g\alpha]$.

Proposition 4.15. $C_L^G = C_K$.

Proof. Something something Galois cohomology. □

Next, we define a norm homomorphism $\mathbb{I}_L \to \mathbb{I}_K$ (for any finite L/K) using local norm maps.

Definition 4.11. For $\mathfrak{P} \mid \mathfrak{p}$, $L_\mathfrak{P}$ is a (finite-dimensional) $K_\mathfrak{p}$-vector space. For any $x \in L_\mathfrak{P}$, its norm is $N_{L_\mathfrak{P}/K_\mathfrak{p}} = \det(\mathrm{mult}_x)$ where $\mathrm{mult}_x : L_\mathfrak{P} \to L_\mathfrak{P}$ is the $K_\mathfrak{p}$-linear map induced by multiplication by x.

Definition 4.12. For any idèle of L, its norm $N_{L/K}(\alpha) \in \mathbb{I}_K$ is defined by $N_{L/K}(\alpha)_\mathfrak{p} = \prod_{\mathfrak{P}\mid\mathfrak{p}} N_{L_\mathfrak{P}/K_\mathfrak{p}}(\alpha_\mathfrak{P})$.

Proposition 4.16. *(i) For any finite extensions $M/L/K$, $N_{M/K} = N_{L/K} \circ N_{M/L}$.*
(ii) For $\alpha \in \mathbb{I}_K$, $N_{L/K}(\alpha) = \alpha^{[L:K]}$.
(iii) The norm of a principal idèle $x \in L^\times$ is its usual norm $N_{L/K}(x)$.

Proof. Immediate. □

4.6 Statements of Class Field Theory via Idèles

Theorem 4.17 (Artin Reciprocity Law)**.** *For any Galois extension L/K, we have a canonical isomorphism $r_{L/K} : \mathrm{Gal}(L/K)^{\mathrm{ab}} \to C_K/N_{L/K}C_L$. The inverse map to $r_{L/K}$ yields a surjective homomorphism $(-, L/K) : C_K \to \mathrm{Gal}(L/K)^{\mathrm{ab}}$ (whose kernel is $N_{L/K}C_L$) is known as the (global) norm-residue symbol.*

We can also of course view this as a homomorphism $\mathbb{I}_K \to \mathrm{Gal}(L/K)^{\mathrm{ab}}$.

Remark. This statement is now compatible with what you must have seen in local class field theory.

Theorem 4.18 (Existence Theorem)**.** *Let K be a number field. Then the map $L \mapsto \mathcal{N}_L = N_{L/K}C_L$ is a one-to-one correspondence between finite abelian extensions L/K and closed subgroups of finite index in C_K. Moreover, $L_1 \subset L_2$ iff $\mathcal{N}_{L_1} \supset \mathcal{N}_{L_2}$, and we have the identities $\mathcal{N}_{L_1L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$, $\mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$, and $\mathrm{Gal}(L/K) \cong C_K/\mathcal{N}_L$.*
L is known as the class field of $\mathcal{N}_L$.

The key part of this is that the norm groups are precisely closed subgroups of finite index in C_K, which are the same as subgroups containings $C_K(\mathfrak{m})$ for some modulus $\mathfrak{m}$ of K.

Definition 4.13. The class field $K(\mathfrak{m})$ for the congruence subgroup $C_K(\mathfrak{m})$ is known as the ray class field of $\mathfrak{m}$.

So in particular $\mathrm{Gal}(K(\mathfrak{m})/K) \cong C_K/C_K(\mathfrak{m})$. Note that if $\mathfrak{m} \mid \mathfrak{m}'$ then $K(\mathfrak{m}) \subset K(\mathfrak{m}')$.

Corollary 4.19. *Every abelian extension L/K is contained in a ray class field.*

Definition 4.14. We say a subgroup $N \leq C_K$ is a norm group if $N = \mathcal{N}_L = N_{L/K}C_L$ for some Galois extension L/K.

Each norm group is in fact the norm group of an abelian extension.

