MATH 223B (GALOIS COHOMOLOGY AND CLASS FIELD THEORY)

LINUS HAMANN

Contents

1. Introduction

Let $\mathbb{Q}$ denote the rational numbers with algebraic closure $\overline{\mathbb{Q}}$. A basic goal in algebraic number theory is to understand the structure of the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, known as the absolute Galois group of $\mathbb{Q}$. Roughly speaking, this is the collection of symmetries of the following sets

$$\{\alpha \in \overline{\mathbb{Q}} | p(\alpha) = 0\} \tag{1.1}$$

for $p(x) \in \mathbb{Q}[x]$ an irreducible polynomial. For example, when $p(x) = x^2 - 5$, we have the solutions $\{\sqrt{5}, -\sqrt{5}\}$ and a corresponding surjection $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} = \langle -1 \rangle$, where $-1 \in \mathbb{Z}/2\mathbb{Z}$ acts via the reflection $\sqrt{5} \leftrightarrow -\sqrt{5}$. More interestingly, for the equation $p(x) = x^q - 1$ for q a prime number, we have the solutions $\{\zeta_q^i | 0 \leq i \leq q-1\}$ for ζ_q a non-trivial qth root of unity and a surjection $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \simeq (\mathbb{Z}/q\mathbb{Z})^*$, where $a \in (\mathbb{Z}/q\mathbb{Z})^*$ acts via $\sigma_a : \zeta_q^i \mapsto \zeta_q^{ia}$.

More precisely, the absolute Galois group is the inverse limit in the category of groups of

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) := \varprojlim_{L} \mathrm{Gal}(L/\mathbb{Q}), \tag{1.2}$$

where $L/\mathbb{Q}$ ranges over finite Galois extensions of $\mathbb{Q}$, and the maps, for an inclusion $\mathbb{Q} \subset L' \subset L$, are given by the natural restriction map $\mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{Gal}(L'/\mathbb{Q})$. As we will discuss in the next lectures, such a projective limit of finite groups gives examples of what are known as pro-finite groups.

One of the basic reasons for wanting to understand the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is that it provides us information about the structure of solutions to the equation $p(x)$. E.g from Galois theory we know

that if the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the solutions of $p(x)$ factors through a finite solvable group then the solutions can be computed in terms of the coefficients and radicals. In this way, the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ together with its action on (1.1) provides some kind of systematic generalization for the notion of solvability of polynomial among radicals.

Another (perhaps more compelling reason) is that the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is intimately related to many interesting arithmetic phenomena. For example, let's consider the polynomial $p(x) = x^2 - 5$ again. We may ask ourselves the following basic arithmetic question.

Question 1.1. *When does $x^2 = 5$ have a solution modulo a prime number p?*

This is the content of quadratic reciprocity; often phrased in terms of the Legendre symbol.

Definition 1.2. Let p be an odd prime. The *Legendre symbol*

$$\left(\frac{a}{p}\right)$$

is defined for any integer a by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if there exists } x \in \mathbb{Z} \text{ such that } x^2 \equiv a \pmod{p}, \\ -1 & \text{otherwise.} \end{cases}$$

This symbol can be completely understood in terms of quadratic reciprocity.

Theorem 1.3 (Quadratic Reciprocity)**.** *Let p and q be distinct odd primes. Then we have an equality*

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

Moreover, for any odd prime p, we have equalities:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Specialized to the case of interest, this gives us the following.

Example 1.4. Let $p \neq 5$ be an odd prime then we have that

$$\left(\frac{p}{5}\right) = \left(\frac{5}{p}\right). \tag{1.3}$$

In particular, if we look at the squares mod 5 then we have that $\{1^2, 2^2, 3^2, 4^2\} \cong \{1, -1, -1, 1\}$ mod 5, which allows us to conclude.

Corollary 1.5. *For $p \neq 5$ an odd prime number*

$$\left(\frac{5}{p}\right) = 1 \iff p \cong \pm 1 \mod 5.$$

We claim that Corollary 1.5 and indeed Theorem 1.3 is a consequence of understanding the action of the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the set of solutions $\{\sqrt{5}, -\sqrt{5}\}$. To see this, we recall that we have an inclusion $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\zeta_5)$, as witnessed by the identity

$$\zeta_5 + \zeta_5^{-1} = \cos(\frac{2\pi}{5}) = \frac{\sqrt{5} - 1}{2}.$$

To proceed further, we recall some basic properties of the arithmetic of the cyclotomic fields $\mathbb{Q}(\zeta_q)/\mathbb{Q}$. In particular, we have the following.

Theorem 1.6. *Let q be an odd prime and $\zeta_q \in \overline{\mathbb{Q}}$ a non-trivial qth root of unity.*

(1) *The extension $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ is Galois with Galois group isomorphic to $(\mathbb{Z}/q\mathbb{Z})^*$ via the mapping*

$$a \mapsto \sigma_a,$$

where $\sigma_a(\zeta_q) = \zeta_q^a$.

(2) *The ring of integers of $\mathbb{Q}(\zeta_q)$ is given by $\mathbb{Z}[\zeta_q]$.*

(3) *A prime p in $\mathbb{Z}$ is unramified in $\mathbb{Q}(\zeta_q)$ if and only if $p \neq q$.*

(4) *If $q \neq p$ then by (1)-(3), we have a factorization as prime ideals $(p)\mathbb{Z}[\zeta_q] = \mathfrak{p}_1 \cdots \mathfrak{p}_g$, and for all $i = 1, \ldots, g$ that $\mathbb{Z}[\zeta_q]/\mathfrak{p}_i \simeq \mathbb{F}_{p^f}$ for some $f \geq 1$ such that*

$$gf = q - 1 \tag{1.4}$$

(5) *For $q \neq p$ as in (4), for any $i = 1, \ldots, g$, we may look at the decomposition group $\mathfrak{D}_{\mathfrak{p}_i} \subset \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ of elements fixing the prime ideal $\mathfrak{p}_i$. Then the natural map*

$$\mathfrak{D}_{\mathfrak{p}_i} \to \mathrm{Gal}((\mathbb{Z}[\zeta_q]/\mathfrak{p}_i)/(\mathbb{Z}/p)) \simeq \mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p) = \langle \{x \mapsto x^p\} \rangle \simeq \mathbb{Z}/f\mathbb{Z}, \tag{1.5}$$

In turn, we obtain a lift $\mathrm{Frob}_p \in \mathfrak{D}_{\mathfrak{p}_i} \subset \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ of the pth power map $x \mapsto x^p$ on $\mathbb{F}_{p^f}$, which is given by σ_p in the parametrization of (1).

Implicitly, we were invoking the abstract structure theory of a Galois extension of number fields L/K specialized to the case of the $\mathbb{Q}(\zeta_q)/\mathbb{Q}$.

Exercise 1.7. *Let L/K be a finite Galois extension of number fields with Galois group $G = \mathrm{Gal}(L/K)$. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a nonzero prime ideal and fix a prime ideal $\mathfrak{P} \subset \mathcal{O}_L$ lying above it (i.e. $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$). Write $k_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$ and $k_{\mathfrak{P}} = \mathcal{O}_L/\mathfrak{P}$ for the residue fields, and denote by $L_{\mathfrak{P}}$ and $K_{\mathfrak{p}}$ the completions of L and K at $\mathfrak{P}$ and $\mathfrak{p}$ respectively. We recall, since $\mathcal{O}_L$, is Dedekind, we have a unique factorization*

$$\mathfrak{p}\,\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i} \tag{1.6}$$

into prime ideals $\mathfrak{P}_i$ of $\mathcal{O}_L$ for integers $e_i \geq 1$.

(1) *Define the* decomposition group *of $\mathfrak{P}$ by*

$$D(\mathfrak{P}|\mathfrak{p}) = \{\, \sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P} \,\}.$$

(a) *Prove that $D(\mathfrak{P}|\mathfrak{p})$ is a subgroup of G.*

(b) *Show that G acts transitively on the set of primes of L above $\mathfrak{p}$ and that the stabilizer of $\mathfrak{P}$ is $D(\mathfrak{P}|\mathfrak{p})$. Deduce that*

$$g = [G : D(\mathfrak{P}|\mathfrak{p})].$$

(2) *Show that all the integers e_i in (1.6) equal to a single integer $e := e(\mathfrak{B}|\mathfrak{p})$. In particular, the decomposition (1.6) becomes*

$$\mathfrak{p}\,\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e}.$$

Show that there exists a single integer $f = f(\mathfrak{P}/\mathfrak{p})$ such that $[k_{\mathfrak{P}_i} : k_{\mathfrak{p}}] = f$ for all i. Deduce the fundamental relation

$$[L : K] = e\, f\, g. \tag{1.7}$$

(3) *Consider the reduction map*

$$\mathrm{red}_{\mathfrak{P}} : \mathcal{O}_L \longrightarrow k_{\mathfrak{P}}.$$

(a) *For $\sigma \in D(\mathfrak{P}|\mathfrak{p})$, show that σ induces a well-defined automorphism $\overline{\sigma}$ of $k_{\mathfrak{P}}$ by*

$$\overline{\sigma}(\mathrm{red}_{\mathfrak{P}}(x)) = \mathrm{red}_{\mathfrak{P}}(\sigma(x)).$$

(b) *Deduce a group homomorphism*

$$\phi_{\mathfrak{P}} : D(\mathfrak{P}|\mathfrak{p}) \longrightarrow \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}}).$$

(c) *Define the* inertia group *by*

$$I(\mathfrak{P}|\mathfrak{p}) = \ker(\phi_{\mathfrak{P}}) = \{\, \sigma \in D(\mathfrak{P}|\mathfrak{p}) : \overline{\sigma} = \mathrm{id} \text{ on } k_{\mathfrak{P}} \,\}.$$

Prove that $I(\mathfrak{P}|\mathfrak{p})$ is a normal subgroup of $D(\mathfrak{P}|\mathfrak{p})$.

(4) *Prove that $\phi_{\mathfrak{P}}$ is surjective and that there is a short exact sequence*

$$1 \longrightarrow I(\mathfrak{P}|\mathfrak{p}) \longrightarrow D(\mathfrak{P}|\mathfrak{p}) \xrightarrow{\phi_{\mathfrak{P}}} \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}}) \longrightarrow 1.$$

Deduce in particular that

$$|D(\mathfrak{P}|\mathfrak{p})| = e(\mathfrak{P}|\mathfrak{p})\, f(\mathfrak{P}|\mathfrak{p}), \qquad |I(\mathfrak{P}|\mathfrak{p})| = e(\mathfrak{P}|\mathfrak{p}), \qquad |\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})| = f(\mathfrak{P}|\mathfrak{p}).$$

(5) (a) *Show that the natural embedding $K \hookrightarrow K_{\mathfrak{p}}$ extends to an embedding $L \hookrightarrow L_{\mathfrak{P}}$ and that restriction induces a canonical isomorphism*

$$D(\mathfrak{P}|\mathfrak{p}) \;\cong\; \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}).$$

(b) *Under this identification, interpret $I(\mathfrak{P}|\mathfrak{p})$ as the subgroup of $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ acting trivially on the residue field $k_{\mathfrak{P}}$.*

(6) *Assume $\mathfrak{p}$ is unramified in L, i.e. $e(\mathfrak{P}|\mathfrak{p}) = 1$. Then $I(\mathfrak{P}|\mathfrak{p}) = 1$ and $\phi_{\mathfrak{P}}$ is an isomorphism. Let $\mathrm{Frob}_{\mathfrak{p}} \in D(\mathfrak{P}|\mathfrak{p})$ be the unique element whose image in $\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$ is the $|k_{\mathfrak{p}}|$-power map.*

(a) *Show that $\mathrm{Frob}_{\mathfrak{p}}$ is characterized by*

$$\mathrm{Frob}_{\mathfrak{p}}(x) \equiv x^{N\mathfrak{p}} \pmod{\mathfrak{P}} \quad \text{for all } x \in \mathcal{O}_L.$$

(b) *Show that if $\mathfrak{P}' = \tau(\mathfrak{P})$ for some $\tau \in G$, then*

$$\mathrm{Frob}_{\mathfrak{p}}(\mathfrak{P}') = \tau\, \mathrm{Frob}_{\mathfrak{p}}(\mathfrak{P})\, \tau^{-1}.$$

In particular, the conjugacy class of $\mathrm{Frob}_{\mathfrak{p}}$ in G is independent of the choice of $\mathfrak{P}|\mathfrak{p}$.

(c) *If L/K is abelian i.e $\mathrm{Gal}(L/K)$ is abelian, deduce that the Frobenius element $\mathrm{Frob}_{\mathfrak{p}} \in G$ (for $\mathfrak{p}$ unramified) is independent of the choice of $\mathfrak{P}|\mathfrak{p}$ as an* element *of G (not just up to conjugacy).*

With this in hand, let's go back to the original problem. In particular, suppose we have a prime p, then we were interested in determining when $\left(\frac{5}{p}\right) = 1$ or equivalently when $x^2 = 5$ has a solution modulo p. We recall that the ring of integers of $\mathbb{Q}(\sqrt{5})$ is given by $\mathbb{Z}[\sqrt{5}]$ (since $5 \cong 1 \mod 4$). In particular, it follows that $x^2 = 5$ has a solution modulo p if and only if the prime p splits in $\mathbb{Z}[\sqrt{5}]$, which is equivalent to the g appearing in Theorem 1.6 (4) being equal 2 (resp. 4) or equivalently that f is equal to 2 (resp. 1). However, in light of 1.6 (5) this is equivalent to $p \cong \pm 1 \mod 5$. In particular, we see that this exactly recovers Corollary 1.5, and this perspective is powerful enough to capture the general picture.

Exercise 1.8. *Use Theorem 1.6 to establish Theorem 1.3. Let $q \neq p$ be odd primes and set $K = \mathbb{Q}(\zeta_q)$, for ζ_q a non-trivial qth root of unity.*

(1) *Show that*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

(2) *Set $H \subset (\mathbb{Z}/q\mathbb{Z})^\times$ be the subgroup of squares, and let $K^+ = K^H$ denote the fixed field. Prove that*

$$K^+ = \mathbb{Q}\left(\sqrt{(-1)^{\frac{q-1}{2}} q}\right).$$

(Hint: *Compare discriminants.)*

(3) Show that p splits completely in K^+ if and only if the image of Frob_p *lies in H.*
(4) Deduce that

$$\left(\frac{q}{p}\right) = 1 \quad \Longleftrightarrow \quad p \text{ splits in } \mathbb{Q}\left(\sqrt{(-1)^{\frac{q-1}{2}}q}\right).$$

(5) Use (1) and (3), to show that

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

In this way, we see that Corollary 1.3 is a consequence of understanding the structure of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and in particular its quotient $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. More specifically, we may organize what happened above as follows. We view the Legendre symbol as giving rise to a map

$$\chi_q : \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \simeq (\mathbb{Z}/q\mathbb{Z})^* \to \langle \pm 1\rangle \subset \mathbb{C}^*$$
$$a \mapsto (\frac{a}{q})$$

where we note that, it easily follows from Definition 1.2, we have an equality $\left(\frac{a}{q}\right)\left(\frac{b}{q}\right) = \left(\frac{ab}{q}\right)$ so this is indeed a multiplicative character. Then quadratic reciprocity follows by explicating the lifts of Frobenius $\mathrm{Frob}_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ of the pth power map for $q \neq p$ and interpreting them in terms of the arithmetic of the cyclotomic field.

In the hopes of generalizing this arithmetic phenomenon, we fix a number field $K/\mathbb{Q}$ with algebraic closure $K \subset \overline{K}$, and a homomorphism

$$\chi : \mathrm{Gal}(\overline{K}/K) \to \mathbb{C}^*,$$

where $\mathrm{Gal}(\overline{K}/K) := \varprojlim_{K\subset L} \mathrm{Gal}(L/K)$ over finite Galois extensions L/K, as in (1.2). Since $\mathbb{C}^*$ is abelian, the character χ will factor through the abelianization $\mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}$ of this group. This can be thought of as the Galois group of an algebraic extension $K \subset K^{\mathrm{ab}} \subset \overline{K}$. In particular, K^{ab} is the union of finite Galois extensions $K \subset L \subset K^{\mathrm{ab}}$ such that $\mathrm{Gal}(L/K)$ is abelain, and is known as the maximal abelian extension of K. We may write

$$\varprojlim_{L} \mathrm{Gal}(L/K) =: \mathrm{Gal}(K^{\mathrm{ab}}/K),$$

and one can check that the natural map $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ identifies with the abelinization of $\mathrm{Gal}(\overline{K}/K)$. To our aim of generalizing the above story, we would now like to define Frobenius elements inside this group. In light of exercise 1.7 (6.c), we see that it is important to pass to the quotient $\mathrm{Gal}(K^{\mathrm{ab}}/K)$, as in general these will only be defined up to conjugacy. However, we still have a problem that in general the existence of Frobenius elements are only well-defined for unramified extensions, as seen in exercise 1.7 (6). For a finite set of prime ideals S of K, we may consider the quotients

$$\varprojlim_{L^S} \mathrm{Gal}(L^S/K) := \mathrm{Gal}(K^S/K),$$
$$(\text{resp. } \varprojlim_{L^S} \mathrm{Gal}(L^S/K) := \mathrm{Gal}(K^{S,\mathrm{ab}}/K))$$

defined by the set of finite extensions $K \subset L^S \subset \overline{K}$ (resp. $K \subset L^S \subset K^{\mathrm{ab}}$) such that, for all prime ideals $\mathfrak{p} \notin S$, $\mathfrak{p}$ is unramified inside L^S. As before, the algebraic extension $K \subset K^S \subset \overline{K}$ (resp. $K \subset K^{S,\mathrm{ab}} \subset \overline{K}$) is defined by the compositum of the collection of all the finite extensions appearing in the above limits, and we refer to them as the maximal unramified extension outside S (resp. maximal abelian unramified extension outside S). The groups $\mathrm{Gal}(K^S/K)$ (resp. $\mathrm{Gal}(K^{S,\mathrm{ab}}/K)$) are the infinite Galois groups of these infinite extensions. As before, it is clear from the definition that there is a natural map $\mathrm{Gal}(K^S/K) \to \mathrm{Gal}(K^{S,\mathrm{ab}}/K)$, which one can verify identifies with the abelianization of $\mathrm{Gal}(K^S/K)$.

Inside these infinite Galois groups, we can now construct our Frobenius elements.

Construction 1.9. *For a number field $K/\mathbb{Q}$ and a finite set of prime ideals S of K and all $\mathfrak{p} \notin S$, we construct a conjugacy class of elements $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(K^S/K)$ (resp. element $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(K^{S,\mathrm{ab}}/K)$) as follows.*

1. *For all finite Galois extensions $K \subset L \subset K^S$, we fix an unramified prime $\mathfrak{P}(L)|\mathfrak{p}$ lying above $\mathfrak{p}$. We consider the conjugacy class of elements $[\mathrm{Frob}_\mathfrak{p}(\mathfrak{P}(L))] \subset \mathrm{Gal}(L/K)$ given by Exercise 1.7 6 (b).*
2. *We choose the prime ideals in (1) such that if we have an inclusion $K \subset L_1 \subset L_2 \subset K^S$, we have that $\mathfrak{P}(L_2)|\mathfrak{P}(L_1)$ then it follows that if we look at the restriction map*
$$\mathrm{Gal}(L_2/K) \to \mathrm{Gal}(L_1/K)$$
that the conjugacy class $[\mathrm{Frob}_\mathfrak{p}(\mathfrak{P}(L_2))]$ maps to the conjugacy class $[\mathrm{Frob}_\mathfrak{p}(\mathfrak{P}(L_1))]$.
3. *In light of (2), we may choose a choice of representatives $\{\mathrm{Frob}_\mathfrak{p}(\mathfrak{P}(L))\}_{K\subset L\subset K^S} \in \varprojlim_{K\subset L\subset K^S} \mathrm{Gal}(L/K) = \mathrm{Gal}(K^S/K)$ of the conjugacy classes compatible under restriction. One can check that this is well-defined up to conjugacy in $\mathrm{Gal}(K^S/K)$ (cf. the last part of the proof of Proposition 2.13).*
4. *As the natural map $\mathrm{Gal}(K^S/K) \to \mathrm{Gal}(K^{S,\mathrm{ab}}/K)$ identifies with the abelianization, the construction in (3) gives rise to a well-defined element $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(K^{S,\mathrm{ab}}/K)$ which only depends on the prime ideal $\mathfrak{p} \notin S$.*

With the Frobenius elements now constructed, we might worry that we have departed too much from our original goal of explicating characters of the form
$$\chi : \mathrm{Gal}(\overline{K}^{\mathrm{ab}}/K) \to \mathbb{C}^*,$$
as we have only constructed Frobenius elements in a certain quotient of $\mathrm{Gal}(K^{S,\mathrm{ab}}/K)$ of the group $\mathrm{Gal}(\overline{K}^{\mathrm{ab}}/K)$. However, we recall that, for any finite extension L/K, it must be unramified outside of some finite set of prime ideals S (as any ramified prime ideal must occur in the factorization of the discriminant of the extension L/K). In particular, this formally implies that we have
$$\mathrm{Gal}(\overline{K}/K) \xrightarrow{\simeq} \varprojlim_S \mathrm{Gal}(K^S/K)$$
and
$$\mathrm{Gal}(K^{S,\mathrm{ab}}/K) \xrightarrow{\simeq} \varprojlim_S \mathrm{Gal}(K^{S,\mathrm{ab}}/K)$$
where the map is induced by the natural quotient maps, and we note that, for any inclusion $S \subset T$ of sets of prime ideals, we have a natural inclusion $K^T \subset K^S$ and therefore a natural map $\mathrm{Gal}(K^S/K) \to \mathrm{Gal}(K^T/K)$. In particular, all characters χ of arithmetic interest will always factor through $\mathrm{Gal}(K^S/K)$ for some finite set of prime ideals S of K.

We now come to the main Theorem describing the structures of these groups in the case of $K = \mathbb{Q}$, which tells us that Theorem 1.6 is sufficient for completely understanding $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ and in turn a general character $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{C}^*$, at least assuming it factors through $\mathrm{Gal}(\mathbb{Q}^S/\mathbb{Q})$ for some finite set of primes S.

Theorem 1.10 (The Kronecker–Weber Theorem and Class Field Theory over $\mathbb{Q}$)**.** *The following is true.*

1. *There is an equality of fields*
$$\mathbb{Q}^{\mathrm{ab}} = \bigcup_{n\geq 1} \mathbb{Q}(\zeta_n),$$
where ζ_n is a primitive n-th root of unity. In particular, every finite abelian extension $\mathbb{Q} \subset L \subset \mathbb{Q}^{\mathrm{ab}}$ is contained in a cyclotomic field.

(2) *In light of the identification*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \;\cong\; (\mathbb{Z}/n\mathbb{Z})^\times,$$

of Theorem 1.6 (1), passing to the inverse limit yields a canonical isomorphism of profinite groups

$$\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \;\cong\; \varprojlim_n (\mathbb{Z}/n\mathbb{Z})^\times \;=: \widehat{\mathbb{Z}}^\times.$$

We note, by the Chinese remainder theorem, we have an identification

$$\widehat{\mathbb{Z}}^\times \simeq \prod_q \mathbb{Z}_q^*, \tag{1.8}$$

where $\mathbb{Z}_q^*$ denotes the invertible elements in the q-adic integers, for q varying over prime numbers.

(3) *Let S be a finite set of primes of $\mathbb{Q}$. For $n \in \mathbb{Z}$, we write* $\mathrm{supp}(n)$ *for the collection of primes dividing n. Then*

$$\mathbb{Q}^S \;=\; \bigcup_{\substack{n\geq 1\\ \mathrm{supp}(n)\subset S}} \mathbb{Q}(\zeta_n),$$

and there is a canonical isomorphism

$$\mathrm{Gal}(\mathbb{Q}^S/\mathbb{Q}) \;\cong\; \varprojlim_{\substack{n\\ \mathrm{supp}(n)\subset S}} (\mathbb{Z}/n\mathbb{Z})^\times.$$

Equivalently,

$$\mathrm{Gal}(\mathbb{Q}^{S,\mathrm{ab}}/\mathbb{Q}) \;\cong\; \prod_{q\in S} \mathbb{Z}_q^\times, \tag{1.9}$$

under the identification of (1.8).

(4) *As in Theorem 1.6 (4), under the identification*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \;\cong\; (\mathbb{Z}/n\mathbb{Z})^\times,$$

the Frobenius element Frob_p *corresponds to the residue class*

$$\mathrm{Frob}_p \;\longleftrightarrow\; p \bmod n.$$

for $p \nmid n$.

Passing to the inverse limit, the Frobenius element at a prime $p \notin S$ corresponds in $\mathrm{Gal}(\mathbb{Q}^S/\mathbb{Q})$ *to the element*

$$(p)_q \in \prod_{q\in S} \mathbb{Z}_q^\times, \qquad (p)_q = p \in \mathbb{Z}_q^\times.$$

In particular, we observe that the group $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ has a remarkably simple structure which is completely describable in terms of the multiplicative structure of certain completions attached to $\mathbb{Q}$ (namely, $\mathbb{Z}_q^*$ for varying primes q). Moreover, this is setup in such a way that passing to the Galois group $\mathrm{Gal}(\mathbb{Q}^{S,\mathrm{ab}}/\mathbb{Q})$ with restricted ramification corresponds to only looking at the completions for $q \in S$ and such that the Frobenius element at p corresponds to the q-adic unit $p \in \mathbb{Z}_q^*$.

As we will discuss in more detail later in the course, this is indeed a general phenomenon. In particular, for any number field $K/\mathbb{Q}$, the profinite group $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ will be explicitly describable in terms of the multiplicative structure of the groups $K_{\mathfrak{q}}$, and $\mathrm{Gal}(K^{\mathrm{ab},S}/K)$ will be describable in terms of the completions $K_{\mathfrak{q}}$ for $\mathfrak{q} \in S$. In such a way that the Frobenius elements $\mathrm{Frob}_{\mathfrak{p}}$ will correspond to certain units in $\mathcal{O}_{K_{\mathfrak{q}}}$. This comprises the main content of what is known as global class field theory. The goal of the course will be to explain the statement and proofs of these statements, and show how it can be used to illuminate arithmetic phenomenon such as quadratic reciprocity.

2. Galois Cohomology, Reference: [Ser94; Mil20a; NSW08; Ked02; Neu99]

We saw in the §1 that of utmost interest for us will be groups of the form

$$G := \varprojlim_{i \in I} G_i,$$

which are projective limits of finite groups G_i, as in (1.2). This is what is known as a pro-finite group. In particular, we were interested in understanding the abelianization

$$G^{\mathrm{ab}} := G/[G, G]$$

of such a group where $[G, G] \subset G$ denotes the subgroup of commutators. In §1, the interest in the abelianization came from the technical requirement to have well-defined Frobenius elements, as in 1.9 (6)-(c). However, the passage to this abelianization will accomplish much more. In particular, as we will see, the abelianization of the group may be re-expressed

$$G^{\mathrm{ab}} \simeq H_{1,\mathrm{cont}}(G, \mathbb{Z})$$

where the RHS will be the 1st continuous homology group of the profinite group G, where $\mathbb{Z}$ will be the integers equipped with the trivial G-action and the discrete topology[1]. As the notation suggests, this group is part of a family $H_{i,\mathrm{cont}}(G, \mathbb{Z})$ for $i \in \mathbb{N}_{\geq 0}$. These will be known as the continuous homology groups of G, which will provide us the essential computation tool for computing $H_1^{\mathrm{cont}}(G, \mathbb{Z})$ and in turn proving the main results of class field theory. To this aim, we begin by describing the structure of profinite groups and building up this algebraic machine known as group (co)-homology.

2.1. **Preliminaries.**

2.1.1. *Profinite Groups.* We start with the basic definition.

Definition 2.1. A topological group G is a said to be *profinite* if it is the projective limit of finite groups

$$\varprojlim_{i \in I} G_i = G,$$

where each of the groups is endowed with the discrete topology, and the inverse limit is computed in the category of topological groups (so that G is endowed with the minimal topology such that the projection maps $G \to G_i$ are continuous for all $i \in I$).

One of the basic reasons to keep track of the topology is the following alternative characterization of such groups.

Proposition 2.2. *A topological group G is profinite if and only if it is compact, totally disconnected, and Hausdorff.*

Proof. We prove the two implications separately.

(⇒) It follows from the definition of profinite, that there exists some directed set $(I, \geq)$ such that we have a continuous map

$$\alpha : G \to \prod_{i \in I} G_i,$$

where the target is endowed with the product topology, and the image is identified with the set of tuples $(g_i)_{i \in I}$ such that $f_{jk}(g_k) = g_j$ for all $j \leq k$ in I. Here $f_{jk} : G_k \to G_j$ denotes the transition maps in a presentation of $G := \varprojlim_{i \in I} G_i$ as a projective limit with respect to the directed set $(I, \geq)$.

[1] As we will discuss later, the homology of a pro-finite group will not be well-behaved if the group is not finite. This will make it more natural to consider the dual notion or what is known as the cohomology. However, we ignore this technical point for the introduction.

In particular, for varying $j \leq k$ in I, the image of α is the intersection of the $A_{jk} := \{(g_i)_{i\in I} | f_{jk}(g_k) = g_j\}$. However, A_{jk} is the preimage of diagonal in $X_j \times X_j$ under the tautologically continous map $\prod_{i\in I} G_i \xrightarrow{p_j \times p_k} G_j \times G_k \xrightarrow{\mathrm{id}\times f_{jk}} G_j \times G_j$. In particular, A_{jk} is closed inside $\prod_{i\in I} G_i$ and therefore so is G. By the Tychonoff theorem, we know that $\prod_{i\in I} G_i$ is compact, and therefore G is as well. Similarly, $\prod_{i\in I} G_i$ is easily checked to be Hausdorff and totally disconnected so that G is as well.

($\Leftarrow$) Let G be a compact totally disconnected Hausdorff topological group. For any locally compact totally disconnected group, it follows (e.g by van-Dantzig's theorem) that the identity element has a basis of open neighborhoods given by open subgroups $U \subset G$. We consider such a $U \subset G$. This automatically has finite index since G is compact. Hence, its conjugates gUg^{-1} are finite in number and therefore their intersection $V \subset G$ is an open normal subgroup. Therefore, we conclude the set of open normal subgroups $V \subset G$ form a basis of open neighborhoods of the identity element. We consider the natural continous map

$$G \to \varprojlim G/V,$$

where V ranges over all such subgroups. The map is injective continuous, and has dense image, and therefore it is an isomorphism. Indeed, both sides are easily verified to be compact Hausdorff by the argument given above (see Lemma 2.3 (1)), so the map is automatically closed. □

Note that in the proof we also exhibited proofs of the following claims, which we record for future use.

Lemma 2.3. *The following is true.*

1. *A projective limit $X := \varprojlim_{i\in I} X_i$ of compact (resp. totally disconnected, Hausdorff) topological spaces X_i endowed with the inverse limit topology is also compact (resp. totally disconnected, Hausdorff).*
2. *For a profinite group G, the identity element has a basis of open neighborhoods $U_i \subset G$ for some directed set $(I, \geq)$ given by open (hence of finite index) normal subgroups and the ordering is determined by inclusion. In particular, we can always find an isomorphism*

$$G \xrightarrow{\simeq} \varprojlim_{i\in I} G/U_i,$$

of topological groups.

Remark 2.4. For (2), we note that, given a presentation

$$G = \varprojlim_{i\in I} G_i,$$

we may simply take $U_i := \mathrm{Ker}(G \xrightarrow{\pi_i} G_i)$.

We have the following basic examples.

Example 2.5.

1. Let L/K be an extension of fields which can be written as the union of its finite Galois subextensions $K \subset L_i \subset L$. We then define the infinite Galois group

$$\mathrm{Gal}(L/K) := \varprojlim_{i\in I} \mathrm{Gal}(L_i/K),$$

   where the limit is over finite Galois extensions $K \subset L_i \subset L$ and the ordering on I is determined by inclusion. Since the compositum of two finite Galois extension is again finite Galois, the set I is directed and therefore $\mathrm{Gal}(L/K)$ is a profinite group.
2. We recall that the p-adic numbers $\mathbb{Z}_p$ are a profinite group with presentation

$$\mathbb{Z}_p \simeq \varprojlim_{n\to 1} \mathbb{Z}/p^n\mathbb{Z}.$$

Similarly, if we consider the group $\mathrm{GL}_n(\mathbb{Z}_p)$ of $n \times n$ invertible matrices with coefficients in $\mathbb{Z}_p$ then this is also a profinite group with presentation given by

$$\mathrm{GL}_n(\mathbb{Z}_p) \simeq \varprojlim_{n \geq 1} \mathrm{GL}_n(\mathbb{Z}/p^n\mathbb{Z}_p).$$

(3) Let G be a discrete topological group, and let $\hat{G}$ be the projective limit of the finite quotients of G. The group $\hat{G}$ is known as the *pro-finite* completion of G. We note that there is a natural map

$$G \to \hat{G}$$

with kernel given by the intersection of all groups of finite index. If we apply this to the group $\mathbb{Z}$ then we obtain what is known as the Prüfer ring

$$\hat{\mathbb{Z}} := \varprojlim_{n \in \mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$$

which by the Chinese remainder theorem is isomorphic to a direct product

$$\hat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p \tag{2.1}$$

indexed by all prime numbers p.

We also have the following important examples of profinite groups coming from duality.

Exercise 2.6. *If M is an abelian group then we define its Pontryagin dual to be $M^* := \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z})$.*

(1) Construct isomorphisms of the form

$$(\mathbb{Z}/n\mathbb{Z})^\vee \simeq \mathbb{Z}/n\mathbb{Z}$$
$$(\mathbb{Q}_p/\mathbb{Z}_p)^\vee \simeq \mathbb{Z}_p,$$

for p a prime number and $n \geq 1$ an integer. Show that

$$\mathbb{Q}^\vee \simeq 0.$$

(2) Suppose that M is a torsion abelian group endowed with the discrete topology. Endow M^* with topology given by pointwise convergence (I.e consider the embedding $M \hookrightarrow M^{\mathbb{Q}/\mathbb{Z}}$, where $M^{\mathbb{Q}/\mathbb{Z}}$ is given the product topology and M is given the subspace topology). Prove that M^* is a commutative profinite group (Hint: write M^* as a directed limit or union of its finite subgroups).

(3) For M a torsion abelian group check that the natural evaluation map

$$\mathrm{ev}_M : M \to (M^*)^*$$
$$m \mapsto (\chi \mapsto \chi(m))$$

is an isomorphism of abelian groups. We let let **TorAb** *be the category of* discrete torsion *abelian groups. Let* **ProFinAb** *be the category of* profinite *(equivalently: compact, Hausdorff, totally disconnected topological) abelian groups (with morphisms being continuous homomorphisms). The above duality upgrades to a contravariant equivalence*

$$\mathbf{TorAb}^{\mathrm{op}} \simeq \mathbf{ProFinAb}.$$

of categories. This is known as Pontryagin duality.

(4) Prove that Pontryagin dual of a torsion-free profinite abelian group is a divisible abelian group.

(5) Combine (1), (4), and Exercise 2.7 below, to deduce that any commutative torsion free profinite group is isomorphic to a (possibly-infinite) product of copies of $\mathbb{Z}_p$ for some prime numbers p.

Exercise 2.7. *Let A be a divisible abelian group, i.e. for every $a \in A$ and every integer $n \geq 1$ there exists $b \in A$ with $nb = a$.*

(1) Show that a finite divisible abelian group is trivial.
(2) Show that A a divisble abelian group is a $\mathbb{Q}$-vector space if and only if it is torsion-free.
(3) Let

$$A_{\text{tors}} := \{a \in A \mid \exists n \geq 1 \text{ with } na = 0\}.$$

Show that A_{tors} is a divisible subgroup of A.
(4) Prove that A_{tors} decomposes canonically as a direct sum of its p-primary components

$$A_{\text{tors}} = \bigoplus_p A[p^\infty], \qquad A[p^\infty] := \{a \in A \mid \exists n \text{ with } p^n a = 0\}.$$

(5) Fix a prime p. Show that every divisible p-primary (in the sense that for every element a there exists $n \geq 0$ such that $p^n a = 0$) abelian group D contains a nonzero element of order p^n for all $n \geq 1$ unless $D = 0$.
(6) Show that $\mathbb{Q}_p/\mathbb{Z}_p$ is a divisible p-primary group.
(7) Prove that any divisible p-primary abelian group is a direct sum of copies of $\mathbb{Q}_p/\mathbb{Z}_p$.
(8) Show that there exists a (non-canonical) decomposition

$$A \cong A_{\text{tors}} \oplus A/A_{\text{tors}}.$$

(9) Show that A/A_{tors} is torsion-free and divisible, hence a $\mathbb{Q}$-vector space by (3).
(10) Deduce that there exist cardinals κ and $\{\lambda_p\}_p$ such that

$$A \cong \mathbb{Q}^{(\kappa)} \oplus \bigoplus_p (\mathbb{Q}_p/\mathbb{Z}_p)^{(\lambda_p)},$$

where p varies over all prime numbers.