Theorem 4.20. *Let L/K be Galois and let L^{ab} be the maximal abelian extension of K contained in L. Then $\mathcal{N}_L = \mathcal{N}_{L^{\mathrm{ab}}}$.*

Proof. The inclusion $K \subset L^{\mathrm{ab}} \subset L$ gives the inclusion $\mathcal{N}_{L^{\mathrm{ab}}} \supset \mathcal{N}_L$. By Theorem 4.17, we have $C_K/\mathcal{N}_L \cong \mathrm{Gal}(L/K)^{\mathrm{ab}} = \mathrm{Gal}(L^{\mathrm{ab}}/K) \cong C_K/\mathcal{N}_{L^{\mathrm{ab}}}$. Since everything's finite, we conclude $\mathcal{N}_L = \mathcal{N}_{L^{\mathrm{ab}}}$. □

Corollary 4.21. *For any Galois L/K, $[C_K : \mathcal{N}_L]$ divides $[L : K]$ with equality iff L/K is abelian.*

Proposition 4.22. *The norm groups $\mathcal{N}_L$ are precisely the closed subgroups of C_K with finite index.*

Sketch of proof. By Theorem 4.17, $\mathcal{N}_L$ has finite index in C_K. We also have $C_K \cong C_K^0 \times \Gamma_K, C_L \cong C_L^0 \times \Gamma_L$ where $\mathbb{R}_+ \cong \Gamma_K = \Gamma_L \subset C_L$ by Proposition 4.10 and its proof. Then $\mathcal{N}_L = N_{L/K}C_L = N_{L/K}C_L^0 \times N_{L/K}\Gamma_K = N_{L/K}C_L^0 \times \Gamma_K^{[L:K]} = N_{L/K}C_L^0 \times \Gamma_K$.
Since $N_{L/K} : C_L \to C_K$ is continuous, $N_{L/K}C_L^0$ is compact hence closed. On the other hand, Γ_K is also closed in C_K, so $\mathcal{N}_L$ is closed.
The other direction is omitted. □

Remark. One can reduce Theorem 4.18 to this proposition, since each closed subgroup of finite index is now the norm group of an abelian extension by Theorem 4.20.

The idèle class group can be used to decompose prime ideals in abelian extensions.

Theorem 4.23 (Decomposition Law)**.** *Let L/K be an abelian extension of degree n and $\mathfrak{p}$ an unramified prime of K. Let $\pi \in K_{\mathfrak{p}}$ be a uniformiser. Let $\bar{n}_{\mathfrak{p}}(\pi) \in C_K$ be the idèle class represented by the idèle $n_{\mathfrak{p}}(\pi) = (1, \ldots, 1, \pi, 1, \ldots)$ and let f be the smallest number such that $\bar{n}_{\mathfrak{p}}(\pi)^f \in \mathcal{N}_L$. Then the prime ideals $\mathfrak{p}$ factors in L into $r = n/f$ distinct prime ideals of degree f.*

This is limited to unramified primes, but we can also use the norm group to detect whether a (general) prime ramifies as follows:

Theorem 4.24. *Let L/K be an abelian extension of degree n and $\mathfrak{p}$ a prime of K, then:*
(i) $\mathfrak{p}$ is unramified in L iff $U_{\mathfrak{p}} \subset \mathcal{N}_L$.
(ii) $\mathfrak{p}$ splits completely in L iff $K_{\mathfrak{p}}^{\times} \subset \mathcal{N}_L$.

4.7 Comparison with the Ideal-Theoretic Version

Let's finally show $I_K(\mathfrak{m})/P_K(\mathfrak{m}) \cong C_K/C_K(\mathfrak{m})$. Recall the approximation theorem:

Theorem 4.25. *Let K be a number field and $|\cdot|_1, \ldots, |\cdot|_n$ pairwise non-equivalent norms on K. Let $\beta_1, \ldots, \beta_n$ be any nonzero element of K. Then for any $\epsilon > 0$, there exists $\alpha \in K$ such that $|\alpha - \beta_j|_j < \epsilon$ for each $j = 1, \ldots, n$.*

Note that if $\mathfrak{p}$ is a real infinite prime (with embedding σ), then $|\alpha - \beta|_{\mathfrak{p}} < \epsilon$ means that $\sigma(\alpha/\beta) > 0$ (for small enough ϵ).
If $\mathfrak{p}$ is finite, then $|\alpha - \beta|_{\mathfrak{p}} < \epsilon$ means that $\alpha \equiv \beta \pmod{\mathfrak{p}^M}$ for suitably large M.