(Hint: Use that divisible abelian groups are injective objects (See Definition 2.22) in the category of abelian groups, so short exact sequences with divisible terms split. For the p-primary case, reduce to showing that a nonzero divisible p-group contains a copy of $\mathbb{Q}_p/\mathbb{Z}_p$ and then use Zorn's lemma to obtain a maximal direct sum of such copies.)

With the basic examples out of the way, let's turn towards the structure of the subgroups profinite groups

Lemma 2.8. *Let $H \subset G$ be a subgroup of a profinite G. Then the following is true.*

(1) If $H \subset G$ is an open subgroup then it is also closed and of finite index. Conversely, if $H \subset G$ is closed and has finite index then it is open.
(2) If $H \subset G$ is a closed subgroup then H is also profinite.

Proof. For (1), this is an easy consequence of the fact that, since G is compact, any open subgroup H is of finite index, since we can write G as a union of translates of H. In particular, this shows that we can write H as the complement of its finitely many non-trivial translates implying it is closed. The converse direction is similar. In particular, if $H \subset G$ is closed and of finite index then H is the complement of its finitely many closed translates.

For (2), we consider a presentation

$$G = \varprojlim_{i \in I} G/U_i,$$

as in Lemma 2.3 (2). We then have a natural map

$$H \to \varprojlim_{i \in I} H/(H \cap U_i),$$

which is easily checked to be continuous and injective with dense image. However, since $H \subset G$ is closed, this is a map of compact Hausdorff spaces using Lemma 2.3 (1), so we conclude that is an isomorphism. □

These basic topological facts can be used to great effect to understand the structure of certain profinite groups.

Example 2.9. A particularly nice example of profinite groups is that of pro-cyclic groups. In particular, we say a profinite group G is pro-cyclic if there exists $g \in G$ such that $G = \overline{\langle g \rangle}$, where $\overline{(-)}$ denotes the operation of taking closure. We note that $\hat{\mathbb{Z}}$ and $\mathbb{Z}_p$ of Example 2.5 (2) and (3) are nice examples of procyclic groups.

In this case, we may find a nice basis of open normal subgroups by taking the subgroups $G^n \subset G$ for $n \geq 1$ of nth powers. It is easy to see that these subgroups are closed. Indeed, the multiplication by n map is continuous, since G is a topological group, and therefore $(-)^n : G \to G$ is a continuous map between compact Hausdorff spaces and therefore sends closed subsets to closed subsets. In particular, the image of G^n of this map is closed. However, G is also of finite index and therefore open by 2.8 (1). Indeed, the natural map $\langle g \rangle / \langle g^n \rangle \to G/G^n$ identifies the target with a dense subgroup of the source, and therefore is an isomorphism. Conversely, we note that if $H \subset G$ is any open normal subgroup then it is of finite index by by lemma 2.8 (1) since $G^n \subset H$ as long as $n \geq [G : H]$.

We now have the following technical lemma, which will play an important technical role in explicating the cohomology of profinite groups.

Proposition 2.10. *Suppose $K \subset H \subset G$ are an inclusion of two closed subgroups of G. Then the natural map $G/K \to G/H$ admits a continuous section $s : G/H \to G/K$.*

Proof. We start out with the following special case.

Lemma 2.11. *Suppose that $K \subset H$ is an inclusion of closed subgroups such that K has finite index in H then $G/K \to G/H$ admits a continuous section.*

Proof. Let U be an open normal subgroup of G such that $U \cap H \subset K$. The restriction of the map $G/K \to G/H$ to the image of U in G/K will then be injective. Its inverse map is therefore a section over the image of U inside G/H which is open by the finite index assumption. One may then extend to a section over all of G/H by translation. □

For the general case, first note that, by replacing G with G/K, we may assume without loss of generality that $K = 1$.

Let X be the set of pairs (S, s), where $S \subset H$ is a closed subgroup of H and s is a continous section of $G/H \to G/S$. This is equipped with a natural partial ordering $(S, s) \geq (S', s')$ if $S \subset S'$ and the induced diagram

$$s : G/H \xrightarrow{s'} G/S' \to G/S$$

commutes. Suppose we have a totally ordered family (S_i, s_i) of elements of X with respect to the partial ordering defined above. We set $S = \cap_{i \in I} S_i$. We note that $S \subset G$ is closed and the natural map

$$G/S \to \varprojlim_{i \in I} G/S_i$$

is an isomorphism of topological groups. Indeed, it is injective and continuous with dense image, and all the spaces are compact Hausdorff using Lemma 2.3 (2). Using this, we may find an element (S, s) that lies above all the (S_i, s_i) in the partial ordering.

We are therefore in a position in which we may invoke Zorn's lemma. We let (S, s) be the resulting maximal element. Let us show that $S = 1$. Suppose that this is not the case. Then, by Lemma 2.3 (2) and Lemma 2.8 (2), this would imply that there exists an open subgroup $U \subset G$ such that

$U \cap S \neq S$. We apply Lemma 2.11 $G/(S \cap U) \to G/S$ to deduce a section of the natural map, and composing this with the section $s : G/H \to G/S$ gives a contradiction to maximality of (S, s) in light of Lemma 2.8 (1). □

A protypical example of a closed subgroup which is not open is the subgroup $\mathbb{Z}_p \subset \hat{\mathbb{Z}}$ given by the inclusion of the pth coordinate in the isomorphism (2.1). The notion of index of course does not make sense for such a subgroup in any kind of naive way. However, as profinite groups are built out of limits of finite groups, this does make sense up to modifying are expectations in a controlled way.

Definition 2.12. We define the following.

(1) A *supernatural number* is a formal product $\prod_p p^{n_p}$, where p ranges over all prime numbers and n_p is an integer that is ≥ 0 or is equal to ∞. We note that we may define the lcm and gcd of such numbers in the obvious way.
(2) For $H \subset G$, the inclusion of a closed subgroup into a profinite group G. We define the index $[G : H]$ to be the supernatural number defined as the lcm of the indeces $[G/U : H/(H \cap U)]$ as U runs over the set of open normal subgroups of G. We define the order of a profinite G to be $[G : 1]$.
(3) We say a group G is *pro-p* if the supernatural number given by its order is a power of p. Equivalently, if it is a projective limit of finite p-order groups.
(4) We say a closed subgroup $H \subset G$ is a p-Sylow subgroup if it is pro-p and the index $[G : H]$ is of order prime to p.

We can now bootstrap the usual Sylow theorems to the profinite context.

Proposition 2.13. *Every profinite subgroup G has Sylow p-Sylow subgroup, and these are all conjugate.*

Proof. The key will be to use the following lemma, which is of manifold use when bootstraping claims from the finite context to the pro-finite context.

Lemma 2.14. *A projective limit $X := \varprojlim_{i \in I} X_i$ for a directed set $(I, \geq)$ of non-empty finite sets is non empty.*

Proof. Recall, as in the proof of the forward implication of Proposition 2.2, we have that X may be identified with the intersection of the closed subsets

$$A_{jk} := \{(x_i)_i \in X \mid f_{jk}(x_k) = x_j\}.$$

For all $j \leq k$ in I inside $\prod_{i \in I} X_i$, where X_i is endowed with the discrete topology and $\prod_{i \in I} X_i$ is endowed with the product topology. The claim is reduced to showing that the intersection of all these sets is non-empty.

As in 2.2, $\prod_{i \in I} X_i$ is compact by Tychonoff and therefore so is A_{jk}. By a standard compactness argument, the claim is therefore reduced to showing that given finitely many $A_{j_1 k_1}, \ldots, A_{j_r k_r}$ their intersection is non-empty. Let J be the finite set of indices appearing. Since I is directed, there exists $m \in I$ with $m \geq k$ for all $j \in J$. Choose any $x_m \in X_m$. For each $k \in J$ define $x_k := f_{mk}(x_m)$, and choose arbitrary elements in $\prod_{i \in I} X_i$ for indices outside J. This defines an element in the intersection $A_{j_1 k_1} \cap \cdots \cap A_{j_r k_r}$, showing the claim. □

Now let I be the directed set determined by a family of open normal subgroups $\{U_i\}_{i \in I}$ of G as in Lemma 2.3 (2). For each $i \in I$, let $P(U_i)$ be the set of Sylow p-subgroups in the finite group G/U. We consider the inverse system $\varprojlim_{i \in I} P(U_i)$ noting that this is well-defined as the transition morphisms $G/U_i \to G/U_j$ are all surjective maps of finite groups, which therefore carries p-Sylow subgroups to p-Sylow subgroups. By applying Lemma 2.14 and invoking the usual Sylow theorems, we obtain a subgroup $H = \varprojlim_{i \in I} H_i$, which one easily checks will be a p-Sylow subgroup of H.

Given any two such choices H and H' of such a p-Sylow subgroup, we consider, for $i \in I$, the set $Q(U_i)$ of elements which conjugate the image of H in G/U_i to H'. By applying Lemma 2.14 to the inverse system $\varprojlim_{i\in I} Q(U_i)$ and invoking the usual Sylow theorems, we construct an element $x \in G$ such that $xHx^{-1} = H'$, as desired. □

We now want to review the following situation in which profinite groups will show up for us in full force.

2.1.2. *Aside on Infinite Galois Theory.* We recall the following basic assertion of Galois theory.

Theorem 2.15. *Let L/K be a finite Galois extension. Then the normal subgroups $H \subset G$ correspond to Galois subextensions $M \subset L$. The correspondence is given by taking a subgroup H to the fixed field L^H and $L/M/K$ to $\mathrm{Gal}(L/M)$.*

As we have already seen in Example 2.5 (1) and in §1, for an infinite Galois extension L/K we may write L as the compositum of finite Galois extensions L_i/K in some index set $i \in I$ and form the inverse limit

$$\mathrm{Gal}(L/K) = \lim_{i\in I} \mathrm{Gal}(L_i/K)$$

to endow the Galois group of this infinite extension with the structure of a profinite group. If $L = K^{\mathrm{sep}}$ denotes the seperable closure of the field K (which agrees with the algebraic closure if K is a perfect field) then it is the inverse limit

$$\lim_{i\in I} \mathrm{Gal}(K_i/K),$$

where K_i runs over all finite Galois extensions of K. We refer to the resulting profinite group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$, as the absolute Galois group of K.

Example 2.16. We set $q = p^f$ for p a prime. We let $\mathbb{F}_q$ be the unique finite extension of $\mathbb{F}_p$ of degree f. Similarly, for all $n \geq 1$, recall that $\mathbb{F}_q$ has exactly one finite extension of degree n which we denote by $\mathbb{F}_{q^n}$. Moreover, the Galois group $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ and is generated by the Frobenius element Frob_p sending $x \mapsto x^p$. The absolute Galois group of $\mathbb{F}_q$ in this case is given by

$$\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \simeq \lim_{n\geq 1} \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \simeq \lim_{n\geq 1} \mathbb{Z}/n\mathbb{Z} =: \hat{\mathbb{Z}},$$

where the RHS is the Prüfer ring introduced in 2.5 (3).

We now want to formulate a version of Galois theory that applies to infinite extensions. In particular, we want to say that subgroups of $\mathrm{Gal}(L/K)$ should correspond to (possibly) infinite subextensions of $L/L'/K$. However, we clearly need to be a bit careful. In particular, the Galois groups of the subextensions should correspond to these subgroups, and therefore they should also be profinite. A simple way of guaranteeing this in light of Lemma 2.8, is to only look at closed subgroups of $\mathrm{Gal}(L/K)$. This leads to the fundamental Theorem of infinite Galois theory.

Theorem 2.17. *Let L/K be a (not necessarily finite) Galois extension. Then there is a correspondence between Galois subextensions $M \subset L$ and normal closed subgroups $H \subset \mathrm{Gal}(L/K)$ given by*

$$H \mapsto L^H$$

and $L/M/K$ to

$$M \mapsto \mathrm{Gal}(L/M).$$

Moreover, the resulting extension L^H is finite if and only if the subgroup $H \subset \mathrm{Gal}(L/K)$ is open. Moreover, if M is the fixed field of a normal subgroup H, we have an isomorphism $\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(L/K)/H$.

Proof. See [Neu99, Chapter 4, Section 1, Theorem 1.2] □

Instead of giving a proof, we give some flavor for what this is saying by working out an important example.

Exercise 2.18. *Consider the infinite Galois extension* $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$. *We recall that we have an isomorphism* $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \simeq \hat{\mathbb{Z}}^*$ *by Theorem 1.10 (2). We now work out what infinite Galois theory is telling us in this particular case.*

1. *Show that we have an isomorphism* $\mathbb{Z}_p^* \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$ *if* p *is off and that* $\mathbb{Z}_2^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$. *Deduce the existence of a surjective continuous map* $\hat{\mathbb{Z}}^* \to \hat{\mathbb{Z}}$ *of profinite groups (Hint: use the* p*-adic exponential map).*
2. *Classify all closed subgroups of* $\hat{\mathbb{Z}}^*$ *using part (1) and the isomorphism* $\hat{\mathbb{Z}}^* \simeq \prod_p \mathbb{Z}_p^*$. *Deduce that* $1 + n\hat{\mathbb{Z}}$, $\prod_p 1 + p^{e_p}\mathbb{Z}_p$ *for* $e_p \geq 1$, *and* $\langle \pm 1 \rangle$ *define closed subgroups of* $\hat{\mathbb{Z}}^*$.
3. *Identify the (possibly infinite abelian extensions) that correspond to the closed subgroups* $1 + n\hat{\mathbb{Z}}$, $\prod_p 1 + p^{e_p}\mathbb{Z}_p$ *for* $e_p \geq 1$, *and* $\langle \pm 1 \rangle$ *described in (2) under infinite Galois Theory.*

We now turn to the cohomology of groups. We begin first with the finite case.

2.2. **Cohomology of Finite Groups.** For the rest of this subsection, we will let G denote a finite group.

2.2.1. *A Bit of Abstract Nonsense.* We write Mod_G for the abelian category with objects given by abelian groups $(A, +)$ with a left action $G \times A \to A$ $(g, a) \mapsto g.a$ of the group G, and morphisms given by G-equivariant maps $f : A \to B$.

Remark 2.19. We can consider the group ring $\mathbb{Z}[G]$ which is given by the collection of formal linear combinations $\sum_{g \in G} a_g g$, where $a_g \in \mathbb{Z}$ and $g \in G$ is an element. This has an obvious addition operation given by adding the coordinates and an obvious (not necesarilly commutative) multiplication induced by the multiplication on G. We note that we can identify Mod_G with the category of left $\mathbb{Z}[G]$-modules under this ring.

We will be interested in the functor

$$(-)^G : \mathrm{Mod}_G \to \mathrm{Ab} \tag{2.2}$$

of G-invariants, where Ab denotes the category of abelian groups. I.e $A^G := \{a \in A | g.a = a\}$ is the subgroup of elements which are fixed under the action of G. The cohomology of groups arises by considering how this functor interacts with the notion of short exact sequences

$$0 \to A \to B \to C \to 0 \tag{2.3}$$

in the category Mod_G. These are just usual short exact sequences in the category of abelian groups, but we insist that the morphisms are in the category Mod_G. In particular, given such a short exact sequence, we obtain an induced left exact sequence

$$0 \to A^G \to B^G \to C^G, \tag{2.4}$$

where injectivity of the map $A^G \to B^G$ is clear; however, surjectivity of the map $B^G \to C^G$ does not hold in general.

Exercise 2.20. *Let* $G = C_p$ *be the cyclic group of order* p, *and let* $k = \mathbf{F}_p$. *We consider the* G*-modules*

$$M = k[G] \qquad N = k,$$

where $k[G]$ *is the group ring of* G *introduced above. We consider the natural map.*

$$\varepsilon : k[G] \to k, \qquad \varepsilon\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} a_g.$$

which is known as the augmentation morphism

(1) *Show that ε is sujrective.*
(2) *Show that M^G is one-dimensional and is spanned by*

$$s = \sum_{g \in G} g.$$

(3) *Compute the induced map on G-invariants*

$$\varepsilon^G : M^G \longrightarrow N^G$$

and show that it is the zero map.

Our main goal will be to extend the sequence (2.4) to a long exact sequence of abelian groups. The main tool will be to use the following, which is the basic building block of all homological algebra.

Lemma 2.21. ***(Snake Lemma)*** *Consider a commutative diagram of abelian groups with exact rows:*

$$\begin{array}{ccccccccc} & & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & & \end{array} \tag{2.5}$$

Then there exists a connecting homomorphism

$$\delta \colon \ker(\gamma) \longrightarrow \operatorname{coker}(\alpha)$$

such that the following sequence is exact:

$$\ker(\alpha) \longrightarrow \ker(\beta) \longrightarrow \ker(\gamma) \xrightarrow{\delta} \operatorname{coker}(\alpha) \longrightarrow \operatorname{coker}(\beta) \longrightarrow \operatorname{coker}(\gamma) \tag{2.6}$$

Moreover, if f is injective then this is exact on the left and if g' is surjective then this is exact on the right.

Proof. This is a standard diagram chase. In particular, we can construct the map δ by taking an element $c \in \operatorname{Ker}(\gamma) \subset C$ and lifting it to an element in B and then pushing to an element B' by the map β. By the commutativity of the diagram and the fact that $c \in \operatorname{Ker}(\gamma)$, this element will vanish upon applying g' and therefore lie in $\operatorname{Im}(f')$ (cf. [Wei80]). By similar arguments, one may check it is well-defined and gives rise to a sequence with the claimed exactness properties. □

The basic idea is now that we can use Lemma 2.21 to build up further terms of left exact sequence (2.4) of abelian groups, by embedding the terms of the original sequence (2.3) in Mod_G into another sequence defined by objects that behave in a simpler way with respect to taking invariants, and then using the snake lemma to conclude some consequences for the sequence (2.4) by taking invariants. More precisely, we want to consider the following.

Definition 2.22. An object $M \in \mathrm{Mod}_G$ is said to be *injective* if, for every commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{\phi} & M \\ \downarrow{\scriptstyle i} & & \\ B & & \end{array},$$

in Mod_G where $i : A \hookrightarrow B$ is an injective map of G-modules, there exists a map $\psi : B \to M$ such that the diagram commutes.

Remark 2.23. We note that we may equivalently think of injectivity as saying that the natural map

$$\mathrm{Hom}(B, M) \to \mathrm{Hom}(A, M)$$

induced by an injection $i : A \to B$ is always surjective, where we note that the injectivity is automatic by the injectivity of i.

Now suppose we have a short exact sequence

$$0 \to A \xrightarrow{i} B \to C \to 0,$$

where the object A is assumed to be injective. Then, by taking $i = \mathrm{id}_A$ in Definition 2.22, we note that injectivity allows us to deduce the existence of a splitting

$$0 \longrightarrow A \underset{s}{\overset{i}{\rightleftarrows}} B \longrightarrow C \longrightarrow 0$$

which gives us an isomorphism $B \simeq A \oplus C$. Similarly, if we take G-invariants then we get a diagram

$$0 \longrightarrow A^G \underset{s^G}{\overset{i^G}{\rightleftarrows}} B^G \longrightarrow C^G$$

which would in turn gives us a splitting $B^G \simeq A^G \oplus C^G$. In turn applying, this a priori only left exact sequence is right exact for injective objects. Therefore, by embedding a general short exact sequence (2.3) into a short exact sequence involving injective objects, we will obtain an interesting structure by taking G-invariants and using Lemma 2.21. We now have the following basic fact which tells us that we can always do this.

Exercise 2.24. *Show that, for every $A \in \mathrm{Mod}_G$, there exists an injection $A \hookrightarrow M$ in Mod_G such that M is injective (Hint: first think about the case of usual abelian groups (e.g when G is trivial). We already discussed examples of injective objects in this category in Exercise 2.7).*

This exercise allows us to deduce the existence of the following.

Definition 2.25. We say an injective resolution of $M \in \mathrm{Mod}_G$ is a long exact sequence

$$0 \to M \to I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \xrightarrow{d^2} \cdots, \tag{2.7}$$

in Mod_G, where the objects I^j are all injective in the sense of Definition 2.22. We note that the existence of such a resolution is guaranteed by iteratively applying Exercise 2.24. We will denote such a resolution by the notation $M \to I^*$.

We now have the following sequence of invariants attached to any $M \in \mathrm{Mod}_G$.

Definition 2.26. Given $M \in \mathrm{Mod}_G$, we consider the injective resolution

$$I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \xrightarrow{d^2} \cdots,$$

of M, and apply $(-)^G : \mathrm{Mod}_G \to \mathrm{Ab}$. This gives us a sequence of maps

$$(I^0)^G \xrightarrow{(d^0)^G} (I^1)^G \xrightarrow{(d^1)^G} I^2 \xrightarrow{(d^2)^G} \cdots,$$

however this is not exact. Nonetheless, we still have, for all $i \geq 0$, an inclusion $\mathrm{Im}((d^i)^G) \subset \mathrm{Ker}((d^i)^G)$, where we set $(d^{-1})^G$ to be the natural map $0 \to (I^0)^G$. We form the cohomology groups

$$H^i(G, M) := \mathrm{Ker}((d^i)^G)/\mathrm{Im}((d^{i-1})^G) \in \mathrm{Ab}$$

which are known as the *group cohomology groups* of M. We observe, by the exactness of the sequence (2.7) defining the notion of injective resolution and the left exactness of the functor $(-)^G$, that we have a canonical identification

$$H^0(G, M) \simeq M^G.$$

We note that a priori this depends on the choice $M \to I^*$ of injective resolution. We will come back to this point in a second. For now, let us consider a G-module map $f : M \to N$, and suppose that we have an injective resolutions $0 \to M \to I^*$ and $0 \to N \to J^*$. We note that, by the lifting property of injective objects 2.22, we may inductively lift f to a map $f^i : I^i \to J^i$ for all $i \geq 0$, giving rise to a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & I^0 & \xrightarrow{d^0} & I^1 & \xrightarrow{d^1} & \cdots \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f^0} & & \downarrow{\scriptstyle f^1} & & \\ 0 & \longrightarrow & N & \longrightarrow & J^0 & \xrightarrow{d^0} & J^1 & \xrightarrow{d^1} & \cdots \end{array} \tag{2.8}$$

If we take G-invariants then we note that this is induces for us a morphism

$$H^i(f) : H^i(G, M) \to H^i(G, N)$$

on group cohomology. We now have the following basic lemma checking that this is well-defined.

Lemma 2.27. *The map $H^i(f)$ only depends on f and not on the choice of injective resolutions or of lifts f^i filling in the commutative diagram 2.8.*

Proof. It suffices to check that if $f = 0$ then $H^i(f) = 0$ for all $i \geq 0$, regardless of the choice of the lifts f^i. If $f = 0$ then for any choice of lifts f^i, we may, by exercise 2.28 construct morphisms $g^i : I^{i+1} \to J^i$ satisfying the identity

$$f^i = g^i \circ d^i + d^{i-1} \circ g^{i-1}.$$

In particular, if we take G-invariants and evaluate this on $a \in \mathrm{Ker}((d^i)^G)) \subset (I^i)^G$ representing a class in $H^i(G, M)$ then we see that

$$(f^i)^G(a) = (d^{i-1} \circ g^{i-1})^G(a) \in \mathrm{Im}((d^{i-1})^G)$$

which implies that it vanishes in $H^i(G, N)$. □

In the above proof, we implicitly used the following which we leave as an exercise.

Exercise 2.28. *Show that if we are given a map $f : M \to N$ in Mod_G such that $f = 0$ then, for any lifts f^i filling in a commutative diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & I^0 & \xrightarrow{d^0} & I^1 & \xrightarrow{d^1} & \cdots \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f^0} & & \downarrow{\scriptstyle f^1} & & \\ 0 & \longrightarrow & N & \longrightarrow & J^0 & \xrightarrow{d^0} & J^1 & \xrightarrow{d^1} & \cdots \end{array}$$

between injective resolutions $M \to I^*$ and $N \to I^*$, we may construct morphisms $g^i : I^{i+1} \to J^i$ such that

$$f^i = g^i \circ d^i + d^{i-1} \circ g^{i-1}.$$

(Hint: Proceed by induction on i and use the lifting property for injective objects).

We now have the following promised Corollary of this.

Corollary 2.29. *For $M \in \mathrm{Mod}_G$, the cohomology groups $H^i(G, M)$ do not depend on the choice of injective resolution $M \to I^*$.*

Proof. We apply Lemma 2.27 to $M = N$, the identity map, and two different injective resolutions of M. We see that the resulting map must give the identity on $H^i(G, M)$. □

In particular, as a consequence of the above discussion, we obtain well-defined functors

$$H^i(G, -) : \mathrm{Mod}_G \to \mathrm{Ab}$$

extending the functor of G-invariants. These are known as the right derived functors of $(-)^G$. We now have the following important property, which is easy consequence of Lemma 2.21.

Proposition 2.30. *Suppose we have a short exact sequence*

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

in Mod_G*. Then we have a long exact sequence*

$$0 \to H^0(G,A) \xrightarrow{H^0(f)} H^0(G,B) \xrightarrow{H^0(g)} H^0(G,C) \xrightarrow{\delta_0} H^1(G,A) \xrightarrow{H^1(f)} \cdots H^i(G,C) \xrightarrow{\delta_i} H^{i+1}(G,A) \to \cdots$$

in Ab*.*

These cohomology groups will be of utmost importance for us. We now turn our attention to computing with them.

2.2.2. *From the Abstract to the Concrete.* In order to render the cohomology groups computable, we note that they can be computed in terms of the following.

Definition 2.31. We define the following.

(1) We say that $M \in \mathrm{Mod}_G$ is *acylic* if $H^i(G,M) = 0$ is trivial for all $i \geq 1$.
(2) We say an *acylic resolution* of $M \in \mathrm{Mod}_G$ is a long exact sequence

$$0 \to M \to M_0 \xrightarrow{d^0} M_1 \xrightarrow{d^1} \cdots,$$

in Mod_G, where each M_i for $i \geq 0$ is acyclic in the sense of (1).

We now have the following, which essentially tells us that acylic resolutions are sufficient for computing cohomology.

Exercise 2.32. *Show the following.*

(1) Show that if $M \in \mathrm{Mod}_G$ is injective then it is acyclic. I.e that

$$H^i(G,M) = 0.$$

(Hint: We discussed how an injective map from an injective module must split, so apply this to the injective resolution.).

(2) Let $M \to M_*$ be an acyclic resolution of $M \in \mathrm{Mod}_G$. We apply G-invariants to the terms of the resolution and consider the resulting complex

$$M_0^G \xrightarrow{(d^0)^G} M_1^G \to \cdots M_i^G \xrightarrow{(d^i)^G} M_{i+1}^G \to \cdots$$

and consider, for all $i \geq 0$, the resulting cohomology

$$\mathrm{Ker}((d^i)^G)/\mathrm{Im}((d^{i-1})^G).$$

where we set $d_{-1}^G : 0 \to M_0^G$. Show that this is isomorphic to $H^i(G,M)$ (Hint: inductively apply the long exact cohomology sequence).

We will now be interested in constructing an acyclic resolution of a general G-module M. The recipe for doing this will be using the following functors.

Definition 2.33. Let $H \subset G$ be a subgroup. We define the following.

(1) We consider the functor

$$\mathrm{Ind}_H^G : \mathrm{Mod}_H \to \mathrm{Mod}_G$$
$$M \mapsto \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M,$$

where we have implicitly used the description of G and H-modules described in Remark 2.19.

(2) We consider the functor

$$\mathrm{Res}_H^G : \mathrm{Mod}_G \to \mathrm{Mod}_H$$

given by remembering the H-action and forgetting the rest of the action.

Remark 2.34. Alternatively, we may identify $\mathrm{Ind}_H^G(M)$ as the set of functions $\phi : G \to M$ such that $\phi(hg) = h.\phi(g)$ together with the G-action given by translation on the left. In particular, we may think of elements in $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M$ in terms of sums of elements

$$[g] \otimes m \in \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M,$$

where $[g]$ denotes a coset representative of $g \in G$ inside G/H. Given such a element, it corresponds to the function $\phi_{[g],m}$ taking an $g' \in G$ to $(g'g).m$ if $g'g \in H$ and 0 otherwise.

Remark 2.35.

We now have the following fundamental property of these operations, which effectively say they are an adjoint pair.

Proposition 2.36. ***(Frobenius Reciprocity)*** *Let $H \subset G$ be a subgroup, M a G-module, and N an H-module. Then we have the following isomorphisms between G-equivariant and H-equivariant Hom spaces*

$$\mathrm{Hom}_G(M, \mathrm{Ind}_H^G(N)) \simeq \mathrm{Hom}_H(\mathrm{Res}_H^G(M), N) \tag{2.9}$$

and

$$\mathrm{Hom}_G(\mathrm{Ind}_H^G(N), M) \simeq \mathrm{Hom}_H(N, \mathrm{Res}_H^G(M)), \tag{2.10}$$

which are natural in both M and N.

Proof. We first consider the case where $N = \mathrm{Res}_H^G(M)$. Then the statement says that the identity map $\mathrm{Res}_H^G(M) \to \mathrm{Res}_H^G(M)$ is supposed to correspond to maps

$$\mathrm{Ind}_H^G \mathrm{Res}_H^G(M) \to M$$

and

$$M \to \mathrm{Ind}_H^G \mathrm{Res}_H^G(M).$$

We write down these maps explicitly. The map

$$\mathrm{Ind}_H^G \mathrm{Res}_H^G(M) \to M \tag{2.11}$$

is given by

$$\sum_{[g] \in G/H} [g] \otimes m_g \mapsto \sum_{g \in G} g.m_g,$$

where we use the description of $\mathrm{Ind}_H^G(-)$ as a tensor product over group rings spelled out in Remark 2.34. Moreover, the map

$$M \to \mathrm{Ind}_H^G \mathrm{Res}_H^G(M) \tag{2.12}$$

is given by

$$m \mapsto \sum_{[g] \in G/H} [g^{-1}] \otimes g_i.m.$$

We see that, this is independent of the set of coset representatives of H in G. In particular, for a set of cosets representatives $g_i \in G$ for $i \in I$ and $g \in G$, we can use $g_i g$ instead to see that

$$g.m \mapsto \sum_i [g_i^{-1}] \otimes (g_i g).m = [g].(\sum_{i \in I} [(g_i g)^{-1}] \otimes (g_i g).m)$$

which shows us that this map is indeed G-equivariant.

Now let N be general. Given a homomorphism $\mathrm{Res}_H^G M \to N$ of H-modules, we can apply Ind_H^G to obtain a homomorphism

$$\mathrm{Ind}_H^G \mathrm{Res}_H^G M \to \mathrm{Ind}_H^G N$$

which we can then precompose with the map (2.12) to get a map

$$M \to \mathrm{Ind}_H^G \mathrm{Res}_H^G M \to \mathrm{Ind}_H^G N,$$

as desired. In summary, we have constructed a map

$$\mathrm{Hom}_H(\mathrm{Res}_H^G M, N) \to \mathrm{Hom}_G(M, \mathrm{Ind}_H^G N).$$

We now need to see that we have an inverse map. Consider a homomorphism $M \to \mathrm{Ind}_H^G N$ and apply Res_H^G to obtain a map

$$\mathrm{Res}_H^G M \to \mathrm{Res}_H^G \mathrm{Ind}_H^G N.$$

Using Remark 2.34, we may identify $\mathrm{Res}_H^G \mathrm{Ind}_H^G N$ with functions $\phi : G \to N$, therefore we have a natural map $\mathrm{Res}_H^G \mathrm{Ind}_H^G N \to N$ taking ϕ to $\phi(e)$. In particular, postcomposing with this we obtain a map $\mathrm{Res}_H^G M \to N$, as desired. This establishes the isomorphism (2.9).

For (2.10), we proceed similarly. In particular, we consider a homomorphism $N \to \mathrm{Res}_H^G M$ of H-modules and apply Ind_H^G to it. This gives us a map

$$\mathrm{Ind}_H^G N \to \mathrm{Ind}_H^G \mathrm{Res}_H^G M,$$

which we may postcompose with the map (2.11) to get a morphism

$$\mathrm{Ind}_H^G N \to \mathrm{Ind}_H^G \mathrm{Res}_H^G M \to M.$$

Therefore, we have given a map

$$\mathrm{Hom}_H(N, \mathrm{Res}_H^G M) \to \mathrm{Hom}_G(\mathrm{Ind}_H^G N, M).$$

To exhibit an inverse, we consider a map $\mathrm{Ind}_H^G N \to M$ of G-modules and then apply Res_H^G to get a morphism $\mathrm{Res}_H^G \mathrm{Ind}_H^G N \to \mathrm{Res}_H^G M$. Now we note that we have a natural map $N \to \mathrm{Res}_H^G \mathrm{Ind}_H^G N$ given by sending $n \mapsto [e] \otimes n$, where e is the identity element. □

Remark 2.37. We note that for $M \in \mathrm{Mod}_G$ the natural maps

$$M \to \mathrm{Ind}_1^G \mathrm{Res}_1^G(M)$$

and

$$\mathrm{Ind}_1^G \mathrm{Res}_1^G(M) \to M$$

are injective and surjective, respectively. In particular, we always obtain short exact sequences.

$$0 \to M \to \mathrm{Ind}_1^G \mathrm{Res}_1^G(M) \to N \to 0$$

and

$$0 \to N' \to \mathrm{Ind}_1^G \mathrm{Res}_1^G(M) \to M \to 0$$

in Mod_G. These short exact sequences will be important for us later. In particular, the point is that the middle term will be acylic in the sense of 2.32, by Schapiro's Lemma below. In particular, Proposition 2.30, will give us natural isomorphisms

$$H^i(G, N) \xrightarrow{\simeq} H^{i+1}(G, M)$$

and

$$H^i(G, M) \xrightarrow{\simeq} H^{i+1}(G, N')$$

for any $M \in \mathrm{Mod}_G$, which will allow us to move claims on cohomology groups in higher degree to lower degree and vice-versa.

This in particular implies that Res_H^G and Ind_H^G are both left and right adjoints of one another. In other words, we have a repeating sequence of adjunctions

$$\cdots \dashv \mathrm{Ind}_H^G \dashv \mathrm{Res}_H^G \dashv \mathrm{Ind}_H^G \dashv \cdots$$

To deduce something interesting from this, we have the following basic categorical lemma which now helps us out.

Lemma 2.38. *Suppose $\mathcal{C}$ and $\mathcal{D}$ are locally small categories (in the sense that the set of maps between objects X and Y is a set) and that we have a pair of adjoint functors*

$$F \dashv G.$$

Then F commutes with colimits and G commutes with limits.

Proof. Suppose we have a colimit $\mathrm{colim}_{i\in I}\, c_i$ in C for some index set I then we want to show that the natural map

$$F(\mathrm{colim}_{i\in I}\, c_i) \to \mathrm{colim}_{i\in I}\, F(c_i)$$

induced by the universal property of the colimit is an isomorphism. The Yoneda lemma now tells us that to check this is an isomorphism, it suffices to show the induced map

$$\mathrm{Hom}(\mathrm{colim}_{i\in I}\, F(c_i)), d) \to \mathrm{Hom}(F(\mathrm{colim}_{i\in I}\, c_i), d)$$

for all $d \in \mathcal{D}$ is an isomorphism. However, now note that we can rewrite the RHS, as

$$\mathrm{Hom}(\mathrm{colim}_{i\in I}\, c_i, G(d)) \simeq \lim_{i\in I} \mathrm{Hom}(c_i, G(d)) \simeq \lim_{i\in I} \mathrm{Hom}(F(c_i), d) \simeq \mathrm{Hom}(\mathrm{colim}_{i\in I}\, F(c_i), d),$$

which implies the desired claim for F. The proof for the claim for G is completely analogous. □

In particular, given a map $f : A \to B$ in Mod_G, we note that the kernel is the limit with respect to the following diagram

$$\begin{array}{ccc} & & 0 \\ & & \downarrow \\ A & \xrightarrow{f} & B \end{array}$$

and the cokernel is the colimit with respect to the diagram

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow & & \\ 0 & & \end{array}$$

In particular, any functor that commutes with colimits will be right exact, and any functor that commutes with limits will be left exact. In particular as a consequence of Lemma 2.38, we deduce the following Corollary of Proposition 2.36.

Corollary 2.39. *For $H \subset G$ an inclusion of finite groups, the functors Ind_H^G and Res_H^G are exact.*

We also have the following basic consequence.

Corollary 2.40. *Suppose I is an injective H-module then $\mathrm{Ind}_H^G(I)$ is an injective G-module.*

Proof. This immediately follows from combining Remark 2.23 with Proposition 2.36. □

We now have the following basic result, which is known as Schapiro's lemma, and will provide us our main source of acyclic resolutions of G-modules M.