Proposition 4.26. *There is an isomorphism of groups* $\overline{(-)}_{\mathfrak{m}} : C_K/C_K(\mathfrak{m}) \to I_K(\mathfrak{m})/P_K(\mathfrak{m})$.

Before we prove this, recall that we have a map $(-) : \mathbb{I}_K \to I_K, \alpha \mapsto \prod_{\mathfrak{p} \text{ finite}} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}$. Note also the isomorphism $C_K/C_K(\mathfrak{m}) \cong \mathbb{I}_K(\mathfrak{m})/(\mathbb{I}_K(\mathfrak{m})K^\times)$.

Proof. Write $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{r_{\mathfrak{p}}}$.
For each idèle class $[\alpha] \in \mathbb{I}_K(\mathfrak{m})/(\mathbb{I}_K(\mathfrak{m})K^\times)$, let's show that α can be chosen in $\mathbb{I}^{\langle \mathfrak{m} \rangle} = \{\alpha \in \mathbb{I}_K : \forall \mathfrak{p} \nmid \mathfrak{m}, \alpha_{\mathfrak{p}} = 1\}$.
By Theorem 4.25, there exists $x \in K^\times$ such that $\alpha_{\mathfrak{p}} x \equiv 1 \pmod{\mathfrak{p}^{r_{\mathfrak{p}}}}$. So $\alpha x = \alpha' \beta$ where $\alpha'_{\mathfrak{p}} = 1$ for $\mathfrak{p} \mid \mathfrak{m}$ and $\alpha'_{\mathfrak{p}} = \alpha_{\mathfrak{p}} x$ for $\mathfrak{p} \nmid \mathfrak{m}$, and where $\beta_{\mathfrak{p}} = \alpha_{\mathfrak{p}} x$ for $\mathfrak{p} \mid \mathfrak{m}$ and $\beta_{\mathfrak{p}} = 1$ for $\mathfrak{p} \nmid \mathfrak{m}$.
So $\alpha' \in \mathbb{I}^{\langle \mathfrak{m} \rangle}$ and $\beta \in \mathbb{I}_K(\mathfrak{m})$.
We then have

$$\begin{aligned} C_K/C_K(\mathfrak{m}) &\cong \mathbb{I}_K/(\mathbb{I}_K(\mathfrak{m})K^\times) \cong \mathbb{I}^{\langle \mathfrak{m} \rangle}\mathbb{I}_K(\mathfrak{m})K^\times/(\mathbb{I}_K(\mathfrak{m})K^\times) \\ &\cong \mathbb{I}^{\langle \mathfrak{m} \rangle}/((\mathbb{I}_K(\mathfrak{m})K^\times) \cap \mathbb{I}^{\langle \mathfrak{m} \rangle}) \end{aligned}$$

The homomorphism $\mathbb{I}^{\langle \mathfrak{m} \rangle} \to I_K(\mathfrak{m})/P_K(\mathfrak{m})$ sending α to $(\alpha) \pmod{P_K(\mathfrak{m})}$ is surjective and has kernel $(\mathbb{I}_K(\mathfrak{m})K^\times) \cap \mathbb{I}^{\langle \mathfrak{m} \rangle}$, so we are done. □

Proposition 4.27. *Let L/K be an abelian extension. Then the restriction of $\overline{(-)}_{\mathfrak{m}}$ to $N_{L/K}C_L/C_K(\mathfrak{m})$ gives an isomorphism $\overline{(-)}_{\mathfrak{m}} : N_{L/K}C_L/C_K(\mathfrak{m}) \to N_{L/K}(I_L(\mathfrak{m}))P_K(\mathfrak{m})/P_K(\mathfrak{m})$.*

Proof. Let $\mathbb{I}_L^{\langle \mathfrak{m} \rangle} = \{\alpha \in \mathbb{I}_L : \forall \mathfrak{P} \mid \mathfrak{m}, \alpha_{\mathfrak{P}} = 1\}$. By the proof of the preceding proposiiton, $\mathbb{I}_L = \mathbb{I}_L^{\langle \mathfrak{m} \rangle}\mathbb{I}_L(\mathfrak{m})L^\times$ and therefore

$$\frac{N_{L/K}C_L}{C_K(\mathfrak{m})} = \frac{N_{L/K}\mathbb{I}_L K^\times}{\mathbb{I}_K(\mathfrak{m})K^\times} = \frac{(N_{L/K}\mathbb{I}_L(\mathfrak{m}))\mathbb{I}_K(\mathfrak{m})K^\times}{\mathbb{I}_K(\mathfrak{m})K^\times}$$