Lemma 2.41. *For a subgroup $H \subset G$, there is a canonical isomorphism for all H-modules N*

$$H^i(G, \mathrm{Ind}_H^G(N)) \xrightarrow{\simeq} H^i(H, N).$$

Proof. Choose an injective resolution

$$0 \to N \to I^0 \to I^1 \to \cdots \tag{2.13}$$

of N as a H-module. Now apply the functor Ind_H^G,

$$0 \to \mathrm{Ind}_H^G N \to \mathrm{Ind}_H^G I^0 \to \mathrm{Ind}_H^G I^1 \to \cdots,$$

which, by Corollaries 2.40 and 2.39, we note is an injective resolution of $\mathrm{Ind}_H^G N$. Hence, after taking G-invariants, the resulting complex

$$(\mathrm{Ind}_H^G I^0)^G \to (\mathrm{Ind}_H^G I^1)^G \to \cdots \tag{2.14}$$

computes $H^i(G, \mathrm{Ind}_H^G(N))$. However, now for any G-module N, we note that we have an identification $\mathrm{Ind}_H^G(N)^G \simeq N^H$. Indeed, this follows from identifying Ind_H^G with a subspace of functions $f : G \to N$, as in Remark 2.34. This tells us that (2.14) identifies with $(-)^H$ applied to (2.13), implying the desired claim after taking cohomology. □

This gives us the following example of acyclic objects.

Definition 2.42. We say an object $M \in \mathrm{Mod}_G$ is induced if it is isomorphic to $\mathrm{Ind}_e^G(N)$ for N an abelian group. Here $e \in G$ is the identity element.

Remark 2.43. Suppose we have a subgroup $H \subset G$, and we take an induced module $\mathrm{Ind}_{\{e\}}^G(N)$ for the group G. Then one can check that

$$\mathrm{Res}_H^G \mathrm{Ind}_{\{e\}}^G(N) \simeq \mathrm{Ind}_{\{e\}}^H(N^{\oplus [G:H]}).$$

Indeed, giving a function $\phi : G \to N$ is the same as giving on each one of the cosets of H in G, which is the same as giving $[G : H]$ functions on H.

Such acyclic objects come up very naturally in the study of the group cohomology of Galois groups.

Now the following is a consequence of Lemma 2.41 and the fact that $H^i(\{e\}, M) = 0$ tautologically for any $i > 0$.

Corollary 2.44. *If M is an induced G-module then we have that*

$$H^i(G, M) = 0$$

for all $i > 0$.

This finally allows us to answer the question of how to explicitly compute $H^i(G, M)$ for a G-module M. Indeed, in light of Corollary 2.44 and 2.32 (2), we see that it suffices to resolve M by induced G-modules. To this end, we consider for all $n \geq 0$ the set of functions

$$\phi : G^{n+1} \to M$$

with G-action given by

$$(g.\phi)(g_0, \ldots, g_n) = g.\phi(g^{-1}.g_0, \ldots, g^{-1}.g_n).$$

We denote the set of all such functions by $C^n(G, M)$. This is equipped with a natural differential

$$d^n : C^n(G, M) \to C^{n+1}(G, M) \tag{2.15}$$

$$d^n(\phi)(g_0, \ldots, g_{n+1}) = \sum_{i=0}^{n+1} (-1)^i \phi(g_0, \ldots, \hat{g}_j, \ldots, g_{n+1}),$$

where $\hat{g}_j$ means you omit the coordinate. We can check that this does indeed have all the properties we would like for an acyclic resolution.

Exercise 2.45. *Show that the following is true.*

1. *Show that the G-module $C^n(G, M)$ is expressible as $\mathrm{Ind}_e^G(C^n(G, M)_0)$, where $C^n(G, M)_0$ is the subset of $C^n(G, M)$ of functions for which $\phi(g_0, \ldots, g_n) = 0$ when $g_0 \neq e$. In particular, we have that $C^0(G, M) = \mathrm{Ind}_e^G(M)$ which using Frobenius reciprocity is equipped with a natural G-equivariant embedding $M \to \mathrm{Ind}_e^G(M)$.*
2. *Check that map the d^n is indeed G-equivariant for the above G-action on $C^n(G, M)$.*

(3) *Show that for all $n \geq 0$, we have that*

$$d^{n+1} \circ d^n = 0.$$

(4) *Check that we have an exact complex of G-modules*

$$0 \to M \to C^0(G, M) \xrightarrow{d^0} C^1(G, M) \xrightarrow{d^1} \cdots,$$

and deduce that we have an isomorphism

$$H^n(G, M) \simeq \mathrm{Ker}((d^n)^G)/\mathrm{Im}((d^{n-1})^G).$$

for all $n \geq 0$, where we set $(d^{-1})^G : 0 \to C^0(G, M)^G$.

(5) *Show, for all $n \geq 0$, that we have an isomorphism*

$$C^n(G, M)^G \simeq C(G^n, M),$$

where $C(G^n, M)$ denotes the space of all functions $\phi : G^n \to M$. Show that, under this isomorphism, we have an identification of

$$(d^n)^G : C(G^n, M) \to C(G^{n+1}, M)$$

with

(2.16)

$$(d^n)^G(\phi)(g_1, \ldots, g_{n+1}) = g_1.\phi(g_2, \ldots, g_n) + \sum_{i=1}^{n} (-1)^i \phi(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) + (-1)^{n+1} \phi(g_1, \ldots, g_n).$$

Remark 2.46. We call the functions $\phi(g_1, \ldots, g_n) \in C(G^n, M)$ which lie in the kernel of $(d^n)^G$ cocycles. In particular the condition that

$$g_1.\phi(g_2, \ldots, g_n) + \sum_{i=1}^{n} (-1)^i \phi(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) + (-1)^{n+1} \phi(g_1, \ldots, g_n) = 0$$

is known as the cocycle condition. Similarly, we call the functions in $\mathrm{Im}((d^{n-1})^G)$ the coboundaries. This leads to the terminology that $H^n(G, M)$ is the quotient of the cocycles by the coboundaries in $C(G^n, M)$. The space of functions $C(G^n, M)$ or equivalently $C^n(G, M)^G$ by Exercise 2.32 (5) are what are known as cochains. If we compute using $C(G^n, M)$ we will say we are using *inhomogeneous* cochains and if we compute using $C^n(G, M)^G =: C^n(G, M)_{\mathrm{hom}}$ we will say we are using *homogeneous* cochains. We see that the form of the cocycle condition and the form of the cobouandries depends on which type of cochains we are using, and, depending on the precise application, it will be more desirable to work with one or the other.

To illustrate the utility of these resolutions, we now given an explicit interpretation of $H^1(G, M)$ and $H^2(G, M)$.

Example 2.47. Using Exercise 2.32 and in particular Exercise 2.32 (4), we may identify a class in $H^1(G, M)$ with a function $\phi : G \to M$ which satisfies, for all $h \in G$, the cocycle condition

$$h.\phi(g) - \phi(hg) + \phi(h) = 0,$$

as in (2.16) or equivalently,

$$h.\phi(g) = \phi(hg) - \phi(h).$$

Moreover, it is a coboundary if an only if there exists $m \in M$ such that

$$\phi(g) = g.m - m$$

for all $m \in M$. For $m \in M$, we write ϕ_m for the function defined by this relationship. In summary, we have an isomorphism

$$H^1(G, M) \simeq \{\phi : G \to M \mid h.\phi(g) - \phi(hg) + \phi(h) = 0\}/(\phi_m \ , \ m \in M)$$

We now specialize to the case where $M = \mathbb{Z}$ is the trivial G-module. In this case, we see that $\phi_m = 0$ and we are simply looking at functions $\phi : G \to \mathbb{Z}$ such that $\phi(hg) = \phi(h) + \phi(g)$. In other words, homomorphisms, in summary we have

$$H^1(G, \mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Z}) \simeq \mathrm{Hom}(G^{\mathrm{ab}}, \mathbb{Z}).$$

This tells us that $H^1(G, \mathbb{Z})$ is dual as an abelian group to the abelianization G^{ab} of G. This is what what was alluded to in the introduction, where there we were discussing homology which is the dual to the cohomology we are discussing here.

We can similarly find an interpretation for the H^2.

Example 2.48. Suppose that M is finite. Then we claim that $H^2(G, M)$ can be interpreted as extensions

$$0 \to M \to E \to G \to 1$$

in the category of G-modules, where we note that E is it not necesarilly abelian. In particular, it is the space of such extensions up to equivalence, where we say two such extensions are equivalent if there exists a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}_M} & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}_G} & & \\ 0 & \longrightarrow & M & \longrightarrow & E' & \xrightarrow{\pi'} & G & \longrightarrow & 1. \end{array} \tag{2.17}$$

We note (e.g by the Snake Lemma (Lemma 2.21)) that this guarantees that $E \simeq E'$. However, even if we fix the isomorphism class of the central term, there may be multiple extensions. In particular, we note that there are $p - 1$ equivalent extensions of abelian groups

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0$$

given by sending $1 \mapsto ap$, where $a \in (\mathbb{Z}/p\mathbb{Z})^*$ is a unit. Indeed, if we consider $G = M = \mathbb{Z}/p\mathbb{Z}$ where the G-action is trivial then we have an isomorphism $H^2(G, M) \simeq \mathbb{Z}/p\mathbb{Z}$, where $(\mathbb{Z}/p\mathbb{Z})^* \subset \mathbb{Z}/p\mathbb{Z}$ corresponds to the extensions described above, and $0 \in \mathbb{Z}/p\mathbb{Z}$ corresponds to the split extension

$$0 \to \mathbb{Z}/p\mathbb{Z} \to (\mathbb{Z}/p\mathbb{Z})^{\oplus 2} \to \mathbb{Z}/p\mathbb{Z} \to 0.$$

To see why such extensions are parametrized by classes in $H^2(G, M)$, we choose a set-theoretic section $s : G \to E$ (e.g using Proposition 2.10). This gives rise to a function

$$\phi(g, h) = s(g)s(h)s(gh)^{-1}$$

which a priori defines a function $\phi : G^2 \to E$. However, now we note that if we apply the map $\pi : G \to E$ then this maps to 1, which implies that the function lands in $M \hookrightarrow E$. In particular, we get a well-defined function $\phi : G^2 \to E$ which will represent the class in $H^2(G, M)$. One can check that the associativity of the group law in E will guarantee that the function $\phi(g, h)$ satisfies the cocycle condition. Moreover, note that this a priori depends on the choice of section s. In particular, suppose we have two sections s and s', and let ϕ' be the analogous function as constructed above. We may then consider the function

$$b(g) := s'(g)s(g)^{-1} \in \mathrm{Ker}(\pi) = M.$$

Then one may check that

$$\phi'(g, h) = \phi(g, h) + g.b(h) - b(gh) + b(g)$$

where we note that the RHS is precisely given by applying $(d^1)^G$ to b. In particular, the class in $H^2(G, M)$ represented by $\phi(g, h)$ does not depend on s. Moreover, if we are given a section $s : G \to E$ and an equivalent extension given by a commutative diagram (2.17) that if we consider the induced section $G \xrightarrow{s} E \to E'$ the resulting function in $C(G^2, M)$ will be the same by the commutativity of the diagram. Conversely, we have the following.

Exercise 2.49. *Suppose we are given a two cocycle $\phi(g,h) : G^2 \to M$ for $M \in \mathrm{Mod}_G$ then we can produce an extension $0 \to M \to E \to G \to 0$, as follows. As a set, we define $E := M \times G$. However, we endow E with the binary operation*

$$(m,g).(m',h) := (m + g.m' + \phi(g,h), gh).$$

Check the following, by using the two cocycle condition on M. Explicitly, for $g_1, g_2, g_3 \in G$ this says that

$$g_1\phi(g_2,g_3) - \phi(g_1g_2,g_3) + \phi(g_1,g_2g_3) - \phi(g_1,g_2) = 0, \tag{2.18}$$

as in (2.16).

1. *Show that the element $(-\phi(e,e),e)$ is a two side identity element for the group operation described above.*
2. *Show that the binary operation is associative.*
3. *Check that $(-g^{-1}.m - \phi(g^{-1},g) - \phi(e,e), g^{-1})$ is a 2-sided inverse to (m,g).*

   In particular, by (1)-(3) E is a group. We note that there are natural maps

   $$E \to G$$

   $$(m,g) \mapsto g$$

   and natural maps

   $$M \to E$$

   $$m \mapsto (m - \phi(e,e), e)$$

   which will sit in a short exact sequence

   $$0 \to M \to E \to G \to 0$$

   of groups.
4. *Suppose that $\phi'(g,h) = \phi(g,h) + g.b(h) - b(gh) + b(g)$ for some function $b : G \to M$ and let E' be the group attached to ϕ' as above. Show that the map*

   $$\alpha : E \to E'$$

   defined by $(m,g) \mapsto (m - b(g), g)$ is an isomorphism and that we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}_M} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \mathrm{id}_G} & & \\ 0 & \longrightarrow & M & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1. \end{array}$$

Before returning to an abstract study of group cohomology, let's briefly reconnect this to the arithmetic of fields that we want to study.

Theorem 2.50. ***(Hilbert Theorem 90)*** *Let L/K be a Galois extension we consider the multiplicative group $L^* \in \mathrm{Mod}_{\mathrm{Gal}(L/K)}$ then we have an isomorphism*

$$H^1(\mathrm{Gal}(L/K), L^*) \simeq 0$$

Proof. We first start out with the following basic lemma.

Lemma 2.51. *Let $\sigma_1, \ldots, \sigma_n$ be distinct automorphisms of a field E. Then if $c_1, \ldots, c_n \in E$ such that*

$$c_1\sigma_1(x) + \cdots + c_n\sigma_n(x) = 0$$

for all $x \in E$ then $c_i = 0$.

Proof. Without loss of generality, we assume that all the $c_i \neq 0$. We proceed by induction. If $n = 1$ then by evaluating on $x = 1$ we deduce that $c_1 = 0$ showing the claim. Let $n > 1$. Replacing x by ax for any $a \in E$, we obtain

$$c_1\sigma_1(a)\sigma_1(x) + \cdots + c_n\sigma_n(a)\sigma_n(x) = 0$$

We may now multiply the equation $\sum_{i=1}^n c_i\sigma_i(x)$ equation by $\sigma_n(a)$ and subtract the result off from the previous equation to deduce that

$$c_1(\sigma_1(a) - \sigma_n(a))\sigma_1(x) + c_{n-1}(\sigma_{n-1}(a) - \sigma_n(a))\sigma_{n-1}(x) = 0.$$

However, since the σ_i are distinct, we may choose a such that $\sigma_1(a) - \sigma_n(a) \neq 0$. In particular, our inductive hypothesis tells us that $c_1 = 0$, and then we may apply our inductive hypothesis again, to show that the remaining $c_i = 0$. □

Now, using the interpretation of H^1 provided in Example 2.47 and switching to multiplicative notation, we deduce that we are tasked with showing that, for every function $\phi : \mathrm{Gal}(L/K) \to L^*$ satisfying the condition that

$$\phi(\sigma \circ \tau) = \phi(\sigma)\sigma(\phi(\tau)) \tag{2.19}$$

for all $\sigma, \tau \in \mathrm{Gal}(L/K)$ that there exists $\gamma \in L^*$ such that

$$\phi(\sigma) = \sigma(\gamma)\gamma^{-1}.$$

To see this, note that by Lemma 2.51,

$$\sum_{\tau \in \mathrm{Gal}(L/K)} \phi(\tau)\tau(-) : L \to L$$

is not the zero map, since $\phi(\tau) \in L^*$ is non-zero by definition. In particular, there exists some $l \in L^*$ such that

$$\gamma^{-1} := \sum_{\tau \in \mathrm{Gal}(L/K)} \phi(\tau)\tau(l) \in L^*$$

We claim that this is the sought after γ. Indeed, for all $\sigma \in \mathrm{Gal}(L/K)$, we have that

$$\sigma(\gamma)^{-1} = \sum_{\tau \in \mathrm{Gal}(L/K)} \sigma(\phi(\tau))\sigma(\tau(l))$$

which we may rewrite using (2.19) as

$$\sum_{\tau \in \mathrm{Gal}(L/K)} \phi(\sigma)^{-1}\phi(\sigma \circ \tau)\sigma(\tau(l)) = \phi(\sigma)^{-1} \sum_{\tau \in \mathrm{Gal}(L/K)} \phi(\sigma \circ \tau)\sigma(\tau(l)) = \phi(\sigma)^{-1}\gamma^{-1},$$

which gives us

$$\phi(\sigma) = \sigma(\gamma)\gamma^{-1},$$

as desired. □

In the additive case, we have a much more definitive answer.

Exercise 2.52. *Let L/K be a Galois extension. Consider the additive group $(L, +) \in \mathrm{Mod}_{\mathrm{Gal}(L/K)}$ show the following is true.*

1. *Show, using the explicit description of H^1 provided in Example 2.47, that one has $H^1(\mathrm{Gal}(L/K), L) = 0$ (Hint: Your replacement for Lemma 2.51 should be normal basis theorem which says that there exists $\alpha \in L$ such that its conjugates under $\mathrm{Gal}(L/K)$ form a basis for L as a K-vector space).*
2. *Prove that L is actually an induced $\mathrm{Gal}(L/K)$-module and conclude that*

$$H^i(\mathrm{Gal}(L/K), L) = 0$$

for all $i \geq 1$.

2.2.3. *Aside on the Brauer Group.* In light of Exercise 2.52 and Theorem 2.50, one might wonder about $H^2(\mathrm{Gal}(L/K), L^*)$? In particular, is this is always trivial? The answer is no and the structure of this cohomology group is one of the most important invariants of the extension L/K. To explain this, we consider the following a priori unrelated notion.

Definition 2.53. Let k be a field.

(1) A (not necessarily non-commutative) ring D is said to be a division algebra if every non-zero element $d \in D$ has a two sided inverse d^{-1}.
(2) We say that a division algebra D is a division algebra over k if its center is isomorphic to k. In particular, D is a module over k, and we say it is finite-dimensional over k if it is finite-dimensional as a vector space.
(3) A central simple algebra over k is a (not necessarily non-commutative) ring A with no non-trivial two sided ideals and center isomorphic to k.
(4) We note that a central simple algebra has the structure of a vector space over k, by multiplication by the center, and we say that A is a finite dimensional central simple algebra if it is finite-dimensional as a vector space over k.
(5) We note that given a finite dimensional central simple algebra A over k. We can define another finite dimensional central simple algebra A over k, denoted A^{op}, by reversing the order of the multiplication.

Observe that a division algebra D over k is a particular example of a central simple algebra over k. Indeed, any non-zero right or left ideal $I \subset D$ must contain 1 by the existence of two sided inverses inverses and therefore is equal to D. We can push this even further.

Example 2.54. Let $M_n(D)$ be the matrix algebra of a divsion algebra D over k. We claim that this is a central simple algebra over k. We need to check that it has no non-zero two sided ideals and that its center is equal to k. To see this, as in usual linear algebra we note that we have matrices $E_{ij} \in M_n(D)$ which are 1 in the ith row and jth column and 0 everywhere else. Suppose we have $X \in M_n(D)$ with entries given by (X_{ij}). Then the relationship

$$E_{ij}X = XE_{ij}$$

will tell us that $x_{ij} = 0$ unless $i = j$. In particular, X is a diagonal matrix. If X acts on the right it will scale the columns of a matrix, and if it acts on the left then it will scale the rows. This forces the relationship that all the diagonal entries of X are the same. In particular, X lies in the image of the natural map $D \to M_n(D)$ given by the diagonal embedding. However, now it clearly must lie in the image of the center of D, so that we have an isomorphism

$$Z(M_n(D)) \simeq Z(D) \tag{2.20}$$

of centers. Now by assumption that D is a division algebra over k, we have an isomorphism $Z(D) \simeq k$, by the assumption that D is a division algebra over k.

For the statement on two-sided ideals, we suppose X is a non-zero matrix in some two-sided ideal $I \subset M_n(D)$ with non-zero entry x_{pq} for some $1 \leq p, q \leq n$. Then we have that

$$E_{ip}XE_{qj} = x_{pq}E_{ij}$$

lies inside I for all $1 \leq i, j \leq n$. By acting via the diagonal matrices, this tells us that I contains $(x_{pq})E_{ij}$, where (x_{pq}) is the two sided ideal generated by x_{pq} inside D, which must be given by (1) as explained above. Since i and j were arbitrary, this tells us that $I = M_n(D)$, as desired.

In fact, this example captures all finite dimensional central simple algebras over a field k (In fact, the finite dimensionality hypothesis is also not necessary, but we do not adress this for simplicity).

Theorem 2.55. ***(Wedderburn's Theorem)*** *Let A be a finite dimensional central simple algebra over k then there exists $n \geq 1$ and a finite dimensional division algebra D over k such that*

$$M_n(D) \simeq A.$$

Proof. We may choose a non-zero minimal left ideal $I \subset A$. Then the left multiplication of A on I defines a natural non-zero map

$$A \to \mathrm{End}_k(I)$$

which will be necessarily injective. Indeed, the kernel of this map generates a two-sided ideal which must therefore be 0 or (1) by the simplicity of A. Let D be the centralizer of A in $\mathrm{End}_k(I)$. We claim that this is a division algebra. Indeed, by definition we have an identification $D = \mathrm{End}_A(I)$, and any $f : I \to I \in \mathrm{End}_A(I)$ must be injective, since otherwise its kernel would generate a non-zero minimal ideal of A properly contained in I. However, it must also be surjective by rank-nullity (note I is a finite dimensional k-vector space and f is a k-linear map). Therefore, f is invertible. In particular, this endows I with the structure of a left D-module, which must necessarily be free, since, as noted above, any non-zero ideal of D is isomorphic D, so that $I \simeq D^{\oplus n}$. Now, by Lemma 2.56 below, the centralizer of D in $\mathrm{End}_k(I)$ is isomorphic to A. In particular, this gives an identification $M_n(D^{\mathrm{op}}) \simeq \mathrm{End}_D(I) \simeq A$, as desired. By the finite-dimensionality of A, the division algebra D must be finite dimensional, and by (2.20) it must have center equal to k. □

We used the following Lemma in the proof, which is a hard exercise in linear algebra.

Lemma 2.56. *Let A be a k-algebra and V be a semisimple A-module such that the map*

$$A \to \mathrm{End}_k(V)$$

is injective. Then the double centralizer of A in $\mathrm{End}_k(V)$ is equal to A.

Proof. See [Mil20a, Theorem 1.14]. □

Indeed, this tells us that central simple algebras are a straightforward extension of division algebras given by taking matrix algebras. However, we have yet to provide any interesting examples of division algebras.

Example 2.57. (1) If $D = k$ then it is of course a division algebra over k.

(2) The first interesting example of a non-commutative division algebra is the Hamilton quaternions. In particular, we set $\mathbb{H}$ to be the $\mathbb{R}$-algebra $\mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$, where i, j, k are subject to the relationships

$$i^2 = j^2 = k^2 = -1$$
$$ij = -ji = k.$$

Given an element $q = a + ib + cj + dk$, we may define its conjugate $\overline{q} = a - bi - cj - dk$. We have an equality

$$N(q) := q\overline{q} = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}.$$

so that $\overline{q}/N(q)$ gives a well-defined inverse to q. In particular, $\mathbb{H}$ has the structure of a division algebra! Moreover, one easily checks the center is equal to $\mathbb{R}$ via the embedding $\mathbb{R} \to \mathbb{H}$ given by the first coordinate, which extends to an embedding $\mathbb{C} \to \mathbb{H}$ via the first and second coordinate. The field $\mathbb{C}$ defines a maximal commutative subfield of $\mathbb{H}$.

(3) A more interesting family of examples occurs in the case of a finite cyclic extension L/K. We write σ for the generator of the Galois group. For $a \in K^*$, we define the cyclic algebra

$$A = (L/K, \sigma, a)$$

as follows. We consider the K-algebra

$$A := \bigoplus_{i=0}^{n-1} Lu^i$$

generated by L and the symbol u subject to the relationship that

$$u^n = a,$$

and, for all $x \in L$, we have that

$$ux = \sigma(x)u.$$

We can check that this does indeed give a central simple algebra over K, and in certain good situations also division algebras.

Exercise 2.58. *Show the following claims.*

(1) ***(Basic properties)***
   (a) *Show that $A = (L/K, \sigma, a)$ is a central simple K-algebra of dimension n^2 over K.*
   (b) *Show that the natural inclusion $L \hookrightarrow A$ defines a maximal commutative subfield of A.*
   (c) *Prove that*
   $$A \otimes_K L \cong M_n(L).$$
   of central simple L-algebras. (Hint: Recall that we have an isomorphism $L \otimes_K L \simeq \prod_{\tau \in \mathrm{Gal}(L/K)} L$ for any Galois extension L/K. In the case of a cyclic extension, this takes the form of sending $x \otimes y \mapsto (\sigma^i(x)y)_{i=0}^{n-1}$ in the case of a cyclic extension. Use this map to define the isomorphism $A \otimes_K L \simeq M_n(L)$.)

(2) ***(Relationship to the Hamilton Quaternions)*** *Let $K = \mathbb{R}$ and $L = \mathbb{C}$, and let σ be complex conjugation. Consider the cyclic algebra*
   $$A = (\mathbb{C}/\mathbb{R},\ \sigma, -1)$$
   (a) *Let $u \in A$ be the adjoined generator, so that $u^2 = -1$ and $uz = \overline{z}\, u$ for $z \in \mathbb{C}$. Define elements*
   $$i := \sqrt{-1} \in \mathbb{C} \subset A, \qquad j := u, \qquad k := ij.$$
   Show that $i^2 = j^2 = k^2 = -1$ and that
   $$ij = k, \quad ji = -k,$$
   (b) *Show that every element of A can be written uniquely as*
   $$a + bi + cj + dk \qquad (a, b, c, d \in \mathbb{R}),$$
   and conclude that A is isomorphic to the classical Hamilton quaternion division algebra $\mathbb{H}$.

(3) ***(The Splitting Criterion.)*** *We will now be interested in showing the following Theorem. We let $\mathrm{Nm}_{L/K} : L^* \to K^*$ denote the norm map.*

Theorem 2.59. *The central simple algebra $A = (L/K, \sigma, a)$ is isomorphic to $M_n(K)$ if and only if $a = \mathrm{Nm}_{L/K}(b)$ for some $b \in L^*$.*

Assume that $a = \mathrm{Nm}_{L/K}(b)$, for some $b \in L^\times$.
   (a) *Set $v := b^{-1}u \in A$. Compute v^i for $i = 0, \ldots, n-1$ and show that $v^n = 1$.*
   (b) *Consider the element $e = \sum_{i=0}^{n-1} v^i \in A$. Show that Ae is a nonzero left ideal of A of K-dimension n. Deduce that $A \cong M_n(K)$, by arguing similarly to the proof of Wedderburn's theorem. Conclude the converse direction of Theorem 2.59.*

We now establish the forward direction. Suppose that $A \simeq M_n(K)$.
   (c) *Let V be a simple left A-module. Show that $\dim_K V = n$ and that, via the embedding $L \hookrightarrow A$, the space V becomes a 1-dimensional vector space over L.*
   (d) *Choose $0 \neq v \in V$. Since $u^n = a \in K \subset L$, show that*
   $$u^n v = av.$$
   (e) *Because V is 1-dimensional over L, there exists $\lambda \in L^\times$ with $uv = \lambda v$. Using the relation $ux = \sigma(x)u$, prove that*
   $$u^n v = \lambda\, \sigma(\lambda) \cdots \sigma^{n-1}(\lambda)\, v = \mathrm{Nm}_{L/K}(\lambda)\, v.$$

(f) Combine the two previous steps to deduce that $a = \mathrm{Nm}_{L/K}(\lambda)$.

(4) *Combine Theorem 2.59 with Wedderburn's theorem to conclude that* $A = (L/K, \sigma, a)$ *is a division algebra if and only if* $a \neq \mathrm{Nm}_{L/K}(b)$ *for some* $b \in L^*$.

In particular, we see that there is an interesting relationship between the structure of these division algebras and the surjectivity of the maps $\mathrm{Nm}_{L/K} : L^* \to K^*$, which is measured by the group $K^*/\mathrm{Nm}_{L/K}(K^*)$, at least in the case of a cyclic extension. Indeed, we see that if $L = \mathbb{C}$ and $K = \mathbb{R}$ then we have that $\mathbb{R}^*/\mathrm{Nm}_{L/K}(\mathbb{C}^*) = \mathbb{R}^*/\mathbb{R}_{>0} \simeq < -1 >$. Moreover, the non-trivial element -1 gives rise to a the non-trivial division algebra $\mathbb{H}$ over the field $\mathbb{R}$. As we will see later, this is because the group $K^*/\mathrm{Nm}_{L/K}(K^*)$ *classifies* such division algebras in the case of a cyclic extension. This suggested relationship will come full circle after we discuss Tate cohomology later in the course. For now, we begin by linking the classification of division algebras with the cohomology group $H^2(\mathrm{Gal}(L/K), L^*)$. To this aim, we introduce the following.

Definition 2.60. Fix a field K, we define the following.

(1) We say two finite dimensional central simple algebras A, B over K are equivalent $A \sim B$ if there exists a finite-dimensional division algebra D over K and positive integers $n, m \geq 1$ such that
$$A \simeq M_n(D)$$
and
$$B \simeq M_m(D),$$
where we note that such a D always exists by Wedderburn's Theorem (Theorem 2.55). We denote the equivalence class of such a finite dimensional central simple algebra A over k by $[A]$.

(2) We write $\mathrm{Br}(k)$ for the set of equivalence classes of finite central simple algebras over k.

(3) For a finite extension L/K, we write $\mathrm{Br}(L/K) \subset \mathrm{Br}(K)$ for the subset of $[A]$ such that $A \otimes_K L \simeq M_n(L)$ for some $n \geq 1$. This is referred to as the Brauer group of the finite extension L/K.

Remark 2.61. We note that, every finite-dimensional division algebra D over K, gives rise to a class in $\mathrm{Br}(K)$. In particular, by Wedderburn's Theorem (Theorem 2.55), if we vary over the isomorphism classes of such division algebras D over K, this gives rise to every class in $\mathrm{Br}(K)$. In particular, we see that we have bijection of sets:
$$\mathrm{Br}(K) \leftrightarrow \{D \text{ a finite-dimensional division algebra over } K\}/\simeq .$$
Similarly, for a finite extension L/K, we say that a division algebra D splits over K if there exists $n \geq 1$ and an isomorphism
$$D \otimes_K L \simeq M_n(L),$$
and we similarly have a bijection
$$\mathrm{Br}(L/K) \leftrightarrow \{D \text{ a finite-dimensional division algebra over } K \text{ split over } L\}/\simeq$$
In fact, every finite dimensional division algebra D/K can be shown to split over some finite extension L. This is given by a maximal commutative subfield $L \hookrightarrow D$ (cf. Exercise 2.58 (1b,1c)). This gives us an equality
$$\mathrm{Br}(K) := \varinjlim_{L/K} \mathrm{Br}(L/K), \tag{2.21}$$
where L/K ranges over all finite extensions of K.

The terminology "group" here is not just for show.

Exercise 2.62. *Let* K *be a field. Show that the following is true.*

(1) *If A, B are two finite dimensional central simple algebras over K. Show that $A \otimes_K B$ is again a finite dimensional central simple algebra over K.*
(2) *Check that the map*
$$\mathrm{Br}(K) \times \mathrm{Br}(K) \to \mathrm{Br}(K)$$
$$([A], [B]) \mapsto [A \otimes_K B]$$
gives rise to a well-defined binary, commutative, and associative operation on the set of equivalence classes of finite-dimensional central simple algebras over K with identity element K.
(3) *Given a finite-dimensional central simple algebra A of dimension n over K, show that*
$$A \otimes A^{\mathrm{op}} \simeq M_n(K).$$
Conclude that $\mathrm{Br}(K)$ is a commutative group. For a finite extension L/K, prove that $\mathrm{Br}(L/K) \subset \mathrm{Br}(K)$ is a subgroup.

We now want to connect the group $\mathrm{Br}(L/K)$ to the group cohomology $H^2(\mathrm{Gal}(L/K), L^*)$ for a finite Galois extension L/K. We may do this through a generalization of Example 2.57 (3).

Example 2.63. We let L/K be a finite Galois extension. We consider the L-algebra
$$\bigoplus_{\sigma \in \mathrm{Gal}(L/K)} x_\sigma L$$
with multiplication for $\alpha \in L^*$[2] defined by
$$\alpha x_\sigma = x_\sigma \sigma(\alpha) \tag{2.22}$$
and
$$x_\sigma x_\tau = \phi(\sigma, \tau) x_{\sigma\tau},$$
for some $\phi(\sigma, \tau) \in L^*$. The associativity of the multiplication forces the relationship
$$\rho(\phi(\sigma, \tau))\phi(\rho\sigma, \tau) = \phi(\rho, \sigma)\phi(\rho\sigma, \tau) \tag{2.23}$$
for all $\rho, \sigma, \tau \in \mathrm{Gal}(L/K)$, which we readily identify with the condition that $\phi : \mathrm{Gal}(L/K)^2 \to L^*$ is an inhomogeneous cocycle in the multiplicative notation, as described in the additive notation in (2.18). Given a cocycle $\phi : \mathrm{Gal}(L/K)^2 \to L^*$, we denote this central simple K-algebra by $A := (L/K, \phi)$. It is referred to as the cross-product algebra with respect to ϕ. By using the isomorphism, $L \otimes_K L \simeq \prod_{\tau \in \mathrm{Gal}(L/K)} L$ one may check that
$$A \otimes_K L \simeq M_n(L)$$
(cf. Exercise 2.58 (1c)). In particular, this gives rise to a well-defined element $[(L/K, \phi)] \in \mathrm{Br}(L/K)$! We now would like to claim that we can upgrade this to an isomorphism
$$H^2(\mathrm{Gal}(L/K), L^*) \simeq \mathrm{Br}(L/K)$$
of abelian groups. To this aim, we will first need to check that we have a well defined map
$$H^2(\mathrm{Gal}(L/K), L^*) \to \mathrm{Br}(L/K)$$
$$\phi \mapsto [(L/K), \phi)].$$
In other words, we need to check if we multiply ϕ by a coboundary
$$\frac{\sigma(b(\tau))b(\sigma)}{b(\sigma\tau)}$$
for some function $b : \mathrm{Gal}(L/K) \to L^*$ to get some new ϕ' then we have an isomorphism
$$(L/K, \phi) \simeq (L/K, \phi')$$

[2]Note that we have put the copy of L on the right this time, so we need to apply $(-)^{\mathrm{op}}$ when comparing with Example 2.57 (3)!

of central simple algebras over K. We may do this as follows. We define a natural map

$$\Phi_b : \bigoplus_\sigma x_\sigma L \to \bigoplus_\sigma x'_\sigma L$$
$$x_\sigma \mapsto b(\sigma) x_{\sigma'},$$

which, since $b(\sigma) \in L^*$ will define an isomorphism, assuming that it respects the multiplication. To see what this means, we note that

$$\Phi_b(x_\sigma x_\tau) = b(\sigma\tau)\phi(\sigma,\tau)x'_{\sigma\tau}$$

and that

$$\Phi_b(x_\sigma)\Phi_b(x_\tau) = b(\sigma)x'_\sigma b(\tau)x'_\tau$$

and by (2.22) the RHS identifies with

$$b(\sigma)\sigma(b(\tau))\phi'(\sigma,\tau)x'_{\sigma\tau}.$$

In particular, if we have that $\Phi_b(x_\sigma x_\tau) = \Phi_b(x_\sigma)\Phi_b(x_\tau)$, we recover precisely the relationship

$$\frac{\sigma(b(\tau))b(\sigma)}{b(\sigma\tau)}\phi'(\sigma,\tau) = \phi(\sigma,\tau),$$

which was precisely the condition that ϕ and ϕ' differ by a coboundary. In summary, we see that we have a well-defined map

$$H^2(\mathrm{Gal}(L/K), L^*) \to \mathrm{Br}(L/K). \tag{2.24}$$

We now come to the key claim which gives us the desired link between the Brauer group and the group cohomology $H^2(\mathrm{Gal}(L/K), L^*)$.

Theorem 2.64. *For L/K a finite Galois extension, the natural map (2.24) is an isomorphism of groups.*

Proof. (Proof Sketch) Giving a complete proof of this fact, will take us to far a field. Instead, we content ourselves with explaining how to construct an inverse map. To do this, we will invoke the following result.

Theorem 2.65. ***(Stokelm-Noether Theorem)*** *Let k be a field and let $f, g : A \to B$ be a morphism of k-algebras. Suppose that A over k[3] and that B is central simple over k. Then there exists an invertible $b \in B$ such that $f(a) = bg(a)b^{-1}$.*

Proof. See [Mil20a, Theorem 2.10]. □

We now start with a class in $\mathrm{Br}(L/K)$. By Remark 2.61, this will be represented by a finite dimensional division algebra D/K which is split over L. In particular, there will be an isomorphism

$$\psi : M_n(L) \xrightarrow{\simeq} D \otimes_K L.$$

Each $\sigma \in \mathrm{Gal}(L/K)$ will act on the RHS, this will define a natural map

$$\mathrm{Gal}(L/K) \to \mathrm{Aut}_L(M_n(L))$$
$$\sigma \mapsto \psi^{-1} \circ (\mathrm{id} \otimes \sigma) \circ \psi,$$

However, by Theorem 2.65, we have an isomorphism $\mathrm{Aut}_L(M_n(L)) \simeq \mathrm{PGL}_n(L)$. Here $\mathrm{PGL}_n(L)$ is the group defined by the short exact sequence

$$0 \to L^* \to \mathrm{GL}_n(L) \to \mathrm{PGL}_n(L) \to 0, \tag{2.25}$$

where $\mathrm{GL}_n(L)$ is the set of $n \times n$ invertible matrices and $L^* \to \mathrm{GL}_n(L)$ maps via the diagonal matrices. In particular, Theorem 2.65 tells us that we have a surjective map $\mathrm{GL}_n(L) \to \mathrm{Aut}_L(M_n(L))$

[3] I.e it is k-algebra with no non-trivial two sided ideals, but its center is not necessarily k.

given by conjugation and it is easy to check the kernel will be the diagonal matrices. We therefore have a map

$$\mathrm{Gal}(L/K) \to \mathrm{Aut}_L(M_n(L)) \simeq \mathrm{PGL}_n(L),$$

and one may verify that this defines a 1-cocycle in the group cohomology $H^1(\mathrm{Gal}(L/K), \mathrm{GL}_n(L))$[4]. Attached to the sequence (2.25), by an analogue of Proposition 2.30 one obtains a boundary map

$$\delta : H^1(\mathrm{Gal}(L/K), \mathrm{PGL}_n(L)) \to H^2(\mathrm{Gal}(L/K), L^*),$$

and the image of the 1-cocycle will be the desired inverse. □

We now have a good feeling for the structure of the cohomology groups $H^i(G, M)$, so we will return to verifying some additional functoralities of group cohomology in the finite case before proceeding to treat profinite groups.

2.2.4. *Additional Functorality.* We already saw that if we have a map $f : M \to N$ of G-modules that we obtain a well-defined functor

$$H^i(f) : H^i(G, M) \to H^i(G, N)$$

on the cohomology groups. We now want to ask about functorality with respect to a homomorphism $\alpha : G \to G'$ of groups. To this end, we have the following definition.

Definition 2.66. Let G, G' be finite groups and $M \in \mathrm{Mod}_G$ and $M' \in \mathrm{Mod}_{G'}$. Suppose that we have a homomorphism $\alpha : G' \to G$ and $\beta : M \to M'$. We say that these are compatible if

$$\beta(\alpha(g').m) = g'.\beta(m)$$

for all $g' \in G'$ and $m \in M$.

Now in this situation, we construct a natural map $H^i(G, M) \to H^i(G', M')$.

Construction 2.67. *Suppose we are in the situation of Definition 2.66 then we claim that we obtain a map*

$$H^i(G, M) \to H^i(G', M') \tag{2.26}$$

as follows. We first have a map

$$H^i(G, M) \to H^i(G', M),$$

where M is regarded as a G'-module via the map $\alpha : G' \to G$. In terms of the description of cohomology given in 2.32 (4), this may be described in terms of the restriction map

$$C(G^n, M) \to C((G')^n, M)$$

taking a function $G^n \to M$ to the function $(G')^n \xrightarrow{\alpha^n} G^n \to M$,. In particular, one checks that this commutes in the obvious sense with the differentials (2.15), giving rise to a natural map

$$H^i(G, M) \to H^i(G', M)$$

by taking cohomology. We then compose this with the natural map

$$H^i(G', M) \to H^i(G', M')$$

induced by $H^i(\beta)$ or equivalently the map induced by looking at the natural map $C(G^n, M) \to C(G^n, M')$ induced by β' and taking cohomology.

Now we study various examples of this construction, where it gives rise to various important maps.

[4]We note that we only defined group cohomology for abelian groups with an action of a (possibly non-abelian) group. However, with a bit of care one may check that the discussion extends to (possibly) non-abelian groups with an action of a (possibly) non-abelian group. For now, we ask the reader to suspend disbelief.

Example 2.68. Consider a subgroup $H \subset G$. We specialize (2.67) to the case where $M' = M$, β is the identity map, and $\alpha : H \to G$ is the inclusion of the subgroup. Then we obtain a natural map

$$\mathrm{Res}^G_H : H^i(G, M) \to H^i(H, \mathrm{Res}^G_H(M))$$

known as the restriction maps. Alternatively, we may construct this as follows. We consider the natural adjunction map

$$M \to \mathrm{Ind}^G_H \mathrm{Res}^G_H(M)$$

given by applying Proposition 2.36 to the identity map. We then obtain a map

$$H^i(G, M) \to H^i(G, \mathrm{Ind}^G_H \mathrm{Res}^G_H(M)) \simeq H^i(G, \mathrm{Res}^G_H(M)),$$

where the last isomorphism is Lemma 2.41.

We similarly obtain the following dual notion, which comes from the alternative description of the restriction map in 2.68 using Schapiro's Lemma and the adjunction morphisms of Proposition 2.36.

Example 2.69. For M a G-module, we consider the natural map

$$\mathrm{Ind}^G_H \mathrm{Res}^G_H(M) \to M$$

given by Proposition 2.36. By Lemma 2.41, this gives rise to a natural map

$$\mathrm{CoRes}^G_H : H^i(H, \mathrm{Res}^G_H(M)) \xrightarrow{\simeq} H^i(G, \mathrm{Ind}^G_H \mathrm{Res}^G_H(M)) \to H^i(G, M)$$

known as the corestriction homomorphism. This definition might appear a bit obtuse as it was constructed using Schapiro's Lemma. To further elucidate this, we first ask what is the induced map for $i = 0$. It is a map of the form

$$M^H \to M^G,$$

which may be described as follows.

Definition 2.70. For $M \in \mathrm{Mod}_G$, we define the norm map

$$\mathrm{Nm}_{G/H} : M^H \to M^G$$

$$m \mapsto \sum_{[g] \in G/H} g.m,$$

where the sum runs over a set of left coset representatives of G/H.

We may now use this map to give an alternative construction of CoRes^G_H. We do this by choosing a resolution $M \to I_*$ which is acyclic for M as both a H and a G-module (e.g if M is induced by Remark 2.43), and then looking at the induced map

$$\begin{array}{ccccc} I_0^H & \xrightarrow{(d^0)^H} & I_1^H & \xrightarrow{(d^1)^H} & \cdots \\ \downarrow{\scriptstyle \mathrm{Nm}_{G/H}} & & \downarrow{\scriptstyle \mathrm{Nm}_{G/H}} & & \\ I_0^G & \xrightarrow{(d^0)^G} & I_1^G & \xrightarrow{(d^1)^G} & \cdots \end{array}$$

and passing to cohomology. Indeed, one may see this from using that the above construction of CoRes^G_H on $i = 0$ agrees with $\mathrm{Nm}_{G/H}$ and the fact that CoRes^G_H as constructed above commutes with the natural boundary maps

$$\delta_i : H^i(G, C) \to H^{i+1}(G, A)$$

for an exact triangle of $0 \to A \to B \to C \to 0$ of G-modules. We may use this perspective to also compute in a different way. In particular, we consider the map

$$\mathrm{cor} : C^n(H, M)^H \to C^n(G, M)^G$$

defined by

$$\mathrm{cor}(\phi)(x_0,\dots,x_n) = \sum_{[g]\in G/H} g\phi(g^{-1}x_0gx_0^{-1},\dots,gx_ngx_n^{-1}). \tag{2.27}$$

and considered the induced map on cohomology, which we easily verify is well-defined. One can indeed check this also agrees with CoRes^G_H by observing that it gives the norm map in degree 0 and it respects the boundary maps δ_i in an obvious way, as before, by using the dimension shifting principle mentioned in Remark 2.37.

The corestriction and restriction homomorphism are very useful tools for gaining some basic insight into the structure of the groups $H^i(G,M)$. In particular, we have the following.

Lemma 2.71. *Suppose $H\subset G$ is a subgroup of a finite group G. Then the natural map*

$$\mathrm{CoRes}^G_H\circ\mathrm{Res}^G_H : H^i(G,M)\to H^i(G,M)$$

is given by multiplication by $[G:H]$.

Proof. We recall from the proof of Proposition 2.36 that the natural adjunction map

$$M\to \mathrm{Ind}^G_H\mathrm{Res}^G_H M$$

is given by

$$m\mapsto \sum_{[g]\in G/H}[g^{-1}]\otimes g.m,$$

where the sum is over coset representatives $[g]$ of G/H for $i\in I$. The natural adjunction map

$$\mathrm{Ind}^G_H\mathrm{Res}^G_H M\to M$$

is given by

$$\sum_{[g]\in G/H}[g]\otimes m_{[g]}\mapsto \sum_{g\in G} g.m_{[g]}.$$

In particular, we see that the composite

$$M\to \mathrm{Ind}^G_H\mathrm{Res}^G_H M\to M$$

is given by

$$m\mapsto \sum_{[g]\in G/H} m = [G:H]m.$$

Therefore, by the description of $\mathrm{Cor}\circ\mathrm{Res}$ provided in Examples 2.68 and 2.69, this identifies with the natural map on $H^i(G,M)$ induced by multiplication by $[G:H]$ on M. □

We now deduce the following nice consequence of this.

Corollary 2.72. *For G a finite group, the cohomology groups*

$$H^i(G,M)$$

are torsion of order dividing $|G|$ for $i\geq 1$.

Proof. We apply lemma 2.71 to the case where $H=\{e\}$ is the trivial group. In this case, we observe that $\mathrm{Cor}\circ\mathrm{Res}$ is given by multiplication by $|G|$ on $H^i(G,M)$. On the other hand, it factors through

$$H^i(G,M)\to H^i(G,\mathrm{Ind}^G_H\mathrm{Res}^G_H(M))\simeq H^i(\{e\},\mathrm{Res}^G_H(M))\to H^i(G,M).$$

However, $H^i(\{e\},\mathrm{Res}^G_H(M))=0$ tautologically. □

By combining this with Theorem 2.64, we have the following consequence, which is a priori not clear from the definition of the Brauer group (Definition 2.60) and its group structure (Exercise 2.62).

Corollary 2.73. *Let L/K be a finite Galois extension, and let D be a finite dimensional division algebra over K of dimension n which is split over L. Then we have an isomorphism*

$$D^{\otimes_K [L:K]} \simeq M_{n[L:K]}(K)$$

of central simple algebras over K.

Another useful consequence of this is the following acyclicity result.

Lemma 2.74. *For G a finite group and let $\mathbb{Q}$ be equipped with the trivial G-action then it is acylic in the sense of 2.32. In particular, we have that*

$$H^i(G, \mathbb{Q}) = 0$$

for all $i > 0$.

Proof. We note that multiplication by $|G|$ induces an isomorphism on $H^i(G, \mathbb{Q})$, as it induces an isomorphism on $\mathbb{Q}$. However, by Corollary 2.72, the group $H^i(G, \mathbb{Q})$ is $|G|$-torsion and therefore it must be 0. □

We now leave off with one more important example of Construction 2.67.

Example 2.75. Let $H \subset G$ be a normal subgroup of G and let $\alpha : G \to G/H$ be associated surjection. We let $\beta : M^H \hookrightarrow M$ be the injection of the H-invariants and note that G/H acts on M^H. In this case, Construction 2.67 yields a map

$$\mathrm{Inf}^G_{G/H} : H^i(G/H, M^H) \to H^i(G, M)$$

which is known as the inflation map.

These functors satisfy the following basic compatibilities with one another.

Proposition 2.76. *Let G be a finite group, let $N \subset G$ be a normal subgroup, and let $N \subset H \subset G$ be a subgroup. Then, for each $n \geq 0$, the following is true.*

(1) The diagram

$$\begin{array}{ccc} H^n(H/N, A^N) & \xrightarrow{\mathrm{CoRes}^{G/N}_{H/N}} & H^n(G/N, A^N) \\ \downarrow{\scriptstyle \mathrm{Inf}^H_{H/N}} & & \downarrow{\scriptstyle \mathrm{Inf}^G_{G/N}} \\ H^n(H, A) & \xrightarrow[\mathrm{CoRes}^G_H]{} & H^n(G, A)\,. \end{array}$$

commutes.

(2) The diagram

$$\begin{array}{ccc} H^n(H/N, A^N) & \xleftarrow[\mathrm{Res}^{G/N}_{H/N}]{} & H^n(G/N, A^N) \\ \downarrow{\scriptstyle \mathrm{Inf}^H_{H/N}} & & \downarrow{\scriptstyle \mathrm{Inf}^G_{G/N}} \\ H^n(H, A) & \xleftarrow{\mathrm{Res}^G_H} & H^n(G, A)\,. \end{array}$$

commutes.

This one may check, by using that all the functors commute with the boundary maps δ_n, as alluded to in Example 2.68, and that the diagram commutes in the case of $n = 0$.

Exercise 2.77. *Show that Proposition 2.76 is true in the case of $n = 0$.*

We are now in good shape to bootstrap to the profinite case.

2.3. **Cohomology of Profinite Groups.** In this section, we explain how the theory of group cohomology described in the finite case is bootstrapped to the profinite case. We let G be a profinite group for the rest of this subsection.

2.3.1. *Dévissage to the Finite Case.* We write $\mathrm{Mod}_{G,\mathrm{cont}}$ for the category of discrete abelian groups on which G acts continuously with its profinite topology. In particular, an object of $\mathrm{Mod}_{G,\mathrm{cont}}$ is an abelian group equipped with an action of G such that, for every $m \in M$, the set of elements in G stabilizing m is an open subgroup of $U \subset G$. In particular, we have that

$$M = \bigcup_{U \subset G} M^U, \tag{2.28}$$

where M^U denotes the subspace of elements fixed by an open subgroup $U \subset G$ and the union runs over all such open subgroups (equivalently, open normal subgroups). We want to define groups $H^n(G, M)$ which generalize the groups introduced in §2.2 and enjoy some of the same formal properties. To do this, we take the perspective of the definition of these groups provided by Exercise 2.45. In particular, we may consider

$$C_{\mathrm{cont}}(G^n, M),$$

which will be the space of continuous functions $G^n \to M$, where M has the discrete topology. In particular, this is the same as locally constant functions. We equip this with the differential

$$\partial_n : C(G^n, M) \to C(G^{n+1}, M)$$

given by the identity

$$(\partial_n)(\phi)(g_1, \dots, g_{n+1}) = g_1.\phi(g_2, \dots, g_n) + \sum_{i=1}^{n} (-1)^i \phi(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1}) + (-1)^{n+1} \phi(g_1, \dots, g_n),$$

as in (2.15). This will satisfy the identity $\partial_n \circ \partial_{n-1} = 0$ and therefore we can define

$$H^n(G, M) := \mathrm{Ker}(\partial_n)/\mathrm{Im}(\partial_{n-1}),$$

as before.

Remark 2.78. We note that it is also possible to show that the category $\mathrm{Mod}_{G,\mathrm{cont}}$ possesses enough injective objects, as shown in the finite case in Exercise 2.24. In particular, the discussion in §2.2.1 will also allow us to identify $H^n(G, M)$ as the right derived functors of invariants $(-)^G$. However, as the category $\mathrm{Mod}_{G,\mathrm{cont}}$ will not have enough projective objects unless G is finite, this will mean the discussion of homology and Tate cohomology that we will see later will not extend to this profinite case in any naive way. This is one of the reasons that cohomology is more desirable than homology when setting up the theory.

In light of Exercise 2.45, this recovers the usual definition of group cohomology if G is finite, and we may formally reduce to this case as follows.

Let $(G_i)_{i \in I}$ be a projective system of profinite groups with respected to a directed set $(I, \geq)$, and let $(M_i)_{i \in I}$ be an inductive system of discrete G_i-modules so that the transition morphisms $f_{ij} : M_j \to M_i$ and $g_{ij} : A_j \to A_i$ are compatible in the sense of Definition 2.66. By applying the analogue of Construction 2.67, this gives rise to a directed system

$$\varinjlim_{i \in I} H^n(G_i, A_i).$$

We now have the following.

Lemma 2.79. *For $(G_i)_{i \in I}$ and $(M_i)_{i \in I}$ as above, we set $G := \varprojlim_{i \in I} G_i$ and $M = \varinjlim M_i$ then we have a natural isomorphism*

$$H^n(G, M) \xrightarrow{\simeq} \varinjlim_{i \in I} H^n(G_i, M_i)$$

for all $n \geq 0$.

Proof. By taking cohomology, this follows from the fact that the natural map

$$C_{\mathrm{cont}}(G^n, M) \to \varinjlim_{i\in I} C_{\mathrm{cont}}(G_i^n, M_i)$$

is an isomorphism, since every locally constant function $f : G^n \to M$ factors through $G_i^n \to M_i$ for some $i \in I$. □

We deduce the following consequence of this. Namely, by Lemma 2.3 (2), we have a basis of open neighborhoods of the identity element given by the open normal subgroups U_i of G indexed by $i \in I$, and we see that, as in (2.28) that, for any $M \in \mathrm{Mod}_{G,\mathrm{cont}}$, we can write $M := \varinjlim_{i\in I} M^{U_i} = \bigcup_{i\in I} M^{U_i}$ and that this has a compatible action of the inverse system of finite groups $G \simeq \lim_{i\in I} G/U_i$ (cf. Example 2.75). In particular, we deduce the following from Lemma 2.79.

Corollary 2.80. *We have an isomorphism*

$$H^n(G, M) \simeq \varinjlim_{i\in I} H^n(G/U_i, M^{U_i}),$$

where $\{U_i\}$ is the inductive system of open normal subgroups of G and the transition morphisms on the RHS are given by the inflation map described in Example 2.75.

This in particular tells us that we may express the cohomology of any $M \in \mathrm{Mod}_{G,\mathrm{cont}}$ as an inductive limit of cohomology of finite groups on abelian groups. In particular, we deduce the following finiteness result even in this profinite case, by combining Corollary 2.80 with Corollary 2.72.

Corollary 2.81. *For all $n \geq 1$, the cohomology groups*

$$H^n(G, M)$$

are torsion of order dividing $|G|$, where we recall that this is a supernatural number, as in Definition 2.12.

We also have the standard interpretations of these groups.

Example 2.82. As one can see directly from the definition (cf. Example 2.47), we have the following for $M \in \mathrm{Mod}_{G,\mathrm{cont}}$.

(1) $H^0(G, M) \simeq M^G$ is the set of G-invariants
(2) We have an identification

$$H^1(G, M) := \{\phi : G \to M \in C_{\mathrm{cont}}(G, M) \mid h.\phi(g) - \phi(hg) + \phi(h) = 0\}/(\phi_m \ , \ m \in M)$$

where $\phi_m(g) := g.m - m$.
(3) If M is finite then, by arguing as in Example 2.48, we may interpret this as the space of extensions

$$0 \to M \to E \to G \to 0,$$

where E is a G-module with a continuous E-action up to equivalence as defined in (2.17). Here we note that E has naturally the structure of a profinite group by the finiteness of M. Indeed, the exact same argument will work. However, we need to ensure the that the set-theoretic section $s : G \to E$ used there is continuous, but this was already explained in this profinite context in Proposition 2.10.
(4) If K is a perfect field with algebraic closure $\overline{K}$ then we have the absolute Galois group $\mathrm{Gal}(\overline{K}/K) := \varprojlim_{L/K} \mathrm{Gal}(L/K)$ as in (1.2) where L/K runs over finite Galois extensions

with its natural structure as a profinite gorup. The group $\overline{K}^*$ of units defines an object in $\mathrm{Mod}_{\mathrm{Gal}(\overline{K}/K),\mathrm{cont}}$, and we have an identification

$$H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^*) \simeq \varinjlim_{L/K} H^2(\mathrm{Gal}(L/K), L^*) \simeq \varinjlim_{L/K} \mathrm{Br}(L/K) \simeq \mathrm{Br}(K), \tag{2.29}$$

where the inverse limit is over finite Galois extensions L/K. Here the first isomorphism follows from Corollary 2.80, the second isomorphism is Theorem 2.64, and the last isomorphism follows from (2.21).

We now bootstrap some of the discussion of functorality and Schapiro's Lemma to the profinite case.

2.3.2. *Extended Functoriality in the Profinite Case.* We now bootstrap the examples of functoriality described in §2.2.4.

In particular, we may consider two profinite groups G' and G with $M' \in \mathrm{Mod}_{G',\mathrm{cont}}$ and $M \in \mathrm{Mod}_{G,\mathrm{cont}}$. We consider a continuous homomorphism $\alpha : G' \to G$ and a map $\beta : M \to M'$, which are compatible in the sense of Definition 2.66. Just as in Construction 2.67, we obtain a natural map

$$H^i(G, M) \to H^i(G', M')$$

by using the explicit complex computing these objects in terms of $C_{\mathrm{cont}}(G^n, M)$ and the natural maps $C_{\mathrm{cont}}(G^n, M) \to C_{\mathrm{cont}}((G')^n, M)$.

Example 2.83. Suppose that $H \subset G$ is an *closed* subgroup then the inclusion map $H \subset G$ is continuous. Therefore, we get a natural restriction map

$$\mathrm{Res}^G_H : H^i(G, M) \to H^i(H, M)$$

extending Example 2.68.

We now turn to the corestriction map.

Example 2.84. Note that the construction in Example 2.69 involved Schapiro's Lemma, which we don't necessarily have. However, we also saw that we could also give a definition using Norm maps (Definition 2.70), which would make sense assuming that the subgroup $H \subset G$ has finite index. Indeed, we can construct the corestriction map assuming that $H \subset G$ is an *open* subgroup of G. Instead of using the norm map, we will construct it from the finite case by using some categorical maneuvers.

In particular, we consider a family of open normal subgroups $\{U_i\}_{i\in I}$ of G forming a basis of open neighborhoods of the identity element. We may consider the G/U_i-module M^{U_i} and the presentation

$$\varinjlim_{i\in I} H^n(G/U_i, M^{U_i}) \simeq H^n(G, M)$$

guaranteed by Corollary 2.80, where the transition morphisms are given by the inflation maps. Similarly, we have a presentation

$$\varinjlim_{i\in I} H^n(H/U_i \cap H, M^{U_i\cap H}) \simeq H^n(H, M),$$

where we note that $U_i \cap H$ is open and normal in H. By applying Example 2.69, we obtain a natural map

$$\mathrm{CoRes}_i : H^i(G/U_i, M^{U_i}) \to H^n(H/U_i \cap H, M^{U_i\cap H}).$$

By Proposition 2.76 (1), these give rise to an induced map on the colimit

$$\mathrm{CoRes}^G_H : H^n(G, M) \to H^n(H, M),$$

which is precisely the desired corestriction map.

In a similar fashion, by using Proposition 2.76 (2), when $H \subset G$ is open, we may construct Res^G_H as the colimit of the restriction maps for finite index subgroups. When $H \subset G$ is closed, we may write $H = \cap_{i \in I} U_i$ for some open normal subgroups

$$\mathrm{Res}^G_{U_i} : H^n(G, M) \to H^n(U_i, M)$$

and then consider the induced map

$$H^n(G, M) \to \varinjlim_{i \in I} H^n(U_i, M),$$

where the transition morphisms on the RHS are defined restriction. By Lemma 2.79, this gives a map

$$H^n(G, M) \to H^n(H, M),$$

which is precisely the restriction map.

In particular, this allows us to deduce the following formally from Lemma 2.71.

Lemma 2.85. *For $H \subset G$ an open subgroup of finite index, we have that*

$$\mathrm{CoRes} \circ \mathrm{Res} = [G : H].$$

In general, we can use this to get something non-trivial in the pro-p case.

Lemma 2.86. *Suppose that $H \subset G$ is a closed subgroup such that the supernatural number $[G : H]$ is prime to p (e.g if H is the p-Sylow subgroup constructed in Proposition 2.13), as defined in 2.7 (4), then, for $M \in \mathrm{Mod}_{G,\mathrm{cont}}$ the natural map*

$$\mathrm{Res}^G_H : H^n(G, M) \to H^n(H, M)$$

is injective on the p-primary component (as defined in Exercise 2.7 (4)) of $H^n(G, M)$.

Proof. If $[G : H]$ is finite then this is an immediate consequence of Lemma 2.71. In general, we may write H as an intersection of open subgroups containing H and then use Lemma 2.79 to reduce the case of finite index as explained above. □

We can now have some fun with this in the profinite case.

Exercise 2.87. *[Ser94, Section 2.4] Let $f : G \to G'$ be any continuous morphism of profinite groups and p be a prime number.*

(1) Show the equivalence of the following two properties.
- *The index of $f(G)$ in G' is prime to p*
- *For any G'-module M equal to its p-primary part, the homomorphism*

$$H^1(G', M) \to H^1(G, M)$$

is injective.

(2) Show the equivalence of the following properties.
- *f is surjective.*
- *For any G'-module M, the homomorphism*

$$H^1(G', M) \to H^1(G, M)$$

is injective.
- *For any finite G'-module M, the homomorphism*

$$H^1(G', M) \to H^1(G, M)$$

is injective.

We leave off with a discussion of Schapiro's Lemma and induced modules in this case.

2.3.3. *Schapiro's Lemma and (co-)Induced Modules.* We saw in Remark 2.34 that there were two independent interpretations of the functors $\mathrm{Ind}_H^G(M)$ in the finite case. One was in terms of functions $f : G \to M$ and the other one was in terms of a tensor product over the group $M \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G]$. In the profinite case, these two interpretations are different from one another and only one will give rise to the correct form of Schapiro's Lemma.

Definition 2.88. Let $H \subset G$ be a closed subgroup. For $N \in \mathrm{Mod}_{G,\mathrm{cont}}$, we define the co-induced module $\mathrm{coInd}_H^G(N)$ to be the space of continuous functions

$$f : G \to N,$$

where G has the profinite topology and M has the discrete topology such that $f(hg) = h.f(g)$.

This map will satisfy the property

$$\mathrm{Hom}_G(M, \mathrm{coInd}_H^G(N)) \simeq \mathrm{Hom}_H(\mathrm{Res}_H^G(M), N), \tag{2.30}$$

for $M \in \mathrm{Mod}_{G,\mathrm{cont}}$ and $N \in \mathrm{Mod}_{H,\mathrm{cont}}$, by analogous argument the proof of Proposition 2.36 and the other induction operation Ind_H^G (which we don't define for simplicity) will satisfy the other adjunction relationship

$$\mathrm{Hom}_G(\mathrm{Ind}_H^G(N), M) \simeq \mathrm{Hom}_H(N, \mathrm{Res}_H^G(M)) \tag{2.31}$$

of Proposition 2.36. If $H \subset G$ has finite index (e.g in the finite case of 2.36) then they agree by an analogous argument to Remark 2.34, and we recover a generalization of Proposition 2.36. However, only one of these functors will have the desired categorical properties required for Schapiro's Lemma.

Lemma 2.89. *The functor* coInd_H^G *preserves injective objects in* $\mathrm{Mod}_{G,\mathrm{cont}}$ *and is exact.*

Proof. (Sketch) We note that the preservation of injective objects follows from (2.30) and the left exactness of the functor follows from Lemma 2.38 and the proceeding discussion. However, we note that the functor Res_H^G is actually exact and will preserve some generators of categories of $\mathrm{Mod}_G^{\mathrm{cont}}$ (namely, the induced modules (cf. Remark 2.43)), which one can use to reverse the logic. □

In particular, now by the same argument as in 2.41, we deduce Schapiro's Lemma in the profinite case, where we recall we can argue using injective resolutions in the profinite case using Remark 2.78.

Lemma 2.90. *Let $H \subset G$ be an inclusion of a closed subgroup. Then, for all $M \in \mathrm{Mod}_{H,\mathrm{cont}}$ and $n \geq 0$, we have a natural isomorphism*

$$H^n(G, \mathrm{coInd}_H^G(N)) \simeq H^n(H, N)$$

of abelian groups.

In particular, we may apply this in the case that $H = \{e\}$ which gives us a notion of (co-)induced modules in the profinite case with the same formal properties as the finite case. We now turn our attention to the dual notion of cohomology, which will see the abelianization of profinite groups G^{ab} that we want to see.

2.4. **Tate Cohomology.**

2.4.1. *Homology of Finite Groups.* We let G be a finite group and write Mod_G for the category of left G-modules. As described in §2.2, the cohomology of finite groups arised as certain functors measuring the failure of the functor

$$(-)^G : \mathrm{Mod}_G \to \mathrm{Ab}$$

of invariants to be right exact. These were the higher derived functors of invariants. In this section, we want to study the dual notion. Namely, we want to study the failure of the following functor to be left exact and define certain left derived functors measuring this.

Definition 2.91. For $M \in \mathrm{Mod}_G$, we define M_G the coinvariants of G to be the quotient of M by the abelian group generated by $g.m - m$ for $g \in G$. Alternatively, we may think of this in terms of the augmentation ideal of the group ring introduced in Remark 2.19 this is the subset

$$I_G := \{\sum_{g\in G} a_g g \in \mathbb{Z}[G] | \sum_{g\in G} = m_g = 0\}$$

and it is preserved under the action of G-by left translation. In other words, it is the kernel of the natural map

$$\begin{aligned} \varepsilon : \mathbb{Z}[G] &\to \mathbb{Z} \\ \sum_{g\in G} a_g g &\mapsto \sum_{g\in G} a_g \end{aligned}$$

which is the augmentation map already described in 2.20. We then have a natural isomorphism

$$M_G \simeq \mathbb{Z} \otimes_{\mathbb{Z}[G]} M, \tag{2.32}$$

where the tensor product is formed using this map (See Exercise 2.101 (2)). In particular, this presentation makes it clear that this defines a functor

$$(-)_G : \mathrm{Mod}_G \to \mathrm{Ab}$$

which is the functor of G-coinvariants.

The tensor product is a left adjoint functor and therefore it commutes with colimits and is right exact, by Lemma 2.38 and the discussion proceeding it. Similarly, the functor of invariants may be interpreted as $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -)$, which is a right adjoint functor and therefore commutes with limits and is left exact. In particular, one easily checks that given a short exact sequence

$$0 \to A \to B \to C \to 0$$

the induced sequence

$$A_G \to B_G \to C_G \to 0$$

is right exact, but is not always left exact. As before, we want to complete this to a long exact sequence. As one might expect, this can be accomplished by the dual notion to the injective resolutions described in Definition 2.25. In particular, we have the following.

Definition 2.92. A G-module $P \in \mathrm{Mod}_G$ is said to be projective if, for any diagram

$$\begin{array}{ccc} & & P \\ & & \downarrow p \\ A & \xrightarrow{f} & B \end{array}$$

in Mod_G, for f is surjectiv, there exists a lift $p' : P \to A$ such that the diagram commutes.

Remark 2.93. If we compare this with the definition of injective (Definition 2.22) we see that what we essentially did was just reverse the direction of the arrows and replace injection with surjection. In the sense, we can think of projective and injective as dual notions to one another, as duality normally reverses the direction of the arrows.

We have the following basic example of a projective $\mathbb{Z}[G]$-module.

Example 2.94. Suppose we have an $B \in \mathrm{Mod}_G$ and a map $p : \mathbb{Z}[G] \to B$. Since p is a map of G-modules, it is completely determined by where it sends 1. Indeed, if $p(1) = b \in B$ then we must have that $p(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g g.b \in B$. In particular, if we now have a surjection, $f : A \to B$ then we may choose a lift of $p(1) \in B$ to some $a \in A$. We may then define a map $p' : \mathbb{Z}[G] \to A$ by sending $p'(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g g.a$. In this way, we see that $\mathbb{Z}[G]$ is a projective G-module. Similarly, any (possibly infinite) direct sum $\bigoplus_{i\in I} \mathbb{Z}[G]$ of projective G-modules will also be projective.

In particular, we see that it is fairly easy to find examples of projective G-modules by taking direct sums of $\mathbb{Z}[G]$. Moreover, if we are given any G-module M then may fix a set of generators $m_i \in M$ for some index set $i \in I$ such that taking-translates under G and linear combinations of the m_i generates all of M. We may then define a surjection

$$\bigoplus_{i \in I} \mathbb{Z}[G] \to M$$

characterized by the property that 1 in the ith coordinate of the above direct sum maps to the generator m_i, as in Example 2.94. In particular, this shows the following analogue of Exercise 2.24.

Proposition 2.95. *The category* Mod_G *has enough projective objects. In particular, for any* $M \in \mathrm{Mod}_G$*, there exists a surjection* $P \to M$ *from a projective object* P*.*

As in §2.2, we may now define the following.

Definition 2.96. For $M \in \mathrm{Mod}_G$, a projective resolution of M is a long exact sequence

$$\cdots \to P_{i+1} \xrightarrow{d_i} P_i \to \cdots \to P_2 \xrightarrow{d_1} P_1 \xrightarrow{d_0} P_0 \to M \to 0,$$

where P_i for $i \geq 0$ is projective. We will denote such a resolution by $P_* \to M$, and denote the map $P_0 \to M$ by d_{-1}.

As before, Proposition 2.95 tells us that such a resolution always exists, and in turn we may define the following.

Definition 2.97. For $M \in \mathrm{Mod}_G$, we fix a projective resolution $P_* \to M$. We then apply the functor of G-coinvariants

$$\cdots \to (P_2)_G \xrightarrow{(d_2)_G} (P_1)_G \xrightarrow{(d_1)_G} (P_0)_G$$

and then define

$$H_i(G, M) := \mathrm{Ker}((d_{i-1})_G)/\mathrm{Im}((d_i)_G) \in \mathrm{Ab}.$$

We refer to this as the group homology of M.

By essentially the same arguments as in §2.2, we obtain the following.

Proposition 2.98. *The following is true.*

1. *The group homology groups do not depend on the choice of projective resolution.*
2. *Given a map* $f : A \to B$*, there is a natural induced map*
$$H_i(f) : H_i(G, A) \to H_i(G, B)$$
for all $i \geq 0$*.*
3. *For* $M \in \mathrm{Mod}_G$*, we have an isomorphism*
$$H_0(G, M) \simeq M_G.$$
4. *For a short exact sequence*
$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0,$$
there exists natural boundary maps $\delta_i : H_i(G, C) \to H_{i-1}(G, A)$ *for all* $i \geq 1$ *which sit in a long exact sequence*
$$\cdots \to H_i(G, C) \xrightarrow{\delta_i} H_{i-1}(G, A) \xrightarrow{H_{i-1}(f)} H_{i-1}(G, B) \xrightarrow{H_{i-1}(g)} H_{i-1}(G, C) \xrightarrow{\delta_{i-1}}$$
extending the right exact sequence
$$A_G \to B_G \to C_G \to 0$$
in light of (3).

(5) For an inclusion of subgroups $H \subset G$ and $N \in \mathrm{Mod}_H$, we have an isomorphism

$$H_i(H, N) \simeq H_i(G, \mathrm{Ind}_H^G(N)).$$

Similarly, we may define the following.

Definition 2.99. We say that $M \in \mathrm{Mod}_G$ is homologically acyclic if, for all $i \geq 1$, we have that

$$H_i(G, M) = 0.$$

Remark 2.100. As before, we may easily check that the analogue of Exercise 2.32 holds. In particular, projective modules are acyclic, and to compute group homology it suffices to find a resolution by homologically acyclic modules.

We would also like some concrete understanding of the higher homology groups, as was done for cohomology in Example 2.47. To this end, we have the following.

Exercise 2.101. *Consider the short exact sequence in* Mod_G

$$0 \to I_G \to \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0 \tag{2.33}$$

defined by the augmentation map, as in Definition 2.91. Here $\mathbb{Z}$ has the trivial action. Show the following.

(1) By considering the long exact cohomology sequence of homology groups attached to (2.33) show that we have an isomorphism

$$H_1(G, \mathbb{Z}) \simeq I_G/I_G^2,$$

where I_G^2 is the ideal generated by products of elements in I_G with elements in I_G.

(2) Show that I_G is generated as an ideal by the elements $(g-1)$.

(3) Consider the map

$$\phi : G \to I_G/I_G^2$$

sending $\phi(g)$ to $g-1$ mod I_G^2. Show that this is a well-defined homomorphism where I_G/I_G^2 is equipped with its additive group structure.

(4) Show that ϕ factors through $G^{\mathrm{ab}} := G/[G, G]$, where $[G, G]$ is the subgroup of commutators and that the resulting map

$$\phi^{\mathrm{ab}} : G^{\mathrm{ab}} \to I_G/I_G^2$$

is an isomorphism. Conclude that $H_1(G, \mathbb{Z}) \simeq G^{\mathrm{ab}}$ as abelain groups.

In particular, we see that indeed the 1st homology is computing the abelianization of the group G, as was alluded to in the introduction. We now turn to our next topic which will splice together this notion of homology and cohomology.

2.4.2. *Tate Cohomology of Finite Groups.* For a short exact sequence

$$0 \to A \to B \to C \to 0$$

in Mod_G. We have now seen two different long exact sequences we can attach to it. First is the cohomology long exact sequence which has the form

$$0 \to A^G \to B^G \to C^G \to H^1(G, A) \to \cdots,$$

and the second is the homology long exact sequence, which has the form

$$\to H_1(G, A) \to C_G \to B_G \to A_G \to 0.$$

Tate cohomology allows us to splice these two long exact sequences together into an infinite sequence in both directions. The key here is that for $M \in \mathrm{Mod}_G$, we have the norm map

$$\mathrm{Nm}_G : M \to M^G$$

$$m \mapsto \sum_{g \in G} g.m$$

as introduced in Definition 2.70. We note that this will send all the elements $h.m - m$ to 0 for $h \in G$. Indeed, $h.\sum_{g\in G} g.m = \sum_{g\in G} h.gm = \sum_{g\in G} g.m$, as left multiplication permutes the elements of the group. Therefore, this induces a map

$$\overline{\mathrm{Nm}}_G : M_G \to M^G$$

between the coinvariants and the invariants. This leads to the following definition.