Now the isomorphism $\underline{(-)}_{\mathfrak{m}}$ associate to the class of $\alpha \in \mathbb{I}_K^{\langle \mathfrak{m} \rangle}$ the class of the ideal (α). The elements of $N_{L/K}C_L/C_K(\mathfrak{m})$ are the classes represented by the norm idèles $N_{L/K}\mathbb{I}_L^{\langle \mathfrak{m} \rangle}$ in $\mathbb{I}_K^{\langle \mathfrak{m} \rangle}$. In particular, they are mapped precisely onto the classes of the norm ideals $N_{L/K}I_L(\mathfrak{m})$ in $I_K(\mathfrak{m})$. Hence $\overline{(-)}_{\mathfrak{m}}$ gives the desired isomorphism. □

$\overline{(-)}_{\mathfrak{m}}$ gives a surjective homomorphism $(-)_{\mathfrak{m}} : C_K \to I_K(\mathfrak{m})/P_K(\mathfrak{m})$ with kernel $C_K(\mathfrak{m})$. It's perhaps enlightening to describe this: Let $\mathfrak{p}$ be a prime of K and $\pi \in K_{\mathfrak{p}}$ a uniformiser. Let $n_{\mathfrak{p}}(\pi) = (1, \ldots, 1, \pi, 1, \ldots)$, then $([n_{\mathfrak{p}}(\pi)])_{\mathfrak{m}} = \mathfrak{p} \pmod{P_K(\mathfrak{m})}$ since $(n_{\mathfrak{p}}(\pi)) = \mathfrak{p}$.

Theorem 4.28. *Let L/K be an abelian extension and let $\mathfrak{m}$ be a modulus of K such that $\mathfrak{f}(L/K) \mid \mathfrak{m}$. Let $T_{L/K}(\mathfrak{m}) = N_{L/K}(I_L(\mathfrak{m}))P_K(\mathfrak{m})$ be the Takagi group. Then we have a commutative diagram*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N_{L/K}C_L & \longrightarrow & C_K & \xrightarrow{(-,L/K)} & \mathrm{Gal}(L/K) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle (-)_{\mathfrak{m}}} & & \downarrow{\scriptstyle (-)_{\mathfrak{m}}} & & \| & & \\ 1 & \longrightarrow & T_{L/K}(\mathfrak{m}) & \longrightarrow & I_K(\mathfrak{m})/P_K(\mathfrak{m}) & \xrightarrow[(L/K,-)]{} & \mathrm{Gal}(L/K) & \longrightarrow & 1 \end{array}$$

with exact rows, where the vertical arrows are surjective.

Proof. We need only to show commutativity. Consider the diagram of isomorphisms:

$$\begin{array}{ccc} C_K/C_K(\mathfrak{m}) & \xrightarrow{(-,L/K)} & \mathrm{Gal}(L/K) \\ {\scriptstyle \overline{(-)}_{\mathfrak{m}}}\downarrow & & \| \\ I_K(\mathfrak{m})/P_K(\mathfrak{m}) & \xrightarrow[(L/K,-)]{} & \mathrm{Gal}(L/K) \end{array}$$

Let $\mathfrak{p}$ be a prime of K and let $\pi \in K_{\mathfrak{p}}$ be a uniformiser. Then $\overline{([n_{\mathfrak{p}}(\pi)])}_{\mathfrak{m}} = \mathfrak{p}$. We will see later (when discussing local class field theory) that $([n_{\mathfrak{p}}(\pi)], L/K) = (L/K, \mathfrak{p})$. So this diagram commutes. The rest follows. □

4.8 Compatibility with Local Class Field Theory

The goal of local class field theory is, of course, to classify finite abelian extensions of a local field K and their Galois groups.
Let K be a local field. We write K^{sep} for a fixed separable closure of K and K^{ab} the maximal abelian extension of K in K^{sep}.