Definition 2.102. For all $i \in \mathbb{Z}$, and $M \in \mathrm{Mod}_G$, we define the Tate cohomology $H^i_T(G, M)$ as follows

$$H^i_T(G, M) := H^i(G, M)$$

if $i \geq 1$

$$H^i_T(G, M) := H_{-i-1}(G, M)$$

if $i < -1$, and

$$H^0_T(G, M) := M^G / \mathrm{Nm}_G(M)$$

and

$$H^{-1}_T(G, M) := \mathrm{Ker}(\mathrm{Nm}_G)/I_G.M \simeq \mathrm{Ker}(\overline{\mathrm{Nm}}_G).$$

We record some additional properties of this which follow from our discussion of cohomology and homology together with a direct calculation for the $i = -1, 0$ Tate cohomology groups.

Proposition 2.103. *The following is true.*

(1) For an inclusion of finite groups $H \subset G$ and $N \in \mathrm{Mod}_H$, we have a natural isomorphism

$$H^i_T(G, \mathrm{Ind}^G_H(N)) \simeq H^i_T(H, N)$$

for all $i \in \mathbb{Z}$.

(2) For any map $f : A \to B$ in Mod_G, we have, for all $i \in \mathbb{Z}$, a natural induced map

$$H^i_T(f) : H^i_T(G, A) \to H^i_T(G, B)$$

extending the usual maps on cohomology and homology.

We also have the following most important property.

Exercise 2.104. *Suppose we have a short exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$. Show the following.*

(1) Check that we have a commutative diagram of the form

(2.34)

$$\begin{array}{ccccccccccc}
 & & & & H^{-1}_T(G,A) & \longrightarrow & H^{-1}_T(G,B) & \longrightarrow & H^{-1}_T(G,C) & & \\
 & & & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & H_{-1}(G,C) & \longrightarrow & A_G & \longrightarrow & B_G & \longrightarrow & C_G & \longrightarrow & 0 \\
 & & & & \downarrow{\scriptstyle \overline{\mathrm{Nm}}_G} & & \downarrow{\scriptstyle \overline{\mathrm{Nm}}_G} & & \downarrow{\scriptstyle \overline{\mathrm{Nm}}_G} & & \\
 & & 0 & \longrightarrow & A^G & \longrightarrow & B^G & \longrightarrow & C^G & \longrightarrow & H^1(G,A) \longrightarrow \cdots \\
 & & & & \downarrow & & \downarrow & & \downarrow & & \\
 & & & & H^0_T(G,A) & \longrightarrow & H^0_T(G,B) & \longrightarrow & H^0_T(G,C) & &
\end{array},$$

where the second and third row are given by the long exact sequence for homology and cohomology, respectively, and the remaining arrows are the obvious ones.

(2) *Check that by applying the snake lemma (Lemma 2.21) to the middle part of (2.34) that we obtain a long exact sequence*

$$\cdots \to H_T^{i-1}(G,C) \to H_T^i(G,A) \xrightarrow{H_T^i(f)} H_T^i(G,B) \xrightarrow{H_T^i(g)} H_T^i(G,C) \to H_T^{i+1}(G,A) \to \cdots \tag{2.35}$$

for all $i \in \mathbb{Z}$.

In particular, Tate cohomology successfully "stiches together" the cohomology and the homology of a finite group G in a way that is compatible with the long exact sequences. As we will see, this provides a powerful tool that allows us to connect invariants such as the Brauer group of a field together with the abelianization of its Galois group and the multiplicative structure of the field, which will ultimately be the mechanism by which we prove the main results of local and global class field theory.

Before moving on to more interesting applications, we first discuss some examples of extended functorality in the context of homology and Tate-cohomology. Let $\alpha : G' \to G$ be a homomorphism of finite groups and $M \in \mathrm{Mod}_G$ and $M' \in \mathrm{Mod}_{G'}$. We suppose we have a homomorphism $\beta : M \to M'$ which is α-compatible in the sense of Definition 2.66. We would like to say that this induces a map

$$H_i(G,M) \to H_i(G',M'),$$

as in Construction 2.67 for all $i \geq 0$. However, we note that Definition 2.66 is not enough to guarantee that β gives rise to a well-defined map $M_G \to M'_{G'}$ on coinvariants. Moreover, for Tate-cohomology, we would like to say that this induces a map

$$H_T^i(G,M) \to H_T^i(G',M')$$

for all $i \in \mathbb{Z}$. However, we also do not know that $M \to M'$ gives rise to a well defined map on $\mathrm{Nm}_G(M) \to \mathrm{Nm}_{G'}(M')$. In particular, we need to know that there exists (a necessarily unique) map $\beta_G : M_G \to M_{G'}$ in Ab such that the diagram

$$\begin{array}{ccc} M & \xrightarrow{\beta} & M' \\ \downarrow{\scriptstyle (-)_G} & & \downarrow{\scriptstyle (-)_{G'}} \\ M_G & \xrightarrow{\beta_G} & M'_{G'} \end{array} \tag{2.36}$$

commutes to get a map on homology and similarly for projective resolutions of G. Similarly, for Tate cohomology, we need to know that there exists a map $\overline{\beta} : \mathrm{Nm}_G(M) \to \mathrm{Nm}_{G'}(M')$ such that

$$\begin{array}{ccc} \mathrm{Nm}_G(M) & \xrightarrow{\overline{\beta}} & \mathrm{Nm}_{G'}(M') \\ \downarrow & & \downarrow \\ M & \xrightarrow{\beta} & M'. \end{array} \tag{2.37}$$

commutes. This can be arranged in the following special cases.

Example 2.105. (1) We see that we can always construct such a map α_G filling (2.36) if β is surjective. Indeed, this follows from the fact that vertical arrows of (2.36) are surjective. Similarly, we may do this on projective resolutions. Therefore for (α, β) a compatible pair as in Definition 2.66, such that β is surjective we get a well-defined map

$$H_i(G,M) \to H_i(G',M')$$

on homology in this case.

(2) We see that we can always construct such a map filling in the diagram (2.37) if β is injective. Therefore, for (α, β) a compatible pair, we get a well-defined map

$$H_T^i(G,M) \to H_T^i(G',M')$$

in this case for $i \geq -1$.

(3) We see by (1) and (2) that if (α, β) are a compatible pair such that β is an isomorphism, we get a well-defined map
$$H_T^i(G, M) \to H_T^i(G', M')$$
for all $i \in \mathbb{Z}$.

(4) We note that the situation of (3) is satisfied for the compatible pair (α, β) used in defining the restriction map for an inclusion of subgroups $H \subset G$, as in Example 2.68. In particular, we get a well-defined map
$$\mathrm{Res}_H^G : H_T^i(G, M) \to H_T^i(H, \mathrm{Res}_H^G(M)), \tag{2.38}$$
for all $i \in \mathbb{Z}$.

(5) Since we know Schapiro's lemma for Tate-cohomology by Proposition 2.103 (2), we may apply the same logic as in Example 2.69, to deduce the existence of a map
$$\mathrm{CoRes}_H^G : H_T^i(H, \mathrm{Res}_H^G(M)) \to H_T^i(G, M) \tag{2.39}$$
for all $i \in \mathbb{Z}$, which will satisfy
$$\mathrm{CoRes}_H^G \circ \mathrm{Res}_H^G = [G : H]$$
as in Lemma 2.71. Similarly, as in Corollary 2.72, we may deduce that $H_T^i(G, M)$ is always $|G|$-torsion.

(6) If we consider the restriction map (2.38) for $i = -2$ and $M = \mathbb{Z}$ with the trivial G-action for $H \subset G$ an inclusion of subgroups then, by Exercise 2.101, we see that we obtain a map
$$G^{\mathrm{ab}} \simeq H_T^{-2}(G, \mathbb{Z}) \to H^{\mathrm{ab}} \simeq H_T^{-2}(H, \mathbb{Z})$$
from the abelianization of G to the abelinization of H. This is know as the Verlagerung (or transfer) morphism. We can describe this explicitly as follows. We write
$$G = Hg_1 \cup Hg_2 \cup \cdots \cup Hg_n.$$
for a set of coset representatives of $H \subset G$. We then consider the map sending $g \in G$ to g_i if $g \in Hg_i$. We then define
$$V : G \to H^{\mathrm{ab}}$$
by
$$V(g) := \prod_{i=1}^{n} g_i g \phi(g_i g)^{-1} \bmod [H, H]$$
where $[H, H] \subset H$ is the subgroup of commutators. One check that this gives rise to a well-defined homomorphism, and therefore induces a map
$$G^{\mathrm{ab}} \to H^{\mathrm{ab}},$$
which is precisely the map described above.

We now analyze these Tate cohomology groups in the case of a cyclic group.

2.5. **Tate Cohomology of a Cyclic Group.** One of the most beautiful things about Tate cohomology is that it exhibits a remarkably simple structure when specialized to the case of a cyclic group.

Theorem 2.106. ***(Tate's Periodicity Theorem)*** *Let G be a finite cyclic group and $M \in \mathrm{Mod}_G$. Then, for all $i \in \mathbb{Z}$, there is a natural in M isomorphism*
$$H_T^i(G, M) \xrightarrow{\simeq} H_T^{i+2}(G, M)$$
determined by a generator of G.

Proof. We let m denote the order of G and choose a generator $\langle\sigma\rangle$ of G. We note that we have an identification

$$\mathbb{Z}[G] \simeq \mathbb{Z}[x]/(x^m - 1)$$

by sending σ to x. In particular, $\mathbb{Z}[G]$ is a commutative ring in this case. We can consider the multiplication by $(x-1)$ map on $\mathbb{Z}[G]$. We recall the interpretation of induction as tensoring over the group ring 2.34. This tells us that the multiplication by $x-1$ map gives rise to a map

$$\times(x-1) : \mathrm{Ind}_1^G \mathrm{Res}_1^G M \simeq M \otimes_{\mathbb{Z}} \mathbb{Z}[G] \to M \otimes_{\mathbb{Z}} \mathbb{Z}[G] \simeq \mathrm{Ind}_1^G \mathrm{Res}_1^G M.$$

In light of the factorization $x^m - 1 = (x-1)(x^{m-1} + \cdots + x + 1)$, the kernel of the multiplicaiton by $x-1$ map on $\mathbb{Z}[G]$ is the image of multiplication of $x^{m-1} + \cdots + 1$, while the image is the ideal generated by $x-1$. This tells us that we get an exact sequence

$$0 \to M \to \mathrm{Ind}_1^G \mathrm{Res}_1^G M \xrightarrow{\times(x-1)} \mathrm{Ind}_1^G \mathrm{Res}_1^G M \to M \to 0 \tag{2.40}$$

where the outer arrows are given by adjunction maps coming from 2.36. Indeed, if we examine the construction of these maps provided in the proof of 2.36 we see that the first map is given by $m \mapsto \sum_{i=0}^{n-1} \sigma^i \otimes m$ and the last map is given by $\sum_{i=0}^{n-1} \sigma^i \otimes m_i \mapsto \sigma^i(m_i)$. We now can apply the following Lemma to (2.40) in light of Schapiro's Lemma for Tate cohomology (Proposition 2.103 (1)), which will give us the desired result.

Lemma 2.107. *For G a finite group, suppose we have an exact sequence*

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \to 0$$

and B and C have vanishing Tate-cohomology for all $i \in \mathbb{Z}$. Then we have a natural isomorphsim

$$H_T^{i+2}(G, A) \simeq H_T^i(G, D)$$

for all $i \in \mathbb{Z}$.

Proof. We consider the long exact cohomology sequence of (2.104) coming from the short exact sequence

$$0 \to A \to B \to B/\mathrm{Im}(f) \to 0$$

then we deduce that we have an isomorphism

$$H_T^{i+2}(G, A) \simeq H_T^{i+1}(G, B/\mathrm{Im}(f))$$

for all $i \in \mathbb{Z}$. Similarly, we apply the long exact cohomology sequence of (2.104) induced from the short exact sequence

$$0 \to B/\mathrm{Ker}(g) \to C \to D \to 0$$

to deduce an isomorphism

$$H_T^{i+1}(G, B/\mathrm{Ker}(g)) \simeq H_T^i(G, D).$$

However, we have that $B/\mathrm{Ker}(g) \simeq B/\mathrm{Im}(f)$ by exactness in the middle, so we get the desired result. □

□

Despite the remarkably elementary proof of this theorem, it has several amazing consequences especially when combined with Theorem 2.64. In particular, we deduce the following.

Corollary 2.108. *For L/K a finite cyclic Galois extension, we have an isomorphism*

$$\mathrm{Br}(L/K) \simeq K^*/\mathrm{Nm}_{L/K}(L^*).$$

In particular, by Remark 2.61, the set of isomorphism classes of division algebras over K split over L is in bijection with $K^*/\mathrm{Nm}_{L/K}(L^*)$

Proof. Indeed, we have an identification

$$H^2_T(\mathrm{Gal}(L/K), L^*) = H^2(\mathrm{Gal}(L/K), L^*) \simeq \mathrm{Br}(L/K)$$

by Theorem 2.64. Similarly, we have an identification

$$H^0_T(\mathrm{Gal}(L/K), L^*) = (L^*)^{\mathrm{Gal}(L/K)}/\mathrm{Nm}_{\mathrm{Gal}(L/K)}(L^*) \simeq K^*/\mathrm{Nm}_{L/K}(L^*)$$

Therefore, the result is an immediate consequence of 2.106. □

In particular, this allows us to very beautifully see the relationship already alluded to in Exercise 2.58. Namely, that the existence of a non-split division algebras attached to a cyclic extension L/K is intimately related to the surjectivity of the norm map $\mathrm{Nm}_{L/K} : L^* \to K^*$! We can use this to understand the structure of a division algebras in a wide variety of contexts.

Exercise 2.109 (Division Algebras over Finite and p-adic Fields)**.** *Fix a prime p and let $q = p^f$ for some integer $f \geq 1$. Let $g \geq 1$ and consider the finite cyclic Galois extension $\mathbb{F}_{q^g}/\mathbb{F}_q$. We write $\mathrm{Frob}_q : \mathbb{F}_{q^g} \to \mathbb{F}_{q^g}$ for the qth power Frobenius $x \mapsto x^q$.*

Similarly, we consider $\mathbb{Q}_q/\mathbb{Q}_p$ to be an unramified extension of degree f (i.e the natural map $\mathrm{Gal}(\mathbb{Q}_{p^g}/\mathbb{Q}_p) \to \mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)$) given by reduction mod p is an isomorphism (See §3.2.1 for a review). We let $\mathbb{Q}_{q^g}/\mathbb{Q}_q$ be the unramified extension of $\mathbb{Q}_q$ of degree g, and write $\sigma \in \mathrm{Gal}(\mathbb{Q}_{q^g}/\mathbb{Q}_q)$ to be the natural lift of Frob_q under the isomorphism $\mathrm{Gal}(\mathbb{Q}_{q^g}/\mathbb{Q}_q) \to \mathrm{Gal}(\mathbb{F}_{q^g}/\mathbb{F}_q)$ given by mod p-reduction.

Recall that, for any finite extension $K/\mathbb{Q}_p$, with ring of integers $\mathcal{O}_K$ and uniformizing element $\pi \in \mathcal{O}_K$, we have an isomorphism

$$K^* \simeq \mathcal{O}_K^* \times \langle \pi^{\mathbb{Z}} \rangle, \tag{2.41}$$

of abelian groups. Moreover, we have a short exact sequence

$$0 \to U_K^1 \to \mathcal{O}_K^* \to (\mathcal{O}_K/\pi)^* \to 0 \tag{2.42}$$

of abelian groups, where the last map is given by mod π-reduction. Show the following.

(1) Consider the norm map

$$\mathrm{Nm}_{\mathbb{F}_{q^g}/\mathbb{F}_q} : \mathbb{F}_{q^g}^* \to \mathbb{F}_q^*.$$
$$x \mapsto \prod_{i=0}^{g-1} (\mathrm{Frob}_q)^i(x).$$

Show that $\mathrm{Nm}_{\mathbb{F}_{q^g}/\mathbb{F}_q}$ is surjective and compute the kernel. Describe the Tate cohomology groups $H^i_T(\mathrm{Gal}(\mathbb{F}_{q^g}/\mathbb{F}_q), \mathbb{F}_{q^g}^*)$ for all $i \in \mathbb{Z}$.

(2) Using part (2), deduce the following.

Theorem 2.110. ***(Wedderburn's Little Theorem)*** *Let $\mathbb{F}_q$ be a finite field then every finite-dimensional division algebra over $\mathbb{F}_q$ splits over a finite extension of $\mathbb{F}_q$.*

(3) Show that the short exact sequence (2.42) when specialized to $K = \mathbb{Q}_{q^g}$ and $K = \mathbb{Q}_q$ gives rise to a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U^1_{\mathbb{Q}_{q^g}} & \longrightarrow & \mathcal{O}_{\mathbb{Q}_{q^g}^*} & \longrightarrow & \mathbb{F}_{q^g}^* & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Nm}_{\mathbb{Q}_{q^g}/\mathbb{Q}_q}} & & \downarrow{\scriptstyle \mathrm{Nm}_{\mathbb{Q}_{q^g}/\mathbb{Q}_q}} & & \downarrow{\scriptstyle \mathrm{Nm}_{\mathbb{F}_{q^g}/\mathbb{F}_q}} & & \\ 0 & \longrightarrow & U^1_{\mathbb{Q}_q} & \longrightarrow & \mathcal{O}_{\mathbb{Q}_q^*} & \longrightarrow & \mathbb{F}_q^* & \longrightarrow & 0 \end{array} \tag{2.43}$$

of short exact sequences.

(4) Show that $\mathrm{Nm}_{\mathbb{Q}_{q^g}/\mathbb{Q}_q} : U^1_{\mathbb{Q}_{q^g}} \to U^1_{\mathbb{Q}_q}$ is surjective (Hint: Use Hensel's Lemma).

(5) Combine (1), (3), and (4) with the product decomposition 2.41 to deduce that

$$\mathbb{Q}_q^*/\mathrm{Nm}_{\mathbb{Q}_{q^g}/\mathbb{Q}_q}(\mathbb{Q}_{q^g}^*) \simeq \mathbb{Z}/g\mathbb{Z}.$$

What can you conclude about division algebras over $\mathbb{Q}_q$?

We now leave off with an important invariant that the periodic nature of Tate cohomology highlights for us. In particular, it tells us that the entire Tate-cohomology of a cyclic group is captured by two groups namely the H_T^{-1} and H_T^0 which are both very explicit invariants. We introduce the following invariant to keep track of this.

Definition 2.111. Let G be a finite cyclic group and $M \in \mathrm{Mod}_G$. If the groups $H_T^i(G, M)$ are finite, we define the Herbrand quotient as the ratio

$$h(M) := |H_T^0(G, M)|/|H_T^{-1}(G, M)|,$$

where $|\cdot|$ denotes the cardinality of a set.

We have the following basic example.

Example 2.112. Suppose that G is a cyclic group and $M = \mathbb{Z}$ is equipped with the trivial G-action. Note that the norm map

$$\mathrm{Nm}_G : \mathbb{Z} \to \mathbb{Z}^G = \mathbb{Z}$$

identifies with the multiplication by $|G|$ map. In particular, we have that

$$H_T^0(G, \mathbb{Z}) = \mathbb{Z}/|G|\mathbb{Z}$$

and

$$H_T^{-1}(G, \mathbb{Z}) = 0,$$

so in this case the Herbrand quotient $h(\mathbb{Z})$ exists and we have that $h(\mathbb{Z}) = \mathbb{Z}/|G|\mathbb{Z}$.

The key point behind this definition is that often times it will be easier to compute Herbrand quotient rather than each of the individual Tate cohomology groups. However, knowing the Herbrand quotient will cut our work in half telling us that if we compute the size of one of the cohomology groups we know the other. We have the following basic properties of this.

Proposition 2.113. *The following is true.*

(1) Suppose we have a short exact sequence

$$0 \to A \to B \to C \to 0$$

in Mod_G*. If two out of three terms of the short exact sequence have Herbrand quotients then so does the third. Moreover, in this situation, we have the following relationship*

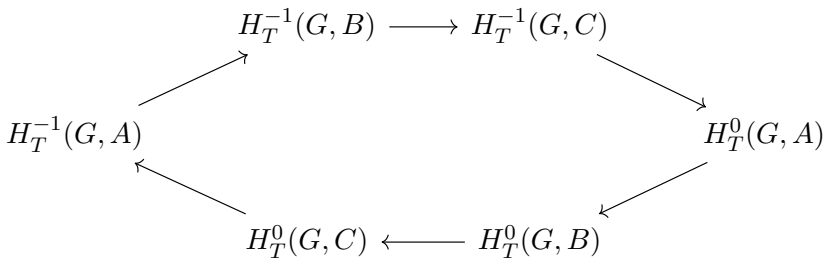
$$h(B) = h(A)h(C)$$

of Herbrand quotients.

(2) Suppose that M is finite then we have that

$$h(M) = 1$$

Proof. In the situation of (1), we note that Theorem 2.106 tells us that the long exact cohomology sequence of 2.104 gives rise to an exact hexagon



,

which in particular implies (1).

If M is finite then obviously $H_T^{-1}(G,M)$ and $H_T^0(G,M)$ are both finite and the Herbrand quotient exists. In order to see it is 1, we observe that we have exact sequences

$$0 \to M^G \to M \to M \to M_G \to 0,$$

where the middle map is given by $m \mapsto \sigma.m - m$ for a cyclic generator $\langle\sigma\rangle = G$ (See Exercise 2.101 (2) for the exactness on the right). Moreover, by definition, we have a short exact sequence

$$0 \to H_T^{-1}(G,M) \to M_G \xrightarrow{\overline{\mathrm{Nm}_G}} M^G \to H_T^0(G,M) \to 0.$$

By the second exact sequence, we see that we have an equality

$$h(M) := |M^G|/|M_G|$$

which by the first exact sequence is equal to 1, as desired. □

We now turn to some final compliments on cohomology before approaching the proof of local class field theory.

2.6. **Final Compliments on Cohomology and Tate's Theorem.** We start with the following notion.

2.6.1. *The Cup Product.* We recall the following.

Proposition 2.114. *Let G be a finite group and $M, N \in \mathrm{Mod}_G$ then there are bilinear maps*

$$(-)\cup(-) : H^p(G,M) \times H^q(G,N) \to H^{p+q}(G, M \otimes_{\mathbb{Z}} N)$$

for all $p, q \geq 0$ and

$$(-)\cup(-) : H_T^p(G,M) \times H_T^q(G,N) \to H_T^{p+q}(G, M \otimes_{\mathbb{Z}} N)$$

for all $p, q \in \mathbb{Z}$, which are functorial in M and N. We refer to the operation $(-)\cup(-)$ as the "cup-product".

Proof. We first describe the construction of the cup product for cohomology and then deduce the claim for the Tate cohomology. We will construct this at the level of cochains. In particular, homogeneous cochains $C^n(G,M)_{\mathrm{hom}}$, as in Remark 2.46. In particular, we define a natural map

$$\begin{aligned} C^p(G,M)_{\mathrm{hom}} \otimes C^q(G,N)_{\mathrm{hom}} &\to C^{p+q}(G, N \otimes M)_{\mathrm{hom}} \\ f(x_0,\dots,x_p) \otimes g(x_0,\dots,x_q) &\mapsto (f \cup g)(x_0,\dots,x_{p+q}), \end{aligned} \tag{2.44}$$

where

$$(f \cup g)(x_0,\dots,x_{p+q}) := f(x_0,\dots,x_p) \otimes g(x_p,\dots,x_{p+q}).$$

We abuse notation and write $\partial : C^n(G,M)_{\mathrm{hom}} \to C^{n+1}(G,M)_{\mathrm{hom}}$ for the natural differential on homogenous cochains, as induced by (2.15). We then check the following.

Lemma 2.115. *We have an equality*

$$\partial(f \cup g) = \partial(f) \cup g + (-1)^p (f \cup \partial(g))$$

in $C^{p+q+1}(G, M \otimes N)_{\mathrm{hom}}$

Proof. We have that

$$\partial(f \cup g)(x_0,\dots,x_{p+q+1}) = \sum_{i=0}^{p+q+1} (-1)^i (f \cup g)(x_0,\dots,\hat{x}_i,\dots,x_{p+q+1}),$$

which we may break up as

$$\sum_{i=0}^{p}(-1)^i f(x_0,\dots,\hat{x}_i,\dots,x_{p+1})\otimes g(x_{p+1},\dots,x_{p+q+1})+\sum_{i=p+1}^{p+q+1}(-1)^i f(x_0,\dots,x_p)\otimes g(x_p,\dots,\hat{x}_i,\dots,x_{p+q+1}).$$

However, we readily identify the first term with $\partial(f)\cup g$ and the second term with $(-1)^p(f\cup\partial(g))$, as desired. □

In particular, the lemma tells us that $f\cup g$ satisfies the cocycle condition if f and g are cocycles. Therefore, the map (2.44) restricts to a well-defined map on cocycles. Moreover, after restricting to cocycles, it tells us that $f\cup g$ is a coboundary if either f or g is a coboundary. Therefore, we get a well-defined map on cohomology. It is clear that this is functorial in M and N and is bi-linear. For the Tate-cohomology, we look at the natural map

$$0\to M'\to \mathrm{Ind}_1^G\mathrm{Res}_1^G M\to M\to 0,$$

where the last map is given by adjunction and M' is the kernel. This in particular gives us an isomorphism $H_T^{i-1}(G,M)\simeq H_T^i(G,M)$ by (2.104) and Schapiro's Lemma 2.103 (1). This allows us to reduce to constructing the desired map to the case where the indices are given by $p\geq 1$ and $q\geq 1$ in which case it follows from the claim on cohomology described above. This is the dimension shifting principle mentioned in 2.37 and 2.69. □

For many applications, one often considers the following variant of the cup product.

Construction 2.116. *Suppose we have $M,N,C\in Mod_G$ together with a bilinear pairing*

$$b: M\otimes_{\mathbb{Z}} N\to C$$

then we obtain a bilinear maps

$$H^p(G,M)\times H^q(G,N)\to H^{p+q}(G,M\otimes_{\mathbb{Z}}N)\xrightarrow{H^{p+q}(f)}H^{p+q}(G,C)$$

for all $p,q\geq 0$ and bilinear maps

$$H_T^p(G,M)\times H_T^q(G,N)\to H_T^{p+q}(G,M\otimes_{\mathbb{Z}}N)\xrightarrow{H_T^{p+q}(f)}H_T^{p+q}(G,C)$$

for all $p,q\in\mathbb{Z}$.

We will also refer to this as a cup-product. It has the following compatibilities whose verification is routine (See [NSW08, Section 4] for a very detailed discussion).

Proposition 2.117. *Suppose we have $M,N\in \mathrm{Mod}_G$, and a bilinear pairing $M\otimes_{\mathbb{Z}}N\to C$, we consider the cup product as in 2.116 defined with respect to this datum. Let $f\in H^p(G,M)$, $g\in H^q(G,M)$, and $h\in H^r(G,M)$ be elements. Then the following is true.*

(1) The cup product is associative and symmetric up to the Koszul rule for signs. I.e we have

$$(f\cup g)\cup h=f\cup(g\cup h)$$

in $H^{p+q+r}(G,C)$, and

$$(f\cup g)=(-1)^{pq}(g\cup f),$$

in $H^{p+q}(G,C)$. The analogous claims hold for Tate cohomology.

(2) The cup product is compatible with restriction. In other words, if we have an inclusion $H\subset G$ of finite groups there is a natural isomorphism

$$\mathrm{Res}_H^G(f\cup g)=\mathrm{Res}_H^G(f)\cup\mathrm{Res}_H^G(g)$$

in $H^{p+q}(H,\mathrm{Res}_H^G(C))$, and similarly for Tate-cohomology.

We now turn to the following.

2.6.2. *Inflation-Restriction Exact Sequence.* We have the following fundamental result.

Proposition 2.118. *Let G be a finite group and $H \subset G$ a normal subgroup and $M \in \mathrm{Mod}_G$. If $H^i(H, \mathrm{Res}^G_H(M)) = 0$ for $i = 1, \dots, r-1$ then the sequence*

$$0 \to H^r(G/H, M^H) \xrightarrow{\mathrm{Inf}^G_H} H^r(G, M) \xrightarrow{\mathrm{Res}^G_H} H^r(H, M)$$

is exact, where we recall that the first map is the inflation map of 2.75.

Proof. We will proceed by induction on r using the dimension shifting principle of Remark 2.37. For $r = 1$, the condition is empty. We recall by 2.47 we may interpret classes in $H^1(G, M)$ as maps $\phi : G \to M$. If it lies in the image of Inf^G_H then up to changing by a coboundary it must factor through $\phi : G/H \to M$; in other words, ϕ is constant when restricted to H. Moreover, the value when restricted to H must lie inside M^H. In particular, if we look now at the cocycle condition

$$h.\phi(g) = \phi(hg) - \phi(h)$$

and assume that $h \in H$ and $g \in H$ then this becomes

$$\phi(g) + \phi(h) = \phi(hg)$$

and this forces ϕ to be trivial when restricted to H, since this is a homomorphism. Therefore, it lies in the kernel of the restriction map, as desired. Conversely, if we have some $m \in M$ such that $\phi(h) = h.m - m$ for all $h \in H$ then $\phi'(g) = \phi(g) - g.m + m$ represents the same class as ϕ inside $H^1(G, M)$, but it has value 0 on H. Indeed, for all $h \in H$ and $g \in G$, we have

$$\phi'(hg) = g\phi'(h) + \phi'(g) = \phi'(g),$$

by the cocycle condition since $\phi'(h) = 0$. However, this implies that ϕ' factors through $G \to G/H$. Similarly, for all $g \in G$ and $h \in H$, we have that

$$h\phi'(g) = \phi'(hg) - \phi'(h) = \phi'(g)$$

by the cocycle condition since $\phi'(h) = 0$, so ϕ' lies in M^H. Exactness on the left is similar. In general, we look at the sequence

$$0 \to M \to \mathrm{Ind}^G_1 \mathrm{Res}^G_1(M) \to N \to 0 \tag{2.45}$$

where the first map is the adjunction map. The long exact sequence in cohomology (Proposition 2.30) and Schapiro's Lemma 2.41 gives us isomorphisms

$$H^i(G, N) \xrightarrow{\simeq} H^{i+1}(G, M)$$

and

$$H^i(H, \mathrm{Res}^G_H(N)) \xrightarrow{\simeq} H^{i+1}(H, \mathrm{Res}^G_H(M)),$$

where, for the second isomorphism, we have used that the restriction of an induced module is again an induced module (Remark 2.43) to apply Schapiro's Lemma. Moreover, we deduce that $H^i(H, \mathrm{Res}^G_H(N))$ vanishes for $i = 1, \dots, r-2$, by our assumption on the vanishing of $H^{i+1}(H, \mathrm{Res}^G_H(M))$. In particular, we may use these isomorphisms to fill in the following commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^{r-1}(G/H, N^H) & \xrightarrow{\mathrm{Inf}^G_H} & H^{r-1}(G, N) & \xrightarrow{\mathrm{Res}^G_H} & H^{r-1}(H, \mathrm{Res}^G_H(N)) \\
 & & & & \downarrow \simeq & & \downarrow \simeq \\
 & & H^r(G/H, M^H) & \xrightarrow{\mathrm{Inf}^G_H} & H^r(G, M) & \xrightarrow{\mathrm{Res}^G_H} & H^r(H, \mathrm{Res}^G_H(M)),
\end{array}$$

where we have used our inductive hypothesis to conclude exactness of the top row. Moreover, we note that have used the compatability of the restriction map with the boundary map in the long

exact sequence to see the commutativity of the right diagram. We would be finished if we could construct an isomorphism

$$H^{r-1}(G/H, N^H) \to H^r(G/H, M^H)$$

making the diagram commute, as exactness of the top row would imply exactness of the bottom row. We accomplish this as follows. We take invariants of (2.45) under H and apply the long exact sequence of cohomology to deduce the existence of a short exact sequence

$$0 \to M^H \to (\mathrm{Ind}_1^G \mathrm{Res}_1^G M)^H \to N^H \to H^1(H, \mathrm{Res}_H^G(M)) = 0,$$

where here we have used our vanishing hypothesis on cohomology. We may now in turn consider the long exact cohomology sequence applied to G/H. We note that the boundary map in turn gives the desired isomorphism

$$H^{r-1}(G/H, N^H) \xrightarrow{\simeq} H^r(G/H, M^H).$$

Indeed $(\mathrm{Ind}_1^G \mathrm{Res}_1^G(M))^H \simeq (\mathbb{Z}[G]^H \otimes_{\mathbb{Z}} M) \simeq \mathbb{Z}[G/H] \otimes_{\mathbb{Z}} M$ is an induced module for G/H. □

We now combine this with the Tate-periodicity Theorem to deduce the following fundamental result, which essentially tells us that one version of the consequences of Tate-periodicity at least always holds for any group G.

Theorem 2.119. *Let $M \in \mathrm{Mod}_G$ suppose that $H^i(H, \mathrm{Res}_H^G(M)) = 0$ for $i = 1, 2$ and H any normal subgroup of G then $H_T^i(G, M) = 0$ for all $i \in \mathbb{Z}$.*

Proof. Note that if G was cyclic this would be an immediate consequence of the Tate periodicity theorem (Theorem 2.106).

We first assume that G is solvable and show the vanishing for all $H_T^i(G, M)$ for all $i \geq 0$. We use induction on the number of subgroups of G. If G is trivial there is nothing prove. In general, since G is solvable, we may find a proper normal subgroup $H \subset G$ for which G/H is cyclic. By the induction hypothesis, $H_T^i(H, \mathrm{Res}_H^G(M)) = 0$ for all $i \geq 0$. Thus, by Proposition 2.118, we have a short exact sequence

$$0 \to H^i(G/H, M^H) \to H^i(G, M) \to H^i(H, \mathrm{Res}_H^G(M)) \tag{2.46}$$

for all $i > 0$ and therefore we obtain an isomorphism $H^i(G/H, M^H) \xrightarrow{\simeq} H^i(G, M) = 0$, for $i = 1, 2$. Since G/H is cyclic, we know that $H_T^i(G/H, M^H)$ is trivial for all $i \in \mathbb{Z}$. However, that then implies that $H^i(G, M) = 0$ for all $i > 0$ by the short exact sequence (2.46). It remains to show that $H_T^0(G, M) = 0$. The vanishing of $H_T^0(G/H, M^H)$ tells you that every $x \in M^G = (M^H)^{G/H}$ can be written in the form $\mathrm{Nm}_{G/H}(y)$ for some $y \in M^H$ and the vanishing of $H_T^0(H, \mathrm{Res}_H^G(M))$ by the inductive hypothesis tells you that $\mathrm{Nm}_H(z) = y$ for some $z \in M$. One easily checks that $\mathrm{Nm}_{G/H} \circ \mathrm{Nm}_H = \mathrm{Nm}_G$, implying the desired claim.

We let G be arbitrary, we prove that $H_T^i(G, M)$ for all $i \geq 0$ by induction on the size of the set $|G|$. We know that the groups $H_T^i(G, M)$ are $|G|$-torsion, as described in Example 2.105 (5). In particular, it suffices to show its p-primary components are trivial for all p. We choose a p-Sylow subgroup $G_p \subset G$, and look at the restriction corestriction sequence

$$H_T^i(G, M) \xrightarrow{\mathrm{Res}_{G_p}^G} H_T^i(G_p, \mathrm{Res}_{G_p}^G(M)) \xrightarrow{\mathrm{CoRes}_{G_p}^G} H_T^i(G, M)$$

which is given by multiplication by $[G : G_p]$, as in Lemma 2.86 this allows to conclude that the first map is an injective on p-primary parts. Moreover, we see that $H_T^i(G_p, \mathrm{Res}_{G_p}^G(M))$ vanishes for $i = 1, 2$ by our assumption on M. Since this is a solvable group, we may use the above case to conclude that $H_T^i(G, \mathrm{Res}_{G_p}^G(M))$ vanishes for all i which implies the p-primary part of $H_T^i(G, M)$ vanishes for all $i \geq 0$, as desired.

The case where $i < 0$ follows from dimension shifting. In particular, one analyzes the sequence

$$0 \to N \to \mathrm{Ind}_1^G \mathrm{Res}_1^G(M) \to M \to 0,$$

of Remark 2.37, where the last map is given by adjunction, as in the proof of Proposition 2.114. □

We will need to following construction in what follows.

Exercise 2.120. *Let $M \in \mathrm{Mod}_G$ and e denote the identity element of G. Suppose we have a homogenous 2-cocycle $\phi : G^3 \to M$ representing a class in $H^2(G, M)$. We recall that this means that*

$$\phi(gg_0, gg_1, g_2g) = g.\phi(g_0, g_1, g_2)$$

and

$$\phi(g_1, g_2, g_3) - \phi(g_0, g_2, g_3) + \phi(g_0, g_1, g_3) - \phi(g_0, g_1, g_2) = 0$$

Moreover, this is a coboundary if and only if

$$\phi(g_0, g_1, g_2) = \rho(g_1, g_2) - \rho(g_0, g_2) + \rho(g_0, g_1) \tag{2.47}$$

for $\rho : G^2 \to M$ satisfying the condition that $\rho(gg_0, gg_1) = \rho(g_0, g_1)$. We let $M[\phi]$ be the splitting module of ϕ. As an abelian group, this is given by

$$M[\phi] := M \oplus \bigoplus_{g \in G \setminus \{e\}} \mathbb{Z}x_g$$

and we equip it with the G-action

$$g.x_h = x_{gh} - x_g + \phi(e, g, gh) \tag{2.48}$$

where in this formula $x_e := \phi(e, e, e)$ and the usual G-action of M on the first coordinate. Show the following.

1. *Check that (2.48) gives rise to a well-defined G-action.*
2. *Combine the above formulae to show that ϕ is a cobounadry if and only if*

   $$\phi(e, g, gh) = g\rho(e, h) - \rho(e, gh) + \rho(e, g).$$

   for some $\rho : G^2 \to M$ as above.
3. *Show that the natural map $M \to M[\phi]$ given by the inclusion of M induces a natural map*

   $$H^2(G, M) \to H^2(G, M[\phi]),$$

   which will send ϕ to 0, by using (2) and setting $\rho(e, g) = x_g$ for all $g \in G$.
4. *Show that the natural map*

   $$\alpha : M[\phi] \to \mathbb{Z}[G]$$

   sending x_g to $[g] - 1$ is a homomorphism of G-modules. Deduce the existence of a a short exact sequence

$$0 \to M \to M[\phi] \to I_G \to 0. \tag{2.49}$$

We now have the following, which will be essential for the proof of local class field theory. In particular, as we will see the proof will essentially reduce us to checking the assumptions of the theorem for $G = \mathrm{Gal}(L/K)$ and $M = L^*$.

Theorem 2.121. ***(Tate-Nakayama Theorem)*** *Let $M \in \mathrm{Mod}_G$. Suppose that, for all normal subgroups $H \subset G$, the following holds:*

1. *We have that $H^1(H, \mathrm{Res}^G_H(M)) = 0$.*
2. *We have that $H^2(H, \mathrm{Res}^G_H(M))$ is cyclic of order $|H|$.*

Then, for any generator γ of $H^2(G, M) = H^2_T(G, M)$ and $i \in \mathbb{Z}$, the cup product

$$\gamma \cup (-) : H^i_T(G, \mathbb{Z}) \to H^{i+2}_T(G, M)$$

of Proposition 2.114 is an isomorphism.

Proof. By Lemma 2.71, we know that Cor$\circ$Res $= [G : H]$. In particular, this implies that $\mathrm{Res}(\gamma)$ also generates $H^2(H, \mathrm{Res}^G_H(M))$ by (2). We choose a homogenous 2-cocycle $\phi : G^3 \to M$ representing γ. We let $M[\phi]$ be the G-module described in Exercise 2.120. We consider the short exact sequences

$$0 \to M \to M[\phi] \to I_G \to 0 \tag{2.50}$$

of (2.49) and

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0. \tag{2.51}$$

of (2.33). The long exact sequence in Tate cohomology applied to (2.51) and Schapiro's Lemma gives us an isomorphism

$$H^1(H, \mathrm{Res}^G_H I_G) \simeq H^0_T(H, \mathbb{Z}) = \mathbb{Z}/|H|\mathbb{Z},$$

where the second equality follows from the fact that the Norm map on a H-module with trivial action is just given by multiplication by $|H|$. Similarly, we have

$$H^2(H, \mathrm{Res}^G_H I_G) \simeq H^1(H, \mathbb{Z}) = 0,$$

where the second equality follows since $H^1(H, \mathbb{Z}) = \mathrm{Hom}(H^{ab}, \mathbb{Z})$ and H is finite, as in Example 2.47. Now, by applying the long exact cohomology sequence to (2.50), we obtain

$$\begin{aligned} 0 = H^1(H, \mathrm{Res}^G_H M) \to H^1(H, \mathrm{Res}^G_H M[\phi]) \to H^1(H, \mathrm{Res}^G_H I_G) \\ \to H^2(H, \mathrm{Res}^G_H M) \to H^2(H, \mathrm{Res}^G_H M[\phi]) \to H^2(H, \mathrm{Res}^G_H I_G) = 0 \end{aligned}$$

However, by construction $H^2(H, \mathrm{Res}^G_H M)$ will be cyclic by assumption and the generator $\mathrm{Res}^G_H(\gamma)$ will map to $\mathrm{Res}^G_H \phi$ under $H^2(H, \mathrm{Res}^G_H M) \to H^2(H, \mathrm{Res}^G_H M[\phi])$, which will vanish by Exercise 2.120 (3). In particular, the map $H^2(H, \mathrm{Res}^G_H M) \to H^2(H, \mathrm{Res}^G_H M[\phi])$ is zero, so we deduce that $H^2(H, \mathrm{Res}^G_H M[\phi]) = 0$. We now deduce that $H^1(H, \mathrm{Res}^G_H(I_G)) \to H^2(H, \mathrm{Res}^G_H M[\phi])$ is a surjective map between two cyclic groups of the same order, and is therefore an isomorphism implying that $H^1(H, \mathrm{Res}^G_H M[\phi]) = 0$. In particular, we may now apply Theorem 2.119, to deduce that $H^i_T(H, \mathrm{Res}^G_H M[\phi])$ for all subgroups $H \subset G$ and $i \in \mathbb{Z}$. We now splice the two short exact sequences (2.50) and (2.51) to deduce a long exact sequence

$$0 \to M \to M[\phi] \to \mathbb{Z}[G] \to \mathbb{Z} \to 0,$$

which, by applying Lemma 2.107, gives an isomorphism $H^i_T(G, \mathbb{Z}) \xrightarrow{\simeq} H^{i+2}_T(G, M)$. Moreover, with a bit more work, one may verify this is the cup product with γ, as desired. □

Now that we have built up our foundations in group cohomology and homology, we are ready to turn to one of the most beautiful applications of this theory: the proof of local class field theory.

3. Local Class Field Theory, Reference: [Mil20a; Ked02]

Let $K/\mathbb{Q}_p$ be a finite extension of the p-adic numbers. We will refer to such fields as p-adic fields. In this section, we will use the machinery built up in the previous section to answer the following question: What is the profinite group $\mathrm{Gal}(K^{\mathrm{ab}}/K) := \lim_{L/K} \mathrm{Gal}(L/K)$, where L/K runs over finite Galois extension with abelian Galois group or alternatively what is $\lim_{L/K} \mathrm{Gal}(L/K)^{\mathrm{ab}}$, where L/K runs over all finite Galois extensions? We first explain the answer to this question before proceeding to use our machinery of Tate cohomology to establish the statements.

3.1. **The Statements.** We fix $K/\mathbb{Q}_p$ and let K^{ab}/K denote the maximal abelian extension. We write $\mathcal{O}_K \subset K$ for the ring of integers with uniformizing element π. The main result of class field theory is as follows.

Theorem 3.1. ***(The Local Reciprocity Law)*** *Let $K/\mathbb{Q}_p$ be a finite extension then there exists a unique map*

$$\phi_K : K^* \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

satisfying the following conditions:

1. *The image of the uniformizing element $\phi_K(\pi)$ is the Frobenius element, defined analogously to the global case, as in Construction 1.9 and Exercise 1.7.*
2. *For any finite abelian extension L/K, the composition*

$$K^* \xrightarrow{\phi_K} \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(L/K)$$

is a surjection with kernel isomorphic to $\mathrm{Nm}_{L/K}(L^*)$. In particular, we have an isomorphism

$$\phi_{L/K} : K^*/\mathrm{Nm}_{L/K}(L^*) \xrightarrow{\simeq} \mathrm{Gal}(L/K).$$

While we note that this essentially accomplishes our goal of describing the structure of all abelian extensions in terms of the multiplicative structure of our field, it is a bit lacking since we do not just have a clean description of the profinite group $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. Indeed, the map ϕ_K is not an isomorphism, as the π-adic topology of $K^* \subset K$ is fundamentally incompatible with that of the profinite group $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. In particular, K^* is locally compact (since it is a union of $\pi^i\mathcal{O}_K^*$ for all $i \in \mathbb{Z}$), but $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ is compact, by virtue of being a profinite group (Proposition 2.2). To resolve this, we have the following.

Theorem 3.2. ***(Local Existence Theorem)*** *Let L/K be a finite extension of p-adic fields then, for every finite (not necessarily abelian extension) the subgroup $\mathrm{Nm}_{L/K}(L^*) \subset K^*$ is open with respect to the π-adic topology and of finite index. Conversely, for every open subgroup $U \subset K^*$, there exists a finite abelian extension L of K such that $U = \mathrm{Nm}_{L/K}(L^*)$.*

We note that the first part of the Theorem is a fairly routine calculation. Indeed, the norm subgroups (I.e the subgroups $\mathrm{Nm}_{L/K}(L^*) \subset K^*$) are fairly explicit subgroups.

Exercise 3.3. *Let L/K be a finite extension of p-adic fields. Show that the following is true.*

1. *Show that $\mathrm{Nm}_{L/K}(L^*) \subset K^*$ is an open subgroup of finite index.*
2. *Show that, for all $n \geq 1$, the subgroup $(K^*)^n \subset K^*$ is an open subgroup of finite index.*

In particular, we note by Theorem 3.2, Theorem 3.1, and 3.3 (2) that there exists a finite abelian extension L/K such that $\mathrm{Nm}_{L/K}(L^*) = (K^*)^n \subset K^*$ and that we have an isomorphism $K^*/(K^*)^n \simeq \mathrm{Gal}(L/K)$. The description of these abelian extensions fits into a more general paradigm known as Kummer Theory.

Exercise 3.4. ***(Kummer Theory)*** *Let K be a field of characteristic 0. Let $\overline{K}/K$ denote the algebraic closure. We write $\mu_n \subset \overline{K}^*$ for the subgroup defined by the elements $x \in \overline{K}^*$ such that $x^n = 1$. We note that this has the natural structure of an object in $\mathrm{Mod}_{\mathrm{Gal}(\overline{K}/K),\mathrm{cont}}$. We consider the short exact sequence*

$$0 \to \mu_n \to \overline{K}^* \to \overline{K}^* \to 0, \tag{3.1}$$

in $\mathrm{Mod}_{\mathrm{Gal}(\overline{K}/K),\mathrm{cont}}$, where the last map is given by the multiplication by n-map. We assume that $\mu_n \subset K^*$.

1. *Show that we have an isomorphism $\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$ as $\mathrm{Gal}(\overline{K}/K)$-modules, where $\mathbb{Z}/n\mathbb{Z}$ has trivial Galois action.*

(2) *Use the long exact cohomology sequence attached to (3.1) to deduce the existence of an injective map*

$$K^*/(K^*)^n \hookrightarrow \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\overline{K}/K), \mu_n).$$

$$a \mapsto \{\sigma \mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}\},$$

(3) *If $a \in K^\times$ and $\alpha \in \overline{K}^*$, show that $\alpha^n = a$, show that for every $\sigma \in \mathrm{Gal}(K(\alpha)/K)$*

$$\sigma(\alpha) = \zeta\alpha \quad \textit{for some } \zeta \in \mu_n.$$

Deduce that $K(\alpha)/K$ is abelian of exponent dividing n.

(4) *If $\Delta \subset K^\times$ contains $(K^\times)^n$, define*

$$L_\Delta = K\big(\sqrt[n]{a} \mid a \in \Delta\big).$$

Show that L_Δ/K is abelian of exponent dividing n. Assume $\Delta/(K^\times)^n$ is finite. Prove that

$$\mathrm{Gal}(L_\Delta/K) \simeq \Delta/(K^\times)^n$$

(5) *Conclude that finite abelian extensions of K of exponent dividing n correspond to finite-index subgroups of $K^\times$ containing $(K^\times)^n$.*

(6) *Let $K/\mathbb{Q}_p$ be a p-adic field. Describe the extension corresponding to the open finite index subgroup $(K^*)^n \subset K^*$ in 3.3 (2) under local class field theory.*

(7) *Let $K/\mathbb{Q}_p$ be a p-adic field (not necessarily containing μ_ℓ) and let ℓ be a prime. Show that if $x \in \mathrm{Nm}_{L/K}(L^*)$ for all finite extensions L/K then x is an ℓth power.*

In particular, from this we deduce the following Corollary by combining Theorems 3.1 and 3.2, which gives us a nice description of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$.

Corollary 3.5. *The reciprocity map $\phi_K : K^* \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ induces an isomorphism*

$$\hat{\phi}_K : \hat{K}^* \xrightarrow{\simeq} \mathrm{Gal}(K^{\mathrm{ab}}/K),$$

where $\hat{K}^*$ is the profinite completion of K^*, as defined in Example 2.5 (3).

Moreover, Theorem 3.2 tells us that actually every subgroup of $\mathrm{Nm}_{L/K}(L^*) \subset K^*$ for a finite extension L/K arises from an abelian extension. However, it is natural to ask which one? This is the content of the norm limitation Theorem.

Theorem 3.6. ***(Norm Limitation Theorem)*** *Let L/K be a (not necessarily Galois) extension of p-adic fields. Let $K \subset M \subset L$ be the maximal abelian subextension of L/K. Then*

$$\mathrm{Nm}_{L/K}(L^*) = \mathrm{Nm}_{M/K}(M^*),$$

as desired.

Remark 3.7. We note that it is obvious by the identity $\mathrm{Nm}_{L/K} = \mathrm{Nm}_{M/K} \circ \mathrm{Nm}_{L/M}$ that we have an inclusion

$$\mathrm{Nm}_{L/K}(L^*) \subset \mathrm{Nm}_{M/K}(M^*).$$

Moreover, as in (Exercise 3.3) is easy to see that $\mathrm{Nm}_{L/K}(L^*)$ will be an open subgroup of finite index by direct calculation. In particular, by Theorem 3.2 we know that there exists some abelian extension $N \subset K$ such that $\mathrm{Nm}_{N/K}(N^*) = \mathrm{Nm}_{L/K}(L^*)$, and by Theorem 3.1 we know that we have an inclusion $N \subset M$. The key point is now to really show that $N = M$.

3.2. **The Key Calculations.** As already mentioned, the proof of Theorem 3.1 will follow from applying Theorem 2.121 to $M = L^*$ and $G = \mathrm{Gal}(L/K)$ for L/K a finite Galois extension of local fields. To do this, for all Galois subextensions $K \subset M \subset L$ with associated subgroup $\mathrm{Gal}(L/M)$, by Galois theory, we need to show the following.

(1) $H^1(\mathrm{Gal}(L/M), L^*) = 0$
(2) $H^2(\mathrm{Gal}(L/M), L^*)$ is cyclic of order $[L : M]$.

Here item (1) will follow by Theorem 2.50. We already essentially saw that $H^2(\mathrm{Gal}(L/M), L^*)$ is cyclic of order $[L : M]$ in the case of the unramified extension $\mathbb{Q}_{q^g}/\mathbb{Q}_q$ in Exercise 2.109, and our goal will now be to push this claim further.Our goal is to extend this to any extension L/K. In particular, we want to show the following.

Goal 3.8. *For L/K finite Galois extensions of p-adic fields, we have an isomorphism*

$$H^2(\mathrm{Gal}(L/K), L^*) \simeq \mathbb{Z}/[L : K]\mathbb{Z}.$$

Indeed, by the above discussion we have the following.

Theorem 3.9. *Assume L/K is a finite Galois extension of p-adic fields, then, assuming 3.8, we have an isomorphism*

$$\mathrm{Gal}(L^{\mathrm{ab}}/K) = \mathrm{Gal}(L/K)^{\mathrm{ab}} \simeq H_T^{-2}(\mathrm{Gal}(L/K), \mathbb{Z}) \xrightarrow{\simeq} H_T^0(\mathrm{Gal}(L/K), L^*) \simeq K^*/\mathrm{Nm}_{L/K}(L^*),$$

induced by cupping with a generator $\langle u_{L/K} \rangle \simeq \mathbb{Z}/[L : K]\mathbb{Z} \simeq H^2(\mathrm{Gal}(L/K), L^*)$.

Before trying to acheive Goal 3.8, we briefly review the structure of the Galois groups of local fields.

3.2.1. *Brief Aside on The Structure of the Galois Group of a Local Field.* For a finite extension $K/\mathbb{Q}_p$, we write $\mathcal{O}_K$ for the ring of integers with uniformizing element $\pi_K \in \mathcal{O}_K$. We denote the residue field by $\kappa_K := \mathcal{O}_K/\pi_K$. We let $v_K(-) : K \to \mathbb{Z} \cup \{\infty\}$ denote the K-adic valuation. We recall that we may define this by

$$v_K := \frac{1}{f(K/\mathbb{Q}_p)} v_p(\mathrm{Nm}_{K/\mathbb{Q}_p}(-)), \tag{3.2}$$

where v_p denotes the usual p-adic valuation on $\mathbb{Q}_p$ and $\mathrm{Nm}_{K/\mathbb{Q}_p} : K \to \mathbb{Q}_p$ is the norm map. Here $f_{K/\mathbb{Q}_p} \in \mathbb{N}_{\geq 1}$ is the ramification index, which we introduce below (See 3.7) We similarly set

$$|\cdot|_K : K \to \mathbb{R} \tag{3.3}$$

to be given by $p^{-v_K(-)}$ on K^* and we let it send 0 to 0. In particular, we note that, by the description of the Norm map for L/K is a finite Galois extension, we have that $|\sigma(\cdot)|_L = |\cdot|_L$ is invariant under the Galois action, and similarly for the valuations. Moreover, we may describe the ring of integers by the formula $\mathcal{O}_K = \nu_K^{-1}(\mathbb{N}_{\geq 0} \cup \{\infty\})$ and the maximal ideal of $\mathcal{O}_K$ generated by the uniformizer π_K by the formula $\mathfrak{m}_K := (\pi_K) = \nu_K^{-1}(\mathbb{N}_{>0} \cup \{\infty\})$.

As a consequence of this discussion we deduce that, for a finite Galois extension L/K the Galois group $\mathrm{Gal}(L/K)$ preserves the extension of ring of integers $\mathcal{O}_L/\mathcal{O}_K$ and induces an automorphism of the extension of finite fields κ_L/κ_K. In particular, we deduce the existence of a well-defined map

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(\kappa_L/\kappa_K),$$

which as in 1.7 (4)-(5) will be a surjective map. This induces a short exact sequence

$$0 \to I(L/K) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(\kappa_L/\kappa_K) \to 0, \tag{3.4}$$

where the kernel $I(L/K)$ of the surjection is referred to as the inertia group. The group $\mathrm{Gal}(\kappa_L/\kappa_K)$ is cyclic as κ_L/κ_K is an extension of finite fields. In particular, this is the first step on a filtration on $\mathrm{Gal}(L/K)$ where the graded pieces are cyclic. To proceed further, we need to analyze the group $I(L/K)$. To this end, we first note that one way of describing $I(L/K)$ is that it is the elements

of $\mathrm{Gal}(L/K)$ which are trivial when one looks at their induced action on $\mathrm{Aut}(\mathcal{O}_L/\mathfrak{m}_L \simeq \kappa_L)$. However, since $\mathrm{Gal}(L/K)$ preserves the valuation, we note that it also preserves the subgroups $\mathfrak{m}_L^n$ for all $n \geq 1$. In particular, we could also look at the homomorphism

$$\mathrm{Gal}(L/K) \to \mathrm{Aut}(\mathcal{O}_L/\mathfrak{m}_L^{n+1})$$

for all $n \geq 0$ and set $I_n(L/K)$ to be the kernel of this map. This defines for us the ramification filtration on $\mathrm{Gal}(L/K)$ with the lower numbering

$$\cdots \subset I_{n+1}(L/K) \subset I_n(L/K) \subset \cdots I_1(L/K) \subset I_0(L/K) = I(L/K) \subset \mathrm{Gal}(L/K).$$

We note that if we have an element in the intersection of all the subgroups $\mathrm{Gal}(L/K) := \bigcap_{n\geq 1} I_n(L/K)$ then the action of this element on $\mathcal{O}_L = \varprojlim_{n\geq 1} \mathcal{O}_L/\pi^n$ is also trivial which implies it must be the identity element. In particular, this filtration is exhaustive. Moreover, since $\mathrm{Gal}(L/K)$ is finite we must have that $I_n(L/K) = \{e\}$ for sufficiently large n. Note that we can also alternatively view $I_n(L/K)$ as the subgroup of elements $\sigma \in \mathrm{Gal}(L/K)$ such that $|\sigma(\pi_L) - \pi_L|_L < |\pi_L|_L^n$ by writing elements of $\mathcal{O}_L$ as power series in π_L. Now, using this description, we can describe the graded pieces of this filtration. More precisely, recalling that $\mathfrak{m}_L^n/\mathfrak{m}_L^{n+1} \simeq \kappa_L$ for all $n \geq 0$, we note that we may define maps

$$\begin{aligned} I(L/K)/I_1(L/K) &\to \kappa_L^* \\ \sigma &\mapsto \frac{\sigma(\pi_L)}{\pi_L} \bmod \mathfrak{m}_L \end{aligned} \tag{3.5}$$

and

$$\begin{aligned} I_n(L/K)/I_{n+1}(L/K) &\to \mathfrak{m}_L^n/\mathfrak{m}_L^{n+1} \simeq \kappa_L \\ \sigma &\mapsto \frac{\sigma(\pi_L)}{\pi_L} - 1 \bmod \mathfrak{m}_L^{n+1} \end{aligned} \tag{3.6}$$

Now we have the following.

Proposition 3.10. *The maps (3.5) and (3.6) are injective. In particular, by combining with the short exact sequence (3.4) we deduce that* $\mathrm{Gal}(L/K)$ *is solvable, for* L/K *a finite Galois extension of p-adic fields.*

Proof. See [Mil20b, Corollary 7.59]. □

We now want to endow this filtration with some more meaning. In particular, we recall that, since $\mathcal{O}_L$ is a DVR, we have that

$$(\pi_K)\mathcal{O}_L = (\pi_L^{e(L/K)}), \tag{3.7}$$

where $e(L/K)$ is referred to as the ramification index of e in L/K. As in Exercise 1.7 (2), we have also have the invariant

$$f(L/K) := [\kappa_L : \kappa_K] \tag{3.8}$$

These two invariants will satisfy the relationship

$$f(L/K)e(L/K) = [L : K], \tag{3.9}$$

analogous to (1.7). In light of the short exact sequence (3.4) and the obvious identification $f(L/K) = |\mathrm{Gal}(\kappa_L/\kappa_K)|$, this will give us an identification $e(L/K) = |I(L/K)|$. We now recall the following basic definitions.

Definition 3.11. Let L/K be a finite Galois extension of p-adic fields then we define the following.

(1) We say the extension L/K is unramified if $e(L/K) = 1$ (equivalently $f(L/K) = [L : K]$ by 3.9) or equivalently if the natural map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(\kappa_L/\kappa_K)$ appearing in (3.4) is an isomorphism.

(2) We say the extension L/K is totally ramified if $f(L/K) = 1$ (equivalently $e(L/K) = [L : K]$ by 3.9) or equivalently if the natural map $I(L/K) \xrightarrow{\simeq} \mathrm{Gal}(L/K)$ appearing in (3.4) is an isomorphism.

We note that we always have the following consequence of the above discussion, by combining (3.4) with Galois theory.

Corollary 3.12. *For any finite extension L/K there exists a factorization*

$$K \subset M \subset L$$

where M/K is unramified and L/M is totally ramified. We have natural isomorphisms

$$\mathrm{Gal}(M/L) \simeq I(L/K) \tag{3.10}$$

and

$$\mathrm{Gal}(K/M) \simeq \mathrm{Gal}(\kappa_L/\kappa_K) \tag{3.11}$$

Remark 3.13. We refer to $K \subset M$ as the maximal unramified subextension. We note that if we have two extensions $K \subset M$ and $K \subset L$ such that M/K is unramified and L/K is totally ramified then they must be disjoint from one another in the sense that, if ML/K denotes the compositum of the extension in the algebraic closure $\overline{K}$, then we have that the intersection of L/K and M/K inside ML is just K. Indeed, suppose the intersection $K \subset K' \subset M, L$ was non-trivial. Then we would have exhibited an unramified subextension $K \subset K' \subset L$, which, by the relationship $e(L/K) = e(K'/K)e(L/K')$, would contradict the fact that L/K is totally ramified.

In particular, we see that we can view $I(L/K)$ and the filtration by the subgroups $I_n(L/K)$ as capturing refined information about the totally ramified extensions of p-adic fields, which is why they are called the ramification subgroups. We also see that the structure of the Galois group of the unramified extensions mirrors that of extensions of finite fields. In particular, this relationship is tight.

Theorem 3.14. *The natural mapping*

$$\{L/K \text{ finite unramified extension } \} \to \{\kappa/\kappa_K \text{ a finite extension}\}$$

$$L \mapsto \kappa_L$$

is bijective.

Proof. See [Mil20b, Proposition 7.50]. The key point is that we may lift any minimal polynomial for the extension κ_L/κ_K using Hensel's lemma to get a minimal polynomial defining an unramified extension with the desired properties. □

Now that we have the basic structural results on the Galois groups of local fields we may proceed with realizing our Goal 3.8. We begin with case of an unramified extension of fields L/K, which was essentially discussed already in Exercise 2.109.

3.2.2. *Unramified Extensions.* We now proceed with the verification of Goal 3.8 for an unramified extension L/K of p-adic fields. For the particular extensions $\mathbb{Q}_{q^g}/\mathbb{Q}_q$ this was essentially seen already in Exercise 2.109. As seen there, a key was the short exact sequence of $\mathrm{Gal}(L/K)$-modules.

$$0 \to \mathcal{O}_{K^*} \to L^* \to \mathbb{Z} \to 0, \tag{3.12}$$

where the last map is the valuation and $\mathbb{Z}$ is equipped with the trivial $\mathrm{Gal}(L/K)$-action. We note that this is a $\mathrm{Gal}(L/K)$-equivariant map, since the valuation on a local field is invariant under the action of the Galois group, by virtue of the formula (3.2) and the fact that the norm map is invariant under the action of the Galois group.

We now have the following special case of Goal 3.8.

Theorem 3.15. *Let L/K be an unramified extension of local fields L/K then we have that*

$$H^2(\mathrm{Gal}(L/K), L^*) \simeq \mathbb{Z}/[L:K]\mathbb{Z}.$$

Proof. The key point is the following, which for the extension $\mathbb{Q}_{q^g}/\mathbb{Q}_q$ follows from Exercise 2.109 (1),(3),(4), and the argument in general is the same.

Lemma 3.16. *For L/K an unramified extension, the norm map $\mathrm{Nm}_{L/K} : L^* \to K^*$ induces a surjective map $\mathcal{O}_{L^*} \to \mathcal{O}_{K^*}$ on the ring of integers.*

In particular, from this we deduce the following corollary.

Corollary 3.17. *For L/K an unramified extension, the Tate cohomology $H^i_T(\mathrm{Gal}(L/K), \mathcal{O}_L^*)$ vanishes for all $i \in \mathbb{Z}$.*

Proof. Since the group $\mathrm{Gal}(L/K)$ is cyclic as in Definition 3.11 (1), it follows by Theorem 2.106 that we only need to check this claim for $i = 0, 1$. The claim that $H^0_T(\mathrm{Gal}(L/K), \mathcal{O}_L^*) = 0$ is an immediate consequence of Lemma 3.16. For $H^1_T(\mathrm{Gal}(L/K), \mathcal{O}_L^*) = H^1(\mathrm{Gal}(L/K), \mathcal{O}_{L^*})$, we note that the short exact sequence (3.12) is split in the case of an unramified extension. Indeed the uniformizing element $\pi_L = \pi_K$ is an element of K and so is fixed by the Galois group. In particular, we deduce that we have an isomorphism:

$$H^i_T(\mathrm{Gal}(L/K), L^*) \simeq H^i_T(\mathrm{Gal}(L/K), \mathcal{O}_L^*) \oplus H^i_T(\mathrm{Gal}(L/K), \mathbb{Z}) \tag{3.13}$$

for all $i \in \mathbb{Z}$. This implies that $H^1(\mathrm{Gal}(L/K), \mathcal{O}_{L^*})$ is a direct summand of $H^1(\mathrm{Gal}(L/K), L^*)$, which vanishes by Theorem 2.50. □

Now we note that we have the following consequence of (3.13) for $i = 2$.

$$H^2(\mathrm{Gal}(L/K), L^*) = H^2(\mathrm{Gal}(L/K), \mathcal{O}_{L^*}) \oplus H^2(\mathrm{Gal}(L/K), \mathbb{Z}) = H^2(\mathrm{Gal}(L/K), \mathbb{Z}),$$

where we have used Corollary 3.17. Then we conclude using Theorem 2.106 that

$$H^2(\mathrm{Gal}(L/K), \mathbb{Z}) \simeq H^0_T(\mathrm{Gal}(L/K), \mathbb{Z}) \simeq \mathbb{Z}/[L:K]\mathbb{Z}.$$

□

Remark 3.18. We note if K_n/K denotes the unique unramified extension of degree n guaranteed by Theorem 3.14, we have that $H^2(\mathrm{Gal}(K_n/K), K_n^*) \simeq \mathbb{Z}/n\mathbb{Z}$ by Theorem 3.15. Moreover, by Tate-periodicity, we have that this is isomorphic to $K^*/\mathrm{Nm}_{K_n/K}(K_n^*)$. Using the identification $K^* \simeq \mathcal{O}_K^* \times \mathbb{Z}$ given by the split (as $\mathrm{Gal}(K_n/K)$-modules) short exact sequence (3.12) for K_n^* and K^* together with Lemma 3.16 (as in 2.109), we may deduce that we may explicitly describe the norm subgroup $\mathrm{Nm}_{K_n/K}(K_n^*) \subset K^*$ as the subgroup $n\mathbb{Z} \times \mathcal{O}_K^* \subset \mathbb{Z} \times \mathcal{O}_{K^*} \simeq K^*$. In particular, we note that $K^*/\mathrm{Nm}_{K_n/K}(K_n^*)$ is generated by π_K.

Remark 3.19. We note that these identifications have the following compatability as we vary the extension. For an unramified extension L/K, we note that we have a natural map

$$H^2(\mathrm{Gal}(L/K), L^*) \simeq \mathbb{Z}/[L:K]\mathbb{Z} \simeq [L:K]\mathbb{Z}/\mathbb{Z} \hookrightarrow \mathbb{Q}/\mathbb{Z}.$$

We refer to this

$$\mathrm{inv}_{L/K} : H^2(\mathrm{Gal}(L/K), L^*) \to \mathbb{Q}/\mathbb{Z} \tag{3.14}$$

as the invariant map. If we have an unramified subextension $K \subset M \subset L$, we also have the natural inflation map

$$H^2(\mathrm{Gal}(L/K), L^*) \to H^2(\mathrm{Gal}(M/K), M^*).$$

This sits in a commutative diagram

$$\begin{array}{ccc} H^2(\mathrm{Gal}(L/K), L^*) & \xrightarrow{\mathrm{inv}_{L/K}} & \mathbb{Q}/\mathbb{Z} \\ \downarrow & & \downarrow \mathrm{id} \\ H^2(\mathrm{Gal}(M/K), M^*) & \xrightarrow{\mathrm{inv}_{M/K}} & \mathbb{Q}/\mathbb{Z} \end{array} \tag{3.15}$$

Indeed, we may see this by reinterpreting $\mathrm{inv}_{L/K}$ as follows. We have a natural isomorphism

$$H^2(\mathrm{Gal}(L/K), L^*) \simeq H^0_T(\mathrm{Gal}(L/K), L^*) \simeq H^0_T(\mathrm{Gal}(L/K), \mathbb{Z})$$

induced by fixing a generator $u_{L/K}$ of $H^2(\mathrm{Gal}(L/K), L^*)$. Now we look at the short exact sequence,

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

and invoke Lemma 2.74 to see that the boundary map in the long exact sequence induces an isomorphism

$$H^0_T(\mathrm{Gal}(L/K), \mathbb{Z}) \simeq H^1(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}),$$

where the last identification is as in 2.47. We now note that we have a canonical map $\mathrm{Gal}(L/K) \to \mathbb{Q}/\mathbb{Z}$ given by evaluating on the Frobenius. In particular, the resulting map

$$H^2(\mathrm{Gal}(L/K), L^*) \to \mathbb{Q}/\mathbb{Z}$$

is $\mathrm{inv}_{L/K}$. Tracing through the identifications, this allows us to see the commutativity of the diagram (3.15) follows from the fact that the surjection $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$ sends the Frobenius to the Frobenius. If we now consider the maximal unramified extension $K \subset K^{\mathrm{un}} \subset \overline{K}$ (i.e the compositum of all unramified extensions of K in $\overline{K}$) then we note this is an object in the category $\mathrm{Mod}_{\mathrm{Gal}(K^{\mathrm{un}}/K),\mathrm{cont}}$. We may form the cohomology

$$H^2(\mathrm{Gal}(K^{\mathrm{un}}/K), K^{\mathrm{un},*}),$$

which, by Corollary 2.80, is a direct limit of $H^2(\mathrm{Gal}(L/K), L^*)$ for L/K finite unramified over the inflation maps. Therefore, we obtain a map

$$\mathrm{inv} : H^2(\mathrm{Gal}(K^{\mathrm{un}}/K), K^{\mathrm{un},*}) \xrightarrow{\simeq} \mathbb{Q}/\mathbb{Z} \tag{3.16}$$

which will now be an isomorphism by virtue of the fact that $\mathbb{Q}/\mathbb{Z}$ is a direct limit over its finite torsion subgroups.

We now turn to the next level of generality

3.2.3. *The Cyclic Case.* We now consider a not necessarily unramified cyclic extension L/K. In this case, we will have to modify our approach slightly. Indeed, we note that the analogue of Lemma 3.16 does not hold in this case (Recall that $\sqrt{p}$ is a uniformizer in $\mathbb{Q}_p(\sqrt{p})$ so that this extension is ramified, as in (3.7)) .

Exercise 3.20. *Let $L = \mathbb{Q}_p(\sqrt{p})$ and $K = \mathbb{Q}_p$. Show the following.*

1. *The natural map*
$$\mathrm{Nm}_{L/K} : L^* \to K^*$$
induces an isomorphism $L^*/\mathcal{O}_L^* \simeq K^*/\mathcal{O}_K^*$.
2. *Compute the cohomology groups $H^i_T(\mathrm{Gal}(L/K), \mathcal{O}_L^*)$ for all $i \in \mathbb{Z}$. Show that $H^0_T(\mathrm{Gal}(L/K), \mathcal{O}_K^*) \neq 0$.*

In particular, we will need some replacement for Lemma 3.16. The idea will be to first consider the additive case and then use the p-adic exponential map to move to the multiplicative case.

Lemma 3.21. *Let L/K be a Galois extension of local fields then there is an open subgroup $U \subset \mathcal{O}_L$ of the ring of integers which satisfies the following.*

(1) U is stable under the action of $\mathrm{Gal}(L/K)$.
(2) We have that the cohomology $H^i(\mathrm{Gal}(L/K), U)$ *vanishes for all* $i > 0$.

Moreover, we may assume that, for all $x \in U$, *the valuations* $v_L(-) : L \to \mathbb{Z}$ *of all elements in* U *are larger than* m, *for any* $m \in \mathbb{Z}$.

Proof. By the normal basis theorem, we may find $\alpha \in L$ such that the $\mathrm{Gal}(L/K)$-translates of α generated L as a K-vector space. We may rescale α to assume that α is in $\mathcal{O}_L^*$. We then consider the subgroup U of $\mathcal{O}_L$ generated by the translates of α under $\mathrm{Gal}(L/K)$ under the scaling action of $\mathcal{O}_K$. We note that, as a $\mathrm{Gal}(L/K)$-module, we have that $U \simeq \mathrm{Ind}_1^{\mathrm{Gal}(L/K)}(\mathcal{O}_K)$. In particular, by Schapiro's Lemma, it satisfies the desired property (cf. Exercise 2.52). To guarantee the condition on the p-adic valuations, we note that it simply suffices to show the desired condition for α since the valuation is Galois equivariant, which may be rearranged after further rescaling. □

We now deduce the analogous result in the multiplicative case.

Lemma 3.22. *Let* L/K *be a Galois extension of local fields then there is an open finite index subgroup* $V \subset \mathcal{O}_L^*$ *of the ring of integers which satisfies the following.*

(1) V is stable under the action of $\mathrm{Gal}(L/K)$.
(2) We have that the cohomology $H^i(\mathrm{Gal}(L/K), V)$ *vanishes for all* $i > 0$.