Theorem 4.29 (Local Artin Reciprocity)**.** *Let K be a (non-Archimedean) local field. Then there is a unique continuous homomorphism $\theta_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ with the property that, for each finite extension L/K in K^{ab}, the homomorphism $\theta_{L/K} : K^\times \to \mathrm{Gal}(L/K)$ given by composing θ_K with the surjection $\mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(L/K)$ satisfies:*
(i) For unramified L/K, $\theta_{L/K}(\pi) = \mathrm{Frob}_{L/K}$ where π is a uniformiser of K.
(ii) In general, $\theta_{L/K}$ is always surjective with kernel $N_{L/K}(L^\times)$.

Here, (when L/K is unramified) $\mathrm{Frob}_{L/K}$ is the unique preimage of the Frobenius of the residue field extension.

Definition 4.15. $\theta_{L/K}$ is also called the local Artin map, or local norm-residue symbol. We sometimes write $\theta_{L/K} = (-, L/K)$.

Remark. By contrast to the global theory, θ_K deals with all (abelian) field extensions at once, and the isomorphism we get is beween the Galois group and quotients of $K^\times$.

Definition 4.16. A norm group of a local field K is a subgroup of the form $N_{L/K}(L^\times) \leq K^\times$ for some L/K finite abelian.

Corollary 4.30. *The map $L \mapsto N_{L/K}(L^\times)$ is an inclusion-reversing bijection between the set of finite abelian extensions L/K and norm groups of K. And every norm group of K has finite index in $K^\times$.*

In fact, norm groups are exactly the open subgroups of finite index in $K^\times$.

Theorem 4.31 (Existence Theorem)**.** *Let K be a local field and H any open subgroup of $K^\times$ of finite index. There is a unique extension L/K in K^{ab} with $N_{L/K}(L^\times) = H$.*

Next, let L/K be a Galois extension of number fields. Pick any prime $\mathfrak{p}$ of K. Then we can embed the local Galois group $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ into $\mathrm{Gal}(L/K)$ for any $\mathfrak{P}$ above $\mathfrak{p}$.
We have a injection $\bar{n}_{\mathfrak{p}} : K_{\mathfrak{p}}^\times \to C_K$ sending any $a_{\mathfrak{p}} \in K_{\mathfrak{p}}^\times$ to the class of the idèle $(1, \ldots, 1, a_{\mathfrak{p}}, 1, \ldots)$. The compatibility between the local and global class field theories can then be stated as follows:

Proposition 4.32. *If L/K is an abelian extension and $\mathfrak{p}$ is a prime of K lying below a prime $\mathfrak{P}$ of L. Then the diagram*

$$\begin{array}{ccc} K_{\mathfrak{p}}^{\times} & \xrightarrow{(-,L_{\mathfrak{P}}/K_{\mathfrak{p}})} & \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \\ {\scriptstyle \bar{n}_{\mathfrak{p}}}\downarrow & & \downarrow \\ C_K & \xrightarrow{(-,L/K)} & \mathrm{Gal}(L/K) \end{array}$$

commutes.

Corollary 4.33. *Let L/K be an abelian extension of number fields and $\alpha \in \mathbb{I}_K$. Then*

$$(\alpha, L/K) = \prod_{\mathfrak{p}} (\alpha_{\mathfrak{p}}, L_{\mathfrak{P}}/K_{\mathfrak{p}})$$

for any choices of $\mathfrak{P} \mid \mathfrak{p}$. For a principal idèle $a \in K^{\times}$, this reduces to the "product formula" $\prod_{\mathfrak{p}} (a, L_{\mathfrak{P}}/K_{\mathfrak{p}}) = 1$.

In particular, if $\mathfrak{p}$ is unramified in L and π is an uniformiser of $K_{\mathfrak{p}}$, then $(n_{\mathfrak{p}}(\pi), L/K) = (\pi, L_{\mathfrak{P}}/K_{\mathfrak{p}}) = \mathrm{Frob}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} = (L/K, \mathfrak{p})$, again for any $\mathfrak{P} \mid \mathfrak{p}$. This finishes the proof of Theorem 4.28.
There also exists a notion of a local conductor $\mathfrak{f}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$, which is not so meaningful but their product equals the global conductor.