Proof. We consider the formal power series

$$\exp(x) := \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

By choosing the subgroup $U \subset \mathcal{O}_L$ of Lemma 3.21 to have sufficiently large valuations, we may arrange that this power series converges p-adically (Use that $v_p(n!) = \sum_{k=0}^{\infty} \lfloor \frac{n}{p^k} \rfloor$), and it will define a topological isomorphism of U onto a subgroup of $V \subset \mathcal{O}_{L^*}$ (as it has an inverse given by the logarithm map), which will be equivariant for $\mathrm{Gal}(L/K)$. In particular, we have isomorphisms

$$H^i(\mathrm{Gal}(L/K), U) \simeq H^i(\mathrm{Gal}(L/K), V),$$

from which the claim follows. □

Using similar logic to the prove of Lemma 3.22, we can deduce the following which will be useful for the proof of the local existence Theorem (Theorem 3.2).

Exercise 3.23. *Suppose* $K/\mathbb{Q}_p$ *is a finite extension. Show that the intersection* $\cap_{n \geq 1}(K^*)^n$ *is trivial (Hint: reduce to checking it for a open finite index subgroup* $V \subset \mathcal{O}_L^*$ *and then argue as in the proof of Lemma 3.22).*

We now deduce the following partial realization of Goal 3.8, using the theory of the Herbrand quotient introduced in Definition 2.111.

Theorem 3.24. *For* L/K *a cyclic extension of p-adic fields, we have that*

$$|H_T^0(\mathrm{Gal}(L/K), L^*)| = |H^2(\mathrm{Gal}(L/K, L^*)|$$

is of cardinality $[L : K]$.

Proof. We note, by Example 2.112 and 2.113 (1) applied to the short exact sequence (2.42) we have an equality

$$h(L^*) = h(\mathbb{Z})h(\mathcal{O}_L^*).$$

However, we note that $V \subset \mathcal{O}_L^*$ is open so it has finite index. In particular, by Proposition 2.113 (1)-(2), we have an equality

$$h(V) = h(\mathcal{O}_L^*),$$

where we note, by Tate-Periodicity and Lemma 3.22 (2), we have that $h(V) = 1$. In summary, we have deduced that

$$h(L^*) = h(\mathbb{Z}) = [L : K],$$

where the last equality follows from Example 2.112. However, by Hilbert 90 (Theorem 2.50) and Tate-periodicity again, this now implies that we have

$$|H^0_T(\mathrm{Gal}(L/K), L^*) = [L : K],$$

as desired. □

In order to push this claim forward, we will need to exploit a particular property of the Galois groups of a finite extension of p-adic fields; namely, that they are always solvable, as explained in Proposition 3.10.

3.2.4. *General Extensions.* We now have the following extension/weakening of Theorem 3.24 to general extensions.

Theorem 3.25. *For any finite Galois extension L/K, we have an inequality*

$$|H^2(\mathrm{Gal}(L/K), L^*)| \leq [L : K].$$

Proof. The case of L/K cyclic was checked in Theorem 3.24. To reduce to the case, we induct on the number of normal subgroups of $\mathrm{Gal}(L/K)$. In particular, by Corollary 2.108, either $\mathrm{Gal}(L/K)$ is cyclic and we are done, or we may choose a non-trivial finite cyclic subextension L/M. To proceed further, we then apply the inflation and restriction exact sequence Proposition 2.118 to the subgroup $\mathrm{Gal}(L/M) \subset \mathrm{Gal}(L/K)$. In particular, by combining with Hilbert 90 (Theorem 2.50), this tells us that we have a left exact sequence

$$0 \to H^2(\mathrm{Gal}(M/K), M^*) \to H^2(\mathrm{Gal}(L/K), L^*) \to H^2(\mathrm{Gal}(L/M), L^*)$$

However, this gives us an inequality

$$|H^2(\mathrm{Gal}(L/K), L^*)| \leq |H^2(\mathrm{Gal}(M/K), M^*)||H^2(\mathrm{Gal}(L/M), L^*)| = [M : K][L : M] = [L : K],$$

where we have used our inductive hypothesis to conclude the equality. □

Now, in light of Theorem 3.24, all that remains to do is exhibit a cyclic subgroup of $H^2(\mathrm{Gal}(L/K), L^*)$ of order $[L : K]$ to achieve Goal 3.8. We will do this by comparing to the case of unramified extensions, where we saw this already in Theorem 3.15 and Exercise 2.109.

Proposition 3.26. *Let L/K be a finite Galois extension of local fields and let M/K be an unramified extension of degree $[L : K]$. We write ML for the compositum of the two fields over K, which is also a finite Galois extension (since L/K and M/K are both finite Galois) with quotients $\mathrm{Gal}(ML/K) \to \mathrm{Gal}(L/K), \mathrm{Gal}(M/K)$. We consider the inflation maps*

$$H^2(\mathrm{Gal}(L/K), L^*) \to H^2(\mathrm{Gal}(ML/K), (ML)^*) \tag{3.17}$$

and

$$H^2(\mathrm{Gal}(M/K), M^*) \to H^2(\mathrm{Gal}(ML/K), (ML)^*). \tag{3.18}$$

However, now the image of (3.17) contains the image of (3.18).

Proof. We consider the diagram
(3.19)

$$\begin{array}{ccccccc} & & & & 0 & & \\ & & & & \downarrow & & \\ & & & & H^2(\mathrm{Gal}(M/K), M^*) & & \\ & & & & \downarrow{\scriptstyle (3.18)} & \searrow & \\ 0 & \longrightarrow & H^2(\mathrm{Gal}(L/K), L^*) & \xrightarrow{(3.17)} & H^2(\mathrm{Gal}(ML/K), (ML)^*) & \longrightarrow & H^2(\mathrm{Gal}(ML/L), (ML)^*), \end{array}$$

where the claimed exactness properties follow from combining (2.118) with Theorem (2.50). By these exactness properties, it suffices to show the diagonal arrow is the zero map, as this will imply the existence of an injective map $H^2(\mathrm{Gal}(M/K), M^*) \to H^2(\mathrm{Gal}(L/K), L^*)$. In order to do this, we let $K \subset U \subset L$ be the maximal unramified subextension of L/K, as in Remark 3.13. We note that we have an inclusion $U \subset M$ since $[U : K] | [M : K]$ by Theorem 3.14. Using the obvious functorality of inflation maps, we may extend (3.19) to a commutative diagram
(3.20)

$$\begin{array}{ccccccc} & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & H^2(\mathrm{Gal}(U/K), U^*) & \longrightarrow & H^2(\mathrm{Gal}(M/K), M^*) & \longrightarrow & H^2(\mathrm{Gal}(M/U), U^*) \\ & & \downarrow & & \downarrow{\scriptstyle (3.18)} & \searrow & \\ 0 & \longrightarrow & H^2(\mathrm{Gal}(L/K), L^*) & \xrightarrow{(3.17)} & H^2(\mathrm{Gal}(ML/K), (ML)^*)] & \longrightarrow & H^2(\mathrm{Gal}(ML/L), (ML)^*), \\ & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & H^2(\mathrm{Gal}(L/U), L^*) & \longrightarrow & H^2(\mathrm{Gal}(ML/M), (ML)^*) & \longrightarrow & H^2(\mathrm{Gal}(ML/L), L^*) \end{array}$$

where exactness of the maps again follows by Theorem 2.50 and Proposition 2.118. In particular, by passing to the quotient of $H^2(\mathrm{Gal}(M/K), M^*)$ (resp. $H^2(\mathrm{Gal}(L/K), L^*)$) by $H^2(\mathrm{Gal}(U/K), U^*)$ and using the exactness properties of the diagram, we see that it suffices to show that $H^2(\mathrm{Gal}(L/U), L^*) \to H^2(\mathrm{Gal}(ML/U), (ML)^*)$ admits an injection from $H^2(\mathrm{Gal}(M/K), M^*)/H^2(\mathrm{Gal}(U/K), U^*) \hookrightarrow H^2(\mathrm{Gal}(M/U), U^*)$. However, this reduces us to showing that the natural map $H^2(\mathrm{Gal}(M/U), U^*) \hookrightarrow H^2(\mathrm{Gal}(ML/M), (ML)^*)$ factors through $H^2(\mathrm{Gal}(L/U), L^*) \to H^2(\mathrm{Gal}(ML/U), (ML)^*)$. In other words, we may replace K by U, and assume without loss of generality that L/K is a totally ramified extension in the sense of Definition 3.11 (2). In particular, by Remark 3.13, this implies that we may assume that L/K and M/K are disjoint extensions. From here, we deduce that $L \cap M = K$ and that the restriction map

$$\mathrm{Gal}(ML/L) \xrightarrow{\simeq} \mathrm{Gal}(M/M \cap L) = \mathrm{Gal}(M/K)$$

is an isomorphism, where $\mathrm{Gal}(M/K)$ and in turn $\mathrm{Gal}(ML/L)$ is cyclic, by Theorem 3.15. Moreover, ML/L will be unramified as it the compositum of an unramified extension M/K with L. In particular, the natural map $M^* \to (ML)^*$ is an map of Galois modules with respect to this isomorphism, and thus we obtain a natural map

$$H^2(\mathrm{Gal}(M/K), M^*) \to H^2(\mathrm{Gal}(ML/L), (ML)^*) \tag{3.21}$$

which is the one we want to show is zero. However, the groups appearing here are both cyclic so we may apply Tate periodicity (Theorem 2.106) to replace (3.21) with the map

$$K^*/\mathrm{Nm}_{M/K}(M^*) \to L^*/\mathrm{Nm}_{ML/L}((ML)^*).$$

However, the target of this map is a cyclic group of order $[L:K]$ generated by π_K (Remark 3.18) and the source is again a cyclic group of order $[L:K]$ by the above discussion. Therefore, it suffices to show the image of π_K is zero. However, since L/K is totally ramified $\pi_K = \pi_L^{[L:K]}$ up to a unit of $\mathcal{O}_L$ as in (3.7) and therefore it is indeed zero, as desired. □

This indeed implies the claim we want, allowing us to finally accomplish Goal 3.8.

Corollary 3.27. *For L/K a finite Galois extension of p-adic fields, we have an isomorphism*

$$\mathbb{Z}/[L:K]\mathbb{Z} \simeq H^2(\mathrm{Gal}(L/K), L^*).$$

Proof. As explained above, by Theorem 3.25, it suffices to exhibit a cyclic subgroup of order $[L:K]$ in $H^2(\mathrm{Gal}(L/K), L^*)$. We consider the situation of Proposition 3.26. By combining Proposition 2.118 with Hilbert Theorem 90 (Theorem 2.50), we deduce the inflation maps

$$H^2(\mathrm{Gal}(L/K), L^*) \xrightarrow{(3.17)} H^2(\mathrm{Gal}(ML/K), (ML)^*)$$

and

$$H^2(\mathrm{Gal}(M/K), M^*) \xrightarrow{(3.18)} H^2(\mathrm{Gal}(ML/K), (ML)^*).$$

are injective, as in (3.19). However, now the desired claim easily follows by applying Theorem 3.15 to deduce that $H^2(\mathrm{Gal}(M/K), M^*) \simeq \mathbb{Z}/[L:K]\mathbb{Z}$ together with Proposition 3.26. □

In particular, by Theorem 3.9, this allows us to (finally) proudly proclaim the following result.

Theorem 3.28. *Assume L/K is a finite Galois extension of p-adic fields, then we have an isomorphism*

$$\mathrm{Gal}(L^{\mathrm{ab}}/K) = \mathrm{Gal}(L/K)^{\mathrm{ab}} \simeq H_T^{-2}(\mathrm{Gal}(L/K), \mathbb{Z}) \xrightarrow{\simeq} H_T^0(\mathrm{Gal}(L/K), L^*) \simeq K^*/\mathrm{Nm}_{L/K}(L^*),$$

induced by cupping with a generator $\langle u_{L/K}\rangle \simeq \mathbb{Z}/[L:K]\mathbb{Z} \simeq H^2(\mathrm{Gal}(L/K), L^*)$ given by Corollary 3.27.

Remark 3.29. We let $K \subset K^{\mathrm{un}} \subset \overline{K}$ be the maximal unramified extension. We view $\overline{K}^*$ as an object in $\mathrm{Mod}_{\mathrm{Gal}(\overline{K}/K),\mathrm{cont}}$ and view $K^{\mathrm{un},*}$ as an object in $\mathrm{Mod}_{\mathrm{Gal}(\overline{K}/K),\mathrm{cont}}$ via the restriction map $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(K^{\mathrm{un}}/K)$. The natural inclusion $K^{\mathrm{un},*} \hookrightarrow \overline{K}^*$ induces a natural map

$$H^2(\mathrm{Gal}(\overline{K}/K), K^{\mathrm{un},*}) \to H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^*), \tag{3.22}$$

by the construction described in 2.3.2. By 3.16, the former also identifies with $\mathbb{Q}/\mathbb{Z}$ by virtue of the invariant map $\mathrm{inv}_{L/K} : H^2(\mathrm{Gal}(L/K), L^*) \to \mathbb{Q}/\mathbb{Z}$ introduced for an unramified extension in (3.14). Using Theorem 3.28, we may construct a map

$$\mathrm{inv}_{L/K} : H^2(\mathrm{Gal}(L/K), L^*) \to \mathbb{Q}/\mathbb{Z} \tag{3.23}$$

after fixing a generator $u_{L/K} \in H^2(\mathrm{Gal}(L/K), L^*)$, by the exact same reasoning. It will also satisfy the obvious functoralities with respect to inflation, as in (3.15). By applying 2.80, we get a map

$$\mathrm{inv} : H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^*) \to \mathbb{Q}/\mathbb{Z} \tag{3.24}$$

and we claim that it is an isomorphism. However, one easily sees that the composition

$$H^2(\mathrm{Gal}(\overline{K}/K), K^{\mathrm{un},*}) \to H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^*) \xrightarrow{\mathrm{inv}} \mathbb{Q}/\mathbb{Z},$$

is the isomorphism (3.16) and that the first map is injective by the proof of Proposition 3.26, which implies that the map (3.23) is an isomorphism. In particular, by combining with (2.29) we deduce the following.

Corollary 3.30. *Let $K/\mathbb{Q}_p$ be a p-adic field. Then we have an isomorphism*

$$\mathrm{Br}(K) \simeq \mathbb{Q}/\mathbb{Z},$$

where $\mathrm{Br}(K)$ denotes the local Brauer group.

In particular, we are now ready to deduce all the main Theorems of local class field theory from this result.

3.3. **Clean Up.** We begin with the proof of the Norm limitation Theorem.

Proof. (Theorem 3.6) We first consider a Galois extension L/K and let $K \subset M \subset L$ be the maximal abelian subextension. However, by applying Theorem 3.28, we deduce that we have an isomorphism

$$\mathrm{Gal}(L/K)^{\mathrm{ab}} \simeq \mathrm{Gal}(M/K) \xrightarrow{\simeq} K^*/\mathrm{Nm}_{L/K}(L^*)$$

and an isomorphism

$$\mathrm{Gal}(M/K) \xrightarrow{\simeq} K^*/\mathrm{Nm}_{M/K}(M^*).$$

However, this forces the obvious containment $\mathrm{Nm}_{L/K}(L^*) \subset \mathrm{Nm}_{M/K}(M^*)$, as described in Remark 3.7 to be an equality, since they are both subgroups of the same index in K^*.

We now consider the case of a general extension L/K, we again have an obvious inclusion $\mathrm{Nm}_{L/K}(L^*) \subset \mathrm{Nm}_{M/K}(M^*)$. To check the reverse inclusion, we replace L by its Galois closure $K \subset M \subset L \subset L^{\mathrm{Gal}}$ and then use the obvious containment

$$\mathrm{Nm}_{L^{\mathrm{Gal}}/K}((L^{\mathrm{Gal}})^*) \subset \mathrm{Nm}_{L/K}(L^*)$$

to reduce to the previous case. □

We now want to turn to the proof of Theorem 3.1.

Proof. (Theorem 3.1) We see that at least that part (2) is essentially covered by our key Theorem 3.28. In particular, we have produced an isomorphism

$$\phi_{L/K} : K^*/\mathrm{Nm}_{L/K}(L^*) \xrightarrow{\simeq} \mathrm{Gal}(L/K).$$

for all finite abelian extensions L/K, and it is fairly easy to check that this will carry the uniformizing element to Frobenius. However, in order to get the map $\phi_K : K^* \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ with the desired properties. We need to show that these maps "patch together" in an appropriate way as we vary the extension. We will do this using the following Lemma.

Lemma 3.31. *For G a finite abelian, the cup product of 2.116*

$$H_T^{-2}(G, \mathbb{Z}) \times H_T^2(G, \mathbb{Z}) \to H_T^0(G, \mathbb{Z})$$

induces a perfect pairing (In the sense that something on either side which pairs to give 0 *with the other side is already* 0*).*

Proof. We note that we have identifications

$$H_T^{-2}(G, \mathbb{Z}) \simeq G$$

by Exercise 2.101 (4) and

$$H_T^0(G, \mathbb{Z}) \simeq \mathbb{Z}/|G|\mathbb{Z}$$

as in Example 2.112. Moreover, we claim that we have an identification

$$H_T^2(G, \mathbb{Z}) \simeq \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}).$$

To see this, we use the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

of G-modules equipped with the trivial G-action. However, $\mathbb{Q}$ is acyclic by Lemma 2.74. This implies that the boundary map in the long exact cohomology sequence of Tate-cohomology then induces the desired identification.

Now, using the above identifications, one can check that the cup product on Tate-cohomology identifies with the obvious pairing

$$G \times \mathbb{Z}/|G|\mathbb{Z} \to \mathrm{Hom}(G, \mathbb{Z}/|G|\mathbb{Z}) \to \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}),$$

given by evaluating a map $\mathrm{Hom}(G, \mathbb{Z}/|G|\mathbb{Z})$ on elements of G. This is easily checked to be perfect. □

In particular, we may now combine 3.31 together with the isomorphism

$$H_T^{-2}(\mathrm{Gal}(L/K), \mathbb{Z}) \to H_T^0(\mathrm{Gal}(L/K), L^*)$$

of Theorem 3.28, which we recall is also induced by cup product, to deduce that the cup product map

$$H_T^0(\mathrm{Gal}(L/K), L^*) \times H_T^2(\mathrm{Gal}(L/K), \mathbb{Z}) \to H^2(\mathrm{Gal}(L/K), L^*) \tag{3.25}$$

is a perfect pairing. We now massage this even further. In particular, after fixing generators $u_{L/K}$ of $H^2(\mathrm{Gal}(L/K), L^*)$, we may define invariant maps (3.23) $H^2(\mathrm{Gal}(L/K), L^*) \to \mathbb{Q}/\mathbb{Z}$, which then gives us a perfect pairing

$$H_T^0(\mathrm{Gal}(L/K), L^*) \times H_T^2(\mathrm{Gal}(L/K), \mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}.$$

Moreover, we see that the fact that this pairing is perfect completely encodes the reciprocity map indeed the inverse of the cup map with a class in $H_T^2(\mathrm{Gal}(L/K), \mathbb{Z})$ induces the desired isomorphism

$$\phi_{L/K} : K^*/\mathrm{Nm}_{L/K}(L^*) \simeq H_T^0(\mathrm{Gal}(L/K), L^*) \to H_T^{-2}(\mathrm{Gal}(L/K), \mathbb{Z}) \simeq \mathrm{Gal}(L/K).$$

However, as we now want to take limits over L/K it is better that we pass to a statement that just involves cohomology and not homology/Tate cohomology (cf. Remark 2.78). In particular, precomposing with the natural map $H^0(\mathrm{Gal}(L/K), L^*) \to H_T^0(\mathrm{Gal}(L/K), L^*)$, we obtain a natural map

$$H^0(\mathrm{Gal}(L/K), L^*) \times H^2(\mathrm{Gal}(L/K), \mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}, \tag{3.26}$$

which only involves cohomology. In particular, to construct the map

$$\phi_K : K^* \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

of Theorem 3.1 (1), we just need to see that this pairing is compatible with varying the extension. We recall that the cup product is compatible with the restriction map induced by $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$, by Proposition 2.117 (2), and we know that the same is true for the invariant map, as explained in Remark 3.29. This gives us the claim. □

All that is left to do now is show the local Existence Theorem. We start with the following.

Proposition 3.32. *Let $K/\mathbb{Q}_p$ be a p-adic field. Then the intersection of all of the norm groups $\mathrm{Nm}_{L/K}(L^*)$ for all finite extensions L/K is trivial.*

Proof. We let D_K denote the intersection of all the norm groups. We note that this is contained in $D_K \subset \mathcal{O}_K^*$. Indeed, for K_n/K the unique unramified extension of $K/\mathbb{Q}_p$ of degree n guaranteed by Theorem 3.14, we note that $\mathrm{Nm}_{K_n/K}(K^*) \simeq n\mathbb{Z} \times \mathcal{O}_{K^*} \subset \mathbb{Z} \times \mathcal{O}_K^* \simeq K^*$, as in Remark 3.18. In particular, the intersection of all of these subgroups is $\mathcal{O}_K^*$. In particular, we deduce that D_K is a compact as a topological group. By Kummer theory, in particular 3.4 (7), we also note that every element of D_K is an ℓth power of an element in K^* for every prime ℓ. We calim that it is actually an ℓth power for an element in D_K, which will in turn allow us to conclude that every element is an nth power of an element in D_K (by looking at the prime factorization of n and iteratively applying the claim on the primes ℓ appearing). In particular, we deduce that $D_K \subset \cap_{n\geq 1}(K^*)^n$, which is trivial by Exercise 3.23.

We first show that for every finite extension, we have that

$$\mathrm{Nm}_{L/K} D_L = D_K \tag{3.27}$$

It is clear that we have an inclusion $\mathrm{Nm}_{L/K} D_L \subset D_K$. For the opposite inclusion, suppose we have $x \in D_K$ then, for any finite extension $K \subset L \subset M$, we can write $x = \mathrm{Nm}_{M/K}(z)$ for some $z \in M^*$. It now suffices to show that that we can choose z such that $y = \mathrm{Nm}_{M/L}(z)$ is equal for

all M. For any fixed M, the set of such y occurring for varying z satisfying $x = \mathrm{Nm}_{M/K}(z)$ is a non-empty compact subset of $\mathcal{O}_L^*$ (as the valuations of the possible y are fixed by the condition $\mathrm{Nm}_{L/K}(y) = x$). In particular, the intersection of all these compact subsets since their pairwise intersection is non-empty, which gives us the desired claim.

Now we need to show that every $x \in D_K$ has an ℓth root. For each finite extension L/K containing a primitive ℓth root of unity let $E(L)$ be the set of ℓth roots of $x \in K$ which belong to $\mathrm{Nm}_{L/K}L^*$. This is non-empty. In particular, by (3.27) paragraph $x = \mathrm{Nm}_{L/K}(y)$ for some $y \in D_L$ by the above logic, and y has an ℓth root $z \in L^*$ by the Kummer theory argument above. Now if we have a finite extension $L \subset M$ we have an inclusion $E(M) \subset E(L)$ again by 3.27. This guarantees that if we look at the set of $E(L)$ for varying L/K it has the property that its pairwise intersection is non-empty, since if we have $E(L)$ and $E(L')$ we have an inclusion $E(LL') \subset E(L) \cap E(L')$. As before, this implies that the intersection of the $E(L)$ over all L/K is non-empty by Lemma 2.14, which implies the desired claim. □

We now have the following weaker version of the norm limitation theorem.

Lemma 3.33. *For every open finite index subgroup $U \subset K^*$, there exists a finite abelian extension L/K such that $\mathrm{Nm}_{L/K}(L^*) \subset U \subset K^*$.*

Proof. By the already established norm limitation theorem 3.6, it suffices to produce a finite extension L/K which is not necessarily abelian such that $\mathrm{Nm}_{L/K}L^* \subset U$. In particular, we have some additional flexibility. We let $n\mathbb{Z} \subset \mathbb{Z}$ be the image of U in the subgroup $K^*/\mathcal{O}_K^* \simeq \mathbb{Z}$ as in (3.12). In particular, if we assume that $K_n \subset L$ contains the maximal unramified extension of degree n we may assume that $\mathrm{Nm}_{L/K}L^*$ is also contained in $n\mathbb{Z}$ by Remark 3.18. By the exactness of (3.12) , we therefore reduce to choosing L such that

$$\mathrm{Nm}_{L/K}L^* \cap \mathcal{O}_K^* \subset U \cap \mathcal{O}_K^*. \tag{3.28}$$

Since $\mathcal{O}_K^*$ is compact we have that subgroup $\mathrm{Nm}_{L/K}L^* \cap \mathcal{O}_K^*$ is open and hence also closed (since $\mathcal{O}_{K^*}$ is profinite, by by Lemma 2.8) and therefore is compact. By Proposition 3.32, we have that the intersection of these compact open subgroups

$$\mathrm{Nm}_{L/K}L^* \cap \mathcal{O}_K^*$$

for varying L/K is also trivial. This in particular implies that the intersection with $\mathcal{O}_K^* \setminus U \cap \mathcal{O}_K^*$ is also trivial. Therefore, by taking L/K sufficiently large, we may arrange that we have the containment (3.28), as desired. □

We may now finally prove the local existence theorem.

Proof. (Theorem 3.2) By Lemma 3.33, we have that we can find a finite abelian extension M/K such that $\mathrm{Nm}_{M/K}M^* \subset U$. However, by the reciprocity isomorphism Theorem 3.1, we have that $\mathrm{Gal}(M/K) \simeq K^*/\mathrm{Nm}_{M/K}M^*$. In particular, if we take L/K to be the fixed field defined by the finite index subgroup $U/\mathrm{Nm}_{M/K}M^*$ this gives us the desired claim. □

We have now finished our discussion of local class field theory. Armed with the knowledged gained here, we now embark on the more treacherous path towards global class field theory.

4. Global Class Field Theory, Reference: [Ked; NSW08; CF10]

As we saw in the proof of local class field theory, a key was using the Theorem of Tate-Nakayam (Theorem 2.121) to reduce the proof of the reciprocity map to showing that the $H^2(\mathrm{Gal}(L/K), L^*)$ for a finite Galois extension L/K was always given by a cyclic group. This is a shadow of a more general formalism that is designed to axiomatize the proofs of global and local class field theory. We start by explaining this axiomatic framework now and then we will apply this to certain groups

attached to number fields known as the ideles. Throughout, we will assume all our fields are perfect (so that the separable and algebraic closure agree).

4.1. **Class Formations and Abstract Class Field Theory.** We first introduce the analogue of the groups L^* for L/K a finite extension, which will allow us to formulate the analogue of Goal 3.8 in the case of local class field theory.

Definition 4.1. Let k be a field with algebraic closure $\overline{k}$. We define the following.

(1) $G := \mathrm{Gal}(\overline{k}/k)$ is the absolute Galois group.
(2) For K/k a subextension, we set $G_K := \mathrm{Gal}(\overline{k}/K)$ to be the closed subgroup of G corresponding to it via Theorem 2.17.
(3) We let $A \in \mathrm{Mod}_{\mathrm{Gal}(\overline{k}/k),\mathrm{cont}}$ be an abelian group with continuous $\mathrm{Gal}(\overline{k}/k)$ action, where we equip A with the multiplcative notation.
(4) We set $A_K := A^{G_K}$, it is equipped with a natural action of the subgroup $\mathrm{Gal}(K/k)$ if K/k is Galois again via Theorem 2.17.

For L/K all finite subextensions of $\overline{k}/k$, we also have the norm map

$$\mathrm{Nm}_{L/K} : A_L \to A_K \qquad a \mapsto \prod_g g.a, \tag{4.1}$$

where g runs over the coset representatives of $\mathrm{Gal}(L/k)/\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(K/k)$ (as in Theorem 2.17) inside G_K. This is precisely the norm map applied to the A_L equipped with its natural $\mathrm{Gal}(L/K) \subset \mathrm{Gal}(L/k)$-module structure. These give rise to the norm subgroups $\mathrm{Nm}_{L/K}A_L \subset A_K$. For an infinite extension L/K, we may similarly define norm subgroups by the formula

$$\mathrm{Nm}_{L/K}A_L := \cap_{M/K}\mathrm{Nm}_{M/K}A_M, \tag{4.2}$$

where M/K is a finite subextension of L/K.

We now have the following analogue of Goal 3.8, where we recall that this goal plus Hilbert 90 allowed us to apply Theorem 2.121.

Definition 4.2. We say that $A \in \mathrm{Mod}_{\mathrm{Gal}(\overline{K}/K),\mathrm{cont}}$ satisfies the class field axiom if for every cyclic extension L/K of finite subextensions of $\overline{k}/k$, we have that

$$|H^0_T(\mathrm{Gal}(L/K), A_L)| = [L : K]$$

and

$$H^{-1}_T(\mathrm{Gal}(L/K), A_L) = 1.$$

The goal is now to combine this axiom with other conditions to construct for each finite Galois extension L/K a map

$$r_{L/K} : \mathrm{Gal}(L/K) \to A_K/\mathrm{Nm}_{L/K}A_L,$$

which will induce an isomorphism after passing to the abelianization of the source. In order to describe this, we will need to encode some ramification theory into our abstract setup. We already saw the required local theory pop up in §3.2.1. In particular, we note that we have a natural map

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(K^{\mathrm{un}}/K) \simeq \hat{\mathbb{Z}},$$

for $K/\mathbb{Q}_p$ a p-adic field, which is the inverse limit of the map appearing in (3.4). Here K^{un}/K is the compositum of all unramified extensions and the isomorphism is given by Theorem 3.14 and Example 2.16. We recall that the Prüfer ring $\hat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$ defined in Example 2.5 (3).

Definition 4.3. With notation as above, we let $d : G \to \hat{\mathbb{Z}}$ be a continuous surjective homomorphism of profinite groups. With respect to this map, we define the following.

(1) We define the Weil group of k, denoted $W_k \subset G$ to be the preimage of $d^{-1}(\mathbb{Z})$. It has the structure of a locally compact group.
(2) We define the inertia group I_k to be the kernel of d. We call the fixed field of I_k as in Theorem 2.17, denoted k^{un}, to be the maximal unramified extension. For any subextension K of $\overline{k}/k$ put $I_K := G_K \cap I_k$ and let $K^{\mathrm{un}} = k^{\mathrm{un}}K$ be the fixed field of I_K
(3) We say a finite extension L/K is unramified if $L \subset K^{\mathrm{un}}$.

Remark 4.4. We note that we have a natural inclusion

$$G_K/I_K \subset G_k/I_k \xrightarrow{d,\simeq} \hat{\mathbb{Z}},$$

and if K/k is finite then this is the inclusion of an open subgroup of $\hat{\mathbb{Z}}$, which one may check is isomorphic to $f_{K/k}\hat{\mathbb{Z}}$ for some $f_{K/k} \in \mathbb{N}_{\geq 0}$. We may renormalize the valuation $d|_{G_K}$ with respect to the finite extension d_K by setting

$$d_K := \frac{1}{f_{K/k}} d|_{G_K}$$

and this gives a surjective continous homomorphism $d_K : G_K \to \hat{\mathbb{Z}}$ with kernel I_K.

As the notation suggests, the indices $f_{K/k}$ appearing in 4.4 should capture ramification of K over k, as in Definition 3.11. In particular, we may define the following.

Definition 4.5. Given a finite extension L/K of subextensions of k, we note that $G_K \subset G_L$ has finite index since L/K is a finite extension. We define the following.

(1) The inertia degree is $f_{L/K} := [d(G_K) : d(G_L)]$,
(2) The ramification degree is $e_{L/K} := [I_K : I_L]$.

These have the following basic properties.

Lemma 4.6. *Let $K \subset L \subset M$ be finite subextensions $\overline{k}/k$. The following is true.*

(1) We have that

$$f_{M/K} = f_{M/L} f_{L/K}.$$

(2) We have that

$$e_{M/K} = e_{M/L} e_{L/K}.$$

(3) If L/K Galois then we have a short exact sequence

$$1 \to I_K/I_L \to \mathrm{Gal}(L/K) \to d(G_K)/d(G_L) \to 0,$$

where $d(G_K)/d(G_L)$ is a finite cyclic group. In particular, L/K is unramified if and only if the second non-zero map is an isomorphism and L/K is ramified if and only if the first non-zero map is an isomorphism.

(4) If L/K is an unramified extension. Then we have an isomorphism

$$\mathrm{Gal}(L/K) \simeq d(G_K)/d(G_L).$$

(5) We have the "fundamental identity"

$$e_{L/K} f_{L/K} = [L : K].$$

Proof. We note that items (1)-(4) follow from the definitions. For (5), we note that it follows from item (3) if L/K is Galois. In general, we may replace L by its Galois closure M, and then apply (1) and (2) with respect to the $L \subset K \subset M$ to deduce the claim in general. □

Remark 4.7. In particular, an extension is unramified if and only if $f_{L/K} = [L : K]$ similarly an extension is totally ramified $e_{L/K} = [L : K]$. If L/K is unramified, we will refer to a generator of $\mathrm{Gal}(L/K)$ for L/K unramified as a Frobenius element. We note by the exact same argument as in Remark 3.13 a tamely ramified and unramified extension will always be disjoint from one another.

In order to get interesting consequences, for A_k satisfying (1), we need to tie A_k with the structure of this valuation in an interesting way. This is accomplished by the following definition.

Definition 4.8. With notation as in 4.1 and 4.3, we say that a Henselian valuation v of A_k with respect to d is a homomorphism $v : A_k \to \hat{\mathbb{Z}}$ satisfying the following.

(1) The group $Z = \mathrm{Im}(v)$ contains $\mathbb{Z}$ and satisfies $Z/nZ \simeq \mathbb{Z}/n\mathbb{Z}$ for all positive integers n.
(2) For every finite extension K/k, we have that $v(\mathrm{Nm}_{K/k}A_K) = f_{K/k}Z$ (We note that since $f_{K/k}$ was defined in terms of d this is where the map d appears).

Remark 4.9. Condition (1) looks a bit bizarre. In particular, one might expect that this is just saying that Z identifies with $\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}}$ or $\hat{\mathbb{Z}}$ itself. However, recall that we have a decomposition $\hat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p$ by the Chinese Remainder Theorem. In particular, we could take the subgroup $\mathbb{Z}$ embedding diagonally, and the subgroup generated by $\mathbb{Z}_p$ on the pth coordinate and 1 elsewhere. This would give an interesting example of a group satisfying (1) that is not one of these two examples.

Given such a Henselian valuation, we define the following.

Definition 4.10. We define the following.

(1) For each finite subextension K/k of $\overline{k}/k$, we obtain a henselian valuation
$$v_K : A_K \to Z$$
by setting
$$v_K = \frac{1}{f_{K/k}}\mathrm{Nm}_{K/k},$$
where we recall that the norm map is defined in 4.1.
(2) For each finite subextension K/k of $\overline{k}/k$, we define the unit subgroup $U_K := \nu_k^{-1}(\{0\})$. Similarly, for infinite extensions we define U_K as the union of these subgroups as we range over finite subextensions.
(3) We say that $\pi \in A_K$ is a uniformizer if $v_K(\pi) = 1$, where we recall this makes sense by the assumption in Definition 4.8 (1) that Z contains $\mathbb{Z}$.

Remark 4.11. Since the Norm map is Galois invariant by definition. We note that we have $v_K(a) = v_{K^g}(g)$ for any $g \in G$. Moreover, for any finite subextension, we have

$$v_L(a) := \frac{1}{f_{L/K}} v_K(\mathrm{Nm}_{L/K}(a)) \tag{4.3}$$

for any $a \in A_L$ (cf. 3.2). In particular, we have that the group of units U_K are $\mathrm{Gal}(K/k)$ sub-module and we have a $\mathrm{Gal}(K/k)$-equivariant short exact sequence

$$0 \to U_K \to A_K \to A_K/U_K \to 0, \tag{4.4}$$

where $A_K/U_K \hookrightarrow Z \hookrightarrow \hat{\mathbb{Z}}$ has the trivial action. In particular, this will play the role of (3.12) in this more abstract setting.

We have already encountered a plethora of examples of this structure.

Exercise 4.12. *Using results already shown in class, explain why the following tuples (k, A, v, d) as in Definition 4.8 and 4.1, satisfy the conditions on the Henselian valuation and the Class Field axiom.*

(1) The tuple:
- *$k/\mathbb{Q}_p$ is a p-adic field.*
- *$A = \overline{k}^*$*
- *$d : \mathrm{Gal}(\overline{k}/k) \to \hat{\mathbb{Z}}$ is the map given by $\mathrm{Gal}(\overline{k}/k) \to \mathrm{Gal}(k^{\mathrm{un}}/k) \simeq \hat{\mathbb{Z}}$ where k^{un}/k is the maximal unramified extension.*

- $v : A_k = k^* \to \hat{\mathbb{Z}}$ *is the map given by the p-adic valuation* v_K.

(2) *The tuple:*
- k *is a finite field.*
- $d : \mathrm{Gal}(\overline{k}/k) \to \hat{\mathbb{Z}}$ *is the isomorphism of Example 2.16.*
- A *is the group* $\mathbb{Z}$ *with its trivial action.*
- $v : A_k = \mathbb{Z} \to \hat{\mathbb{Z}}$ *is the inclusion of* $\mathbb{Z}$ *into its profinite completion.*

We now fix a tuple (k, A, d, v) as in Exercise 4.12 satisfying the class field axiom for the rest of the section. We now have the following analogue of Theorem 3.15 and Corollary 3.17 in this abstract setup.

Theorem 4.13. *Let* L/K *be an unramified extension of finite subextensions of* $\overline{k}/k$. *The following is true.*

(1) *The groups* $H^i_T(\mathrm{Gal}(L/K), U_L) = 0$ *for all* $i \in \mathbb{Z}$.
(2) *The group* $H^0_T(\mathrm{Gal}(L/K), A_L)$ *is cyclic of order* $[L : K]$ *and generated by any uniformizer* π_L *of* L.

Proof. We consider the long exact sequence of Tate cohomology groups attached to (2.42) attached to the subgroup $\mathrm{Gal}(L/K) \subset \mathrm{Gal}(L/k)$. We note that $A_L/U_L \hookrightarrow Z$ has the trivial $\mathrm{Gal}(L/K)$-action.

$$H^0_T(\mathrm{Gal}(L/K), A_L/U_L) \simeq \mathbb{Z}/[L : K]\mathbb{Z}$$

by property 4.8 (2) and the fact that $Z/[L : K]Z \simeq \mathbb{Z}/[L : K]\mathbb{Z}$ together with the assumption that the extension is unramified so that $f_{L/K} = [L : K]$. Similarly, we have that $H^{-1}_T(\mathrm{Gal}(L/K), A_L/U_L) = 0$ by the assumption that $Z \hookrightarrow \hat{\mathbb{Z}}$ and therefore A_L/U_L must be torsion free. In particular, by combining with Tate periodicity (Theorem 2.106) which applies by lemma 4.6 (4) and the unramified assumption, the long exact sequence becomes the following

$$1 = H^{-1}_T(\mathrm{Gal}(L/K), A_L/U_L) \to H^0_T(\mathrm{Gal}(L/K), U_L) \to H^0_T(\mathrm{Gal}(L/K), A_L)$$
$$\to H^0_T(\mathrm{Gal}(L/K), A_L/U_L) \to H^1_T(\mathrm{Gal}(L/K), U_L) \to H^1_T(\mathrm{Gal}(L/K), A_L) = 1$$

By the class field axiom, we have that $H^0_T(\mathrm{Gal}(L/K), A_L) \to H^0_T(\mathrm{Gal}(L/K), A_L/U_L)$ is a map between abelian groups of the same order, and since the target is cyclic it suffices to show that $H^1_T(\mathrm{Gal}(L/K), U_L) = H^1(\mathrm{Gal}(L/K), U_L) = 0$ to prove all the desired claims, again using Tate-periodicity. To do this, we use the assumption that L/K is unramified. In particular, this tells us that the map $A_L \to A_L/U_L$ is split as $\mathrm{Gal}(L/K)$-modules, since a uniformizer of K is also a uniformizer of L. In particular, $H^1(\mathrm{Gal}(L/K), U_L)$ is a direct summand of $H^1(\mathrm{Gal}(L/K), A_L)$, which vanishes by the class field axiom (Definition 4.2) and Tate periodicity. □

We now turn to the construction of the reciprocity map

$$r_{L/K} : \mathrm{Gal}(L/K) \to A_K/\mathrm{Nm}_{L/K}(A_L)$$

for a finite Galois subextension L/K of $\overline{k}/k$. We first give a partial definition of this map. In particular, we recall that under the reciprocity map the uniformizing element should match up with Frobenius. In particular, we can try to construct such a map from the set of Frobenius elements (i.e those coming from lifts of the cyclic groups attached to unramified extensions, as in Lemma 4.6 (3)) to uniformizers as defined in Definition 4.10 (cf. Remark 3.18). In light of Theorem 1.10, we might expect these Frobenius elements to even uniquely pin down the recirpocity map. This is indeed what happens.

Construction 4.14. *Let* L/K *be a Galois extension of finite subextensions of* $\overline{k}/k$. *We let* $\mathrm{Frob}(L/K) \subset \mathrm{Gal}(L/K^{\mathrm{un}})$ *be the semigroup of* $g \in \mathrm{Gal}(L^{\mathrm{un}}/K) \to \mathrm{Gal}(K^{\mathrm{un}}/K) \xrightarrow{d_K} \hat{\mathbb{Z}}$ *such that* $d_K(g)$ *is a positive integer. We define a map*

$$r' : \mathrm{Frob}(L/K) \to A_K/\mathrm{Nm}_{L^{\mathrm{un}}/K}(A_L),$$

as follows. For $g \in \mathrm{Frob}(L/K)$, we let M be the fixed field of g. We consider $\mathrm{Nm}_{M/K}(\pi_M) \in A_K$ for some uniformizer π_M of M and then define $r'(g)$ to be the image in $A_K/\mathrm{Nm}_{L/K}(A_L)$. We recall that $\mathrm{Nm}_{L/K}(A_L)$ is defined as in (4.2).

Remark 4.15. We note that by definition of the extension M/K and the definition of inertial and ramification degree (4.5), we have the following identity

$$f(M/K) = d_K(g).$$

Remark 4.16. We note that $K^{\mathrm{un}}M = M^{\mathrm{un}} \subset L^{\mathrm{un}}$, so in particular, we have a natural surjective map

$$\Gamma := \mathrm{Gal}(L^{\mathrm{un}}/M) \to \mathrm{Gal}(M^{\mathrm{un}}/M) \simeq \hat{\mathbb{Z}} \tag{4.5}$$

of Galois groups. The group Γ however will by Theorem 2.17 identify with the closure of the subgroup of $\mathrm{Gal}(L^{\mathrm{un}}/K)$ generated by the element g. In particular, it is an example of a pro-cylic group, as in Example 2.9. As seen there, Γ^n defines a basis of open normal subgroups of Γ and we have that $|\Gamma/\Gamma^n| \leq n$. On the other hand, the map (4.5) induces a surjection

$$\Gamma/\Gamma^n \to \mathbb{Z}/n\mathbb{Z},$$

which must therefore be an isomorphism. In particular, as a consequence we have that

$$\Gamma = \lim_n \Gamma/\Gamma^n \to \lim_n \mathbb{Z}/n\mathbb{Z} \simeq \hat{\mathbb{Z}}$$

must also be an isomorphism. This in particular forces an equality $M^{\mathrm{un}} = L^{\mathrm{un}}$.

A priori, the construction depends on a choice of uniformizer π_M of M. However, this is precisely where Theorem 4.13 comes to the rescue.

Lemma 4.17. *The construction in 4.14 is well-defined.*

Proof. Suppose we have two uniformizing elements π_M and π'_M of M then $\frac{\pi_M}{\pi'_M}$ lies inside U_M. We now want to show that $\mathrm{Nm}_{M/K}(\frac{\pi_M}{\pi'_M})$ lies in $\mathrm{Nm}_{L^{\mathrm{un}}/K}(A_L)$. However, we note by Theorem 4.13 (1) applied when $i = 0$, that we have an equality $\mathrm{Nm}_{M^{\mathrm{un}}/M}U_{M^{\mathrm{un}}} = U_M$. However, we saw in Remark 4.16, that we have an equality $M^{\mathrm{un}} = L^{\mathrm{un}}$. In particular, this implies that we may rewrite any element in $\mathrm{Nm}_{M/K}U_M$ in terms of an element in $\mathrm{Nm}_{L^{\mathrm{un}}/K}U_{L^{\mathrm{un}}}$, which implies the desired claim. □

Remark 4.18. Suppose that we know that r' is a homomorphism then we may extend it a homomorphism on all of $\mathrm{Gal}(L^{\mathrm{un}}/K)$ by virtue of the fact that either $d_K(g)$ or $d_K(g^{-1})$ is a postive integer. We note that if $g \in H$ actually lies in the subgroup $\mathrm{Gal}(L^{\mathrm{un}}/L)$ then the fixed field M will contain L. In particular, $r'(g) \in \mathrm{Nm}_{M/K}(\pi_M)$ can be rewritten as $\mathrm{Nm}_{L/K}\mathrm{Nm}_{M/L}(\pi_M)$ which implies that if r' were multiplicative it would induce a map

$$r_{L/K} : \mathrm{Gal}(L/K) \simeq \mathrm{Gal}(L^{\mathrm{un}}/K)/\mathrm{Gal}(L^{\mathrm{un}}/L) \to A_K/\mathrm{Nm}_{L^{\mathrm{un}}/K}A_{L^{\mathrm{un}}} \to A_K/\mathrm{Nm}_{L/K}A_L$$

of groups. This will be our candidate for the reciprocity map.

We now want to check that r' is a homomorphism. However, if we just jump straight in from the definition this will become a bit of a nightmare, as we will have to understand how the extension M/K attached to different elements of $g \in \mathrm{Frob}(L/K)$ interact with one another. To deal with this, it is instead convenient to exploit the observation that $M^{\mathrm{un}} = L^{\mathrm{un}}$ made in Remark 4.16 in order to rewrite things in terms of $\mathrm{Nm}_{L^{\mathrm{un}}/K^{\mathrm{un}}}$. To do this, we use the following.

Lemma 4.19. *We fix notation as in Construction 4.14. For fixed $g \in \mathrm{Frob}(L/K)$, we set $n := d_K(g) \in \mathbb{N}_{>0}$. Consider $\phi \in \mathrm{Frob}(L/K)$ such that $d_K(\phi) = 1$ (i.e ϕ is a lift of Frobenius lift along $\mathrm{Gal}(L^{\mathrm{un}}/K) \to \mathrm{Gal}(K^{\mathrm{un}}/K)$) and write $(-)^\phi$ for the action of $\mathrm{Gal}(L^{\mathrm{un}}/K)$ on elements of M inside L^{un}. Then, for all $x \in A_M$, we have an identity*

$$\mathrm{Nm}_{M/K}(x) = \mathrm{Nm}_{L^{\mathrm{un}}/K^{\mathrm{un}}}(xx^{\phi} \cdots x^{\phi^{n-1}}).$$

Proof. Set $F := M \cap K^{\mathrm{un}}$. In particular, by definition of M and Lemma 4.6 (3) and Remark 4.15, we have that F/K is of degree equal to n and $\mathrm{Gal}(F/K)$ is cyclic and generated by ϕ. So, for $y \in A_F$, we have that

$$\mathrm{Nm}_{F/K}(y) = yy^{\phi} \cdots y^{\phi^{n-1}}.$$

Now we combine this with the transitivity of norms to see that

$$\mathrm{Nm}_{M/K}(x) = \mathrm{Nm}_{F/K} \circ \mathrm{Nm}_{M/F}(x) = \mathrm{Nm}_{M/F}(x) \cdots \mathrm{Nm}_{M/F}(x)^{\phi^{n-1}}.$$

However, we note that we have $MK^{\mathrm{un}} = M^{\mathrm{un}} = L^{\mathrm{un}}$ by Remark 4.4 and $K^{\mathrm{un}} \cap M = F$ by definition. In particular, this tells us that $\mathrm{Nm}_{L^{\mathrm{un}}/K^{\mathrm{un}}}((-)|_{A_M}) = \mathrm{Nm}_{M/F}(-)$ in light of the isomorphism $\mathrm{Gal}(L^{\mathrm{un}}/K^{\mathrm{un}}) \simeq \mathrm{Gal}(MK^{\mathrm{un}}/K^{\mathrm{un}}) \xrightarrow{\simeq} \mathrm{Gal}(M/F)$ of Galois groups induced by restricion. □

We consider the following for the finite extension L/K.

$$H_0(\mathrm{Gal}(L^{\mathrm{un}}/K^{\mathrm{un}}), U_{L^{\mathrm{un}}}) = U_{L^{\mathrm{un}}}/I_{\mathrm{Gal}(L^{\mathrm{un}}/K^{\mathrm{un}})},$$

where $I_{\mathrm{Gal}(L^{\mathrm{un}}/K^{\mathrm{un}})}$ is the augmentation subgroup generated by $u^{\tau-1}$ for $u \in U_{L^{\mathrm{un}}}$ and $\tau \in \mathrm{Gal}(L^{\mathrm{un}}/K^{\mathrm{un}})$ (cf. Exercise 2.101 (2)).

We note that the norm map

$$\mathrm{Nm}_{L^{\mathrm{un}}/K^{\mathrm{un}}} : U_{L^{\mathrm{un}}} \to U_{K^{\mathrm{un}}}$$

will factor through the subgroup $I_{\mathrm{Gal}(L^{\mathrm{un}}/K^{\mathrm{un}})}$, as in the definition of Tate-cohomology. In particular, we obtain a map

$$N : H_0(\mathrm{Gal}(L^{\mathrm{un}}/K^{\mathrm{un}}), U_{L^{\mathrm{un}}}) \to U_{K^{\mathrm{un}}}.$$

We now have the following.

Lemma 4.20. *Suppose that $x \in H_0(\mathrm{Gal}(L^{\mathrm{un}}/K^{\mathrm{un}}), U_{L^{\mathrm{un}}})$ is fixed by $\phi \in \mathrm{Gal}(L^{\mathrm{un}}/K)$ (in the sense that if u is a lift of x to U_L, we have that $u^{\phi-1} \in I_{\mathrm{Gal}(L^{\mathrm{un}}/K^{\mathrm{un}})}$) such that $d_K(\phi) = 1$ then*

$$N(x) \in \mathrm{Nm}_{L^{\mathrm{un}}/K}(U_{L^{\mathrm{un}}}) \in U_K \subset U_{K^{\mathrm{un}}}.$$

Proof. Let u denote a representative of the class in homology attached to x. In particular, by assumption, we have that

$$u^{\phi-1} = \prod_{i=1}^{r} u_i^{\tau_i - 1} \tag{4.6}$$

for some $u_i \in U_{L^{\mathrm{un}}}$ and $\tau_i \in \mathrm{Gal}(L^{\mathrm{un}}/K^{\mathrm{un}})$. To show the claim, it suffices to exhibit a finite Galois subextension M/K of L^{un}/K such that $L \subset M$ and $u, u_i \in M$ and to show that

$$\mathrm{Nm}_{L^{\mathrm{un}}/K^{\mathrm{un}}}(u) \in \mathrm{Nm}_{M/K} U_M.$$

We set $n = [M : K]$. Then the fixed field of $\phi^n =: \sigma$, denoted Σ, contains M by the assumption that $d_K(\phi) = 1$. We let Σ_n/Σ be the unramified extension of degree n, which is the fixed field of σ^n. By Theorem 4.13 (1) for $i = 0$, we may find elements $\tilde{u}, \tilde{u}_i \in U_{\Sigma_n}$ such that

$$u = \mathrm{Nm}_{\Sigma_n/\Sigma}(\tilde{u}) \tag{4.7}$$

and

$$u_i = \mathrm{Nm}_{\Sigma_n/\Sigma}(\tilde{u}_i). \tag{4.8}$$

Since $H_T^{-1}(\mathrm{Gal}(\Sigma_n/\Sigma), U_{\Sigma_n})$ vanishes by Theorem 4.13 (1), there also exists $\tilde{y} \in U_{\Sigma_n}$ with

$$\tilde{u}^{\phi-1} / \prod_{i=1}^{r} \tilde{u}_i^{\tau_{i-1}} = \tilde{y}^{\sigma-1}. \tag{4.9}$$

Indeed, the LHS is in the kernel of the norm map and the augmentation ideal is spanned by elements of the form $\tilde{y}^{\sigma-1}$ for $\tilde{y} \in U_N$ by virtue of the fact that $\mathrm{Gal}(\Sigma_n/\Sigma)$ is cyclic and is generated by σ. In particular, we have that

$$\tilde{u}^{\phi-1} = (\tilde{y}\tilde{y}^{\phi}\cdots\tilde{y}^{\phi^{n-1}})^{\phi-1}\prod_{i=1}^{r}\tilde{u}_i^{\tau_i-1}, \tag{4.10}$$

where we note that the last two terms on the RHS give rise to $\tilde{u}^{\phi-1}$ on the LHS by (4.9), since $\sigma = \phi^n$, and then the remaining terms all cancel. Applying $\mathrm{Nm}_{L^{\mathrm{un}}/K^{\mathrm{un}}}(-)$ gives the equation

$$\mathrm{Nm}_{L^{\mathrm{un}}/K^{\mathrm{un}}}(\tilde{u})^{\phi-1} = \mathrm{Nm}_{L^{\mathrm{un}}/K^{\mathrm{un}}}(\tilde{y}\tilde{y}^{\phi-1}\cdots\tilde{y}^{\phi^{n-1}})^{\phi-1}.$$

Indeed, as noted above the augmentation ideal $I_{L^{\mathrm{un}}/K^{\mathrm{un}}}$ is killed under $\mathrm{Nm}_{L^{\mathrm{un}}/K^{\mathrm{un}}}$. In particular, if we set

$$z := \mathrm{Nm}_{L^{\mathrm{un}}/K^{\mathrm{un}}}(\tilde{u})/\mathrm{Nm}_{L^{\mathrm{un}}/K^{\mathrm{un}}}(\tilde{y}\tilde{y}^{\phi}\cdots\tilde{y}^{\phi^{n-1}}) \tag{4.11}$$

then we have $z^{\phi-1} = 1$ and so $z \in U_K$. If we set $y := \tilde{y}\tilde{y}^{\sigma}\cdots\tilde{y}^{\sigma^n-1} = \mathrm{Nm}_{\Sigma_n/\Sigma}(\tilde{y}) \in U_\Sigma$ then we obtain

$$\begin{aligned}
\mathrm{Nm}_{L^{\mathrm{un}}/K^{\mathrm{un}}}(u) &= \mathrm{Nm}_{L^{\mathrm{un}}/K^{\mathrm{un}}}(\tilde{u}\tilde{u}^{\sigma}\cdots\tilde{u}^{\sigma^{n-1}}) \\
&= \mathrm{Nm}_{L^{\mathrm{un}}/K^{\mathrm{un}}}(\tilde{y}\tilde{y}^{\phi}\cdots\tilde{y}^{\phi^{n-1}})^{1+\sigma+\cdots\sigma^{n-1}}z\cdots z^{\sigma^{n-1}} \\
&= \mathrm{Nm}_{L^{\mathrm{un}}/K^{\mathrm{un}}}(yy^{\phi}\cdots y^{\phi^{n-1}})z^n \\
&= \mathrm{Nm}_{\Sigma/K}(y)\mathrm{Nm}_{M/K}(z) \in \mathrm{Nm}_{M/K}(U_M),
\end{aligned}$$

as desired. Here we have:

(1) The first equation follows from (4.7).
(2) The second equation follows from (4.11).
(3) The third equation follows from the fact that $z \in U_K$ and the definition of y.
(4) The fourth equation follows from arguing as in the proof of Lemma 4.19. Indeed, we note that $\Sigma \cap K^{\mathrm{un}} = M \cap K$ is an unramified degree extension of degree K with Frobenius generated by ϕ and $\Sigma^{\mathrm{un}} = M^{\mathrm{un}} = L^{\mathrm{un}}$.

□

We now may finally show that r' is indeed a homomorphism.

Lemma 4.21. *The map r' of construction 4.14 is a homomorphism of semi-groups.*

Proof. Let $g_1, g_2 \in H$ and put $g_3 = g_1g_2$. For $i = 1, 2, 3$, let M_i be the fixed fields of this elements and $\rho_i = \mathrm{Nm}_{M_i/K}(\pi_i)$ the image under the map r' for uniformizing elements $\pi_i \in M_i$. We set $\rho := \frac{\rho_1\rho_2}{\rho_3}$. We note that we have

$$v_K(\rho_i) = f(M_i/K)v_{M_i}(\pi_i) = f(M_i/K) = d_K(g_i)$$

by (4.3) and Remark 4.15. This implies that $v_K(\rho) = 0$, since d_K is a homomorphism. In particular, we have that $\rho \in U_K$ and we want to show that $\rho \in \mathrm{Nm}_{L/K}(A_L)$ in order to conclude.

To do this, we we will use Lemma 4.19. We choose $\phi \in H$ such that $d_K(\phi) = 1$ as in *loc.cit.* Put $d_i := d_K(g_i)$ and $\tau_i := g_i^{-1}\phi^{d_i}$ then

$$\tau_3 = g_2^{-1}g_1^{-1}\phi^{d_1+d_2} = g_2^{-1}\phi^{d_2}(\phi^{-d_2}g_1\phi^{d_2})^{-1}\phi^{d_1} = \tau_2(\phi^{-d_2}g_1\phi^{d_2})^{-1}\phi^{d_1}.$$

We now rewrite $g_1' = \phi^{-d_2}g_1\phi^{d_2}$ and $\tau_1' = (g_1')^{-1}\phi^{d_1}$. We then have

$$\tau_3 = \tau_1'\tau_2$$

We set M_1' to be the fixed field of g_1' and set $\pi_1' = \pi_1^{\phi_{d_2}}$. We note that $\mathrm{Nm}_{M_1'/K}(\pi_1') = \mathrm{Nm}_{M_1/K}(\pi_1) = \rho_1$, since g_1' and g_1 are by definition conjugate under ϕ^{d_2} in $\mathrm{Gal}(L^{\mathrm{un}}/K)$.

We set

$$\sigma_i := \pi_i \pi_i^{\phi} \cdots \pi_i^{\phi^{d_i-1}}$$

for $i = 2, 3$, and

$$\sigma_1' := (\pi_1')(\pi_1')^{\phi} \cdots (\pi_1')^{\phi^{d_i-1}}$$

and $u = \sigma_1'\sigma_2/\sigma_3$ is an element in U_N, where N is a finite subextension of L^{un}/L containing M_1, M_2, M_3, M_1'.

By Lemma 4.19, we have that $\rho = \mathrm{Nm}_{L^{\mathrm{un}}/K^{\mathrm{un}}}(u)$. We claim that actually this equal to an element in $\mathrm{Nm}_{L^{\mathrm{un}}/K}(U_N)$ which would show the desired claim.

We define

$$u_1 := (\pi_1')^{\tau_1 - 1}$$
$$u_2 := \pi_2/\pi_1'$$

and

$$u_3 := \pi_3/\pi_1'$$

which will all lie inside U_N.

Now we compute that

$$\begin{aligned} u^{\phi-1} &= \frac{(\pi_1')^{\tau_1'-1}\pi_2^{\tau_2-1}}{\pi_3^{\tau_3-1}} \\ &= \frac{u_1^{\tau_1'-1}u_2^{\tau_2-1}}{u_3^{\tau_3-1}}, \end{aligned}$$

where for the second equality we have used $\tau_1'\tau_2 = \tau_3$. The claim now follows from lemma 4.20. □

We now may define the following.

Definition 4.22. By Remark 4.18 and Lemma 4.21, we obtain for any Galois extension of finite subextensions of $\overline{k}/k$ a homomorphism

$$r_{L/K} : \mathrm{Gal}(L/K) \to A_K/\mathrm{Nm}_{L/K}A_L,$$

which we refer to as the reciprocity map. We write $r_{L/K}^{\mathrm{ab}} : \mathrm{Gal}(L/K)^{\mathrm{ab}} \to A_K/\mathrm{Nm}_{L/K}A_L$ for the induced map on the abelianization.

We now record some abstract properties of this reciprocity map.

Proposition 4.23. *Let L/K and L'/K' be Galois extensions of finite subextensions of $\overline{k}/k$. Then the reciprocity maps of (4.22) satisfy the following.*

(1) If $K \subset K'$ and $L \subset L'$ then the diagram

$$\begin{array}{ccc} \mathrm{Gal}(L'/K') & \xrightarrow{r_{L'/K'}} & A_{K'}/\mathrm{Nm}_{L'/K'}A_{L'} \\ \downarrow & & \downarrow{\scriptstyle \mathrm{Nm}_{K'/K}} \\ \mathrm{Gal}(L/K) & \xrightarrow{r_{L/K}} & A_K/\mathrm{Nm}_{L/K}A_L \end{array}$$

commutes, where the left vertical arrow is induced by the natural restriction map $\mathrm{Gal}(L'/K') \to \mathrm{Gal}(L/K)$. It follows that we have an analogous claim on abelianizations.

(2) If $L = L'$ and $K \subset K' \subset L$ then the diagram

$$\begin{array}{ccc} \mathrm{Gal}(L/K)^{\mathrm{ab}} & \xrightarrow{r_{L/K}^{\mathrm{ab}}} & A_K/\mathrm{Nm}_{L/K}A_L \\ \downarrow & & \downarrow \\ \mathrm{Gal}(L/K')^{\mathrm{ab}} & \xrightarrow{r_{L/K'}^{\mathrm{ab}}} & A_{K'}/\mathrm{Nm}_{L/K'}A_K \end{array},$$

commutes. Here the right arrow is induced by restriction along the norm map $A_{K'} \to A_K$, and the left vertical arrow is the Verlagerung morphism defined in 2.105 (6).

Proof. See [Neu99, Chapter IV, Section 5, Propositions 5.8, 5.9]. □

This in particular allows us to deduce the following, which will play an essential role in proving that the reciprocity map is an isomorphism.

Corollary 4.24. *Let $M \subset L \subset K$ be a set of Galois subextensions of $\overline{k}/k$ with finite Galois groups. Then there exists a commutative diagram of exact sequences*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(L/M) & \longrightarrow & \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(M/K) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle r_{L/M}} & & \downarrow{\scriptstyle r_{L/K}} & & \downarrow{\scriptstyle r_{M/K}} & & \\ & & A_M/\mathrm{Nm}_{L/M}A_L & \xrightarrow{\mathrm{Nm}_{M/K}} & A_K/\mathrm{Nm}_{L/K}A_L & \longrightarrow & A_K/\mathrm{Nm}_{M/K}A_M & \longrightarrow & 1 \end{array} \tag{4.12}$$

Proof. The commutativity of the left square follows from Proposition 4.23 (1). The exactness of the top row is a standard consequence of Galois theory, and the exactness on the right of the bottom row follows from the inclusion $\mathrm{Nm}_{L/K}A_L \subset \mathrm{Nm}_{M/K}A_M$ given by the transitivity of norms. The commutativity of the right most square now follows from the fact that $r_{M/K}$ is defined by taking $r_{L/K}$ and quotienting out by $\mathrm{Nm}_{M/K}A_M$ and $\mathrm{Gal}(L/M)$ as in Remark 4.18. □

Our goal is now to show that the map $r_{L/K}$ of Definition 4.22 is an isomorphism. As one might expect from local class field theory, the case of an unramified extension is handled by Theorem 4.13.

Lemma 4.25. *For L/K an unramified extension of finite subextensions of $\overline{k}/k$ the natural map*

$$r_{L/K} : \mathrm{Gal}(L/K) \to A_K/\mathrm{Nm}_{L/K}A_L$$

of Definition 4.22 is an isomorphism sending the Frobenius of $\mathrm{Gal}(L/K)$ to a uniformizer of K.

Proof. Let $g \in \mathrm{Gal}(L/K)$ be a generator and choose $h \in \mathrm{Gal}(L^{\mathrm{un}}/K)$ lifting g. Then the fixed field of h is K itself and by definition of r' the element $r'(h)$ is the uniformizer of K. By Theorem 4.13 (2), we have that this generates $H^0(\mathrm{Gal}(L/K), A_L) \simeq A_K/\mathrm{Nm}_{L/K}A_L$, as desired. □

Just as in the proof of local class field theory, we now turn to the case of totally ramified cyclic extensions.

Proposition 4.26. *Let L/K be a cyclic totally ramified extension of finite subextensions of $\overline{k}/k$ then the map $r_{L/K} : \mathrm{Gal}(L/K) \to A_K/\mathrm{Nm}_{L/K}A_L$ is an isomorphism.*

Proof. We note that L^{un}/K is the compositum of two disjoint extensions L/K and K^{un}/K. In particular, the natural map

$$\mathrm{Gal}(L^{\mathrm{un}}/K) \to \mathrm{Gal}(L/K) \times \mathrm{Gal}(K^{\mathrm{un}}/K) \tag{4.13}$$

is an isomorphism. We let σ be a generator of $\mathrm{Gal}(L/K)$ and let ϕ be a generator of $\mathrm{Gal}(K^{\mathrm{un}}/K)$ so that $d_K(\phi) = 1$. We fix the following notation.

(1) $n := [L : K]$
(2) $\tau := \sigma\phi \in \mathrm{Gal}(L^{\mathrm{un}}/K)$ via the isomorphism (4.13) and set $M = (L^{\mathrm{un}})^{\tau}$ to be the fixed field of τ.
(3) Let $N := LM$.
(4) Let $N_0 := N \cap K^{\mathrm{un}}$.
(5) Let π_L (resp. π_M) is a uniformizer of L (resp. M).
(6) j is the order of $r_{L/K}(\sigma) \in A_K/\mathrm{Nm}_{L/K}A_L$.
(7) Let $u := \pi_M^j/\pi_L^j \in U_N$.

We note the following simple features of the situation.

Observations 4.27. *(1) We note that $d_K(\tau) = 1$ by construction.*

(2) We note that, since L/K and K^{un}/K are disjoint extensions, we obtain a natural isomorphism

$$\mathrm{Gal}(L^{\mathrm{un}}/K^{\mathrm{un}}) \xrightarrow{\simeq} \mathrm{Gal}(L/K^{\mathrm{un}} \cap L) = \mathrm{Gal}(L/K).$$

(3) We note that, since $L^{\mathrm{un}} = NK^{\mathrm{un}}$ and $N \cap K^{\mathrm{un}} = N_0$, the natural map

$$\mathrm{Gal}(L^{\mathrm{un}}/K^{\mathrm{un}}) \to \mathrm{Gal}(N/N_0)$$

is an isomorphism. In particular, by (2), and the assumption $\mathrm{Gal}(L/K)$ is cyclic the group $\mathrm{Gal}(N/N_0)$ is also cyclic.

By 4.27 (1) and Lemma 4.19, we have that $r_{L/K}(\sigma) := \mathrm{Nm}_{M/K}(\pi_M) = \mathrm{Nm}_{L^{\mathrm{un}}/K^{\mathrm{un}}}(\pi_M)$. In particular, it follows that $\mathrm{Nm}_{L^{\mathrm{un}}/K^{\mathrm{un}}}(\pi_M^j)$ belongs to $\mathrm{Nm}_{L/K}(A_L)$, by the definition of j. Similarly, we have that $\mathrm{Nm}_{L^{\mathrm{un}}/K^{\mathrm{un}}}(\pi_L^j) = \mathrm{Nm}_{L/K}(\pi_L^j)$ also belongs to $\mathrm{Nm}_{L/K}(A_L)$, where equality follows from observation 4.27 (2). In particular, we may choose $v \in A_L$ such that

$$\mathrm{Nm}_{L^{\mathrm{un}}/K^{\mathrm{un}}}(u) = \mathrm{Nm}_{L/K}(v) = \mathrm{Nm}_{L^{\mathrm{un}}/K^{\mathrm{un}}}(v), \tag{4.14}$$

where we have implicitly used observation 4.27 (2) to compare the norms for different extensions. Since $\mathrm{Nm}_{L/K}(v) \in A_K \cap U_N = U_K$, we must have that $v \in U_L$. Now applying the class field axiom to to the extension N/N_0 (Definition 4.2), we have that

$$1 = H_T^{-1}(\mathrm{Gal}(N/N_0), A_N) = \mathrm{Ker}(\mathrm{Nm}_{N/N_0})/\{a^{\sigma-1} : a \in A_N\},$$

where we have used observation 4.27 (3) to identify the augmentation ideal we are quotienting out by on the RHS. In particular, since $\mathrm{Nm}_{N/N_0}(u/v) = \mathrm{Nm}_{L^{\mathrm{un}}/K^{\mathrm{un}}}(u/v) = 1$ (by observation 4.27 (3) for the first equality and 4.14 for the second equality), we have that

$$u/v = a^{\sigma-1} \tag{4.15}$$

for some $a \in A_N$. Then we have that

$$(\pi_L^j v)^{\sigma-1} = (\pi_L^j v)^{\tau-1} = (\pi_M^j v/u)^{\tau-1} = (v/u)^{\tau-1} = (a/a^\tau)^{\sigma-1}. \tag{4.16}$$

Here we have that.

(1) The first equality follows from the fact that τ projects to σ via $\mathrm{Gal}(L^{\mathrm{un}}/K) \to \mathrm{Gal}(L/K)$ by definition.
(2) The second equality follows from the definition of u.
(3) The third equality follows from the fact that M is the fixed field of τ.
(4) The fourth equality follows from (4.15), where we have switched the $\sigma - 1$ and the $\tau - 1$.

In particular, if we put $x := (\pi_L^j v)(a^\tau/a)$ then $x^\sigma = x$ by (4.16) and therefore $x \in A_{N_0}$. Hence, we have that

$$j = v_N(x) = n v_{N_0}(x) \in n\hat{\mathbb{Z}},$$

where the first equality follows from the fact that $v_N(\pi_L) = 1$ since N/L is unramified, the fact that $v \in U_L$, and the fact that $a^\tau/a \in U_L$. By definition of j, this implies that $r_{L/K}(\sigma)$ in $A_K/\mathrm{Nm}_{L/K}A_L$ is divisible by n. However, by the class field axiom $r_{L/K}$ is a map between two groups of the same order, and therefore it is an isomorphism. □

We now perform a bootstrap.

Proposition 4.28. *Suppose L/K is an abelian extension of finite subextensions of $\overline{k}/k$ then the natural map*

$$r_{L/K} : \mathrm{Gal}(L/K) \to A_K/\mathrm{Nm}_{L/K}A_L$$

is an isomorphism.

Proof. If L/K is cyclic of prime order then by Lemma 4.6 (5), we know that it is either totally ramified or unramified, and the claim follows. In general, we apply induction on $[L : K]$. In particular, we let M be a subextension of L/K and use the diagram (4.12) and apply the snake lemma 2.21. This tells us that the map $r_{L/K}$ is surjective (Note that we don't get injectivity as the sequence coming from the snake lemma isn't exact on the left). If L/K is cyclic then the map $r_{L/K}$ is a map between two groups of the same order by the class field axiom, and therefore must be an isomorphism. Suppose that it is not cyclic. We see by the diagram (4.12) that the the kernel of $r_{L/K}$ lies in the kernel of $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$ for every cyclic subextension M/K. However, the natural map $\mathrm{Gal}(L/K) \to \prod_M \mathrm{Gal}(M/K)$ is injective, by the classification of finite abelian groups. □

We now establish the general case.

Theorem 4.29. *Suppose L/K is a general extension of finite subextensions of $\overline{k}/k$ then the natural map*

$$r^{\mathrm{ab}}_{L/K} : \mathrm{Gal}(L/K)^{\mathrm{ab}} \to A_K/\mathrm{Nm}_{L/K}A_L$$

induced by the reciprocity map in Definition 4.22 is an isomorphism.

Proof. We first note that the map $r^{\mathrm{ab}}_{L/K}$ is injective, since the composition

$$\mathrm{Gal}(L^{\mathrm{ab}}/K^{\mathrm{ab}}) = \mathrm{Gal}(L/K)^{\mathrm{ab}} \xrightarrow{r^{\mathrm{ab}}_{L/K}} A_K/\mathrm{Nm}_{L/K}(A_L) \xrightarrow{\mathrm{Nm}_{K/K^{\mathrm{ab}}}} A_{K^{\mathrm{ab}}}/\mathrm{Nm}_{L^{\mathrm{ab}}/K^{\mathrm{ab}}}(A_{L^{\mathrm{ab}}})$$

identifies with $r_{L^{\mathrm{ab}}/K^{\mathrm{ab}}}$ by Proposition 4.23 (1), and this is an isomorphism by Proposition 4.28. We now need to show it is surjective, it suffices to do this for $r_{L/K}$ instead of $r^{\mathrm{ab}}_{L/K}$. We note that if $\mathrm{Gal}(L/K)$ is solvable, we could finish by combining Proposition 4.28 with (4.12), the snake lemma 2.21, and induction on the degree of $[L : K]$. To reduce to the solvable case, we take a page from our proof of Theorem 2.119 and use the Sylow theorems.

For general L/K, we check that the map becomes a surjection after restricting to each Sylow p-subgroup. In particular, we let M be the fixed field of a p-Sylow subgroup of $\mathrm{Gal}(L/K)$ and we let S_p be the p-sylow subgroup of $A_K/\mathrm{Nm}_{L/K}A_L$. We want to show that the natural map

$$\mathrm{Gal}(L/M) \to \mathrm{Gal}(L/K) \xrightarrow{r_{L/K}} A_K/\mathrm{Nm}_{L/K}A_L$$

surjects onto $S_p \subset A_K/\mathrm{Nm}_{L/K}A_L$. Indeed, by varying the prime p, this will imply the desired surjectivity. We look at the commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(L/M)^{\mathrm{ab}} & \longrightarrow & \mathrm{Gal}(L/K)^{\mathrm{ab}} \\ \downarrow{\scriptstyle r^{\mathrm{ab}}_{L/M}} & & \downarrow{\scriptstyle r^{\mathrm{ab}}_{L/K}} \\ A_M/\mathrm{Nm}_{L/M}A_L & \xrightarrow{\mathrm{Nm}_{M/K}} & A_K/\mathrm{Nm}_{L/K}A_L \end{array} \tag{4.17}$$

given by Proposition 4.23 (1). The composite $\mathrm{Nm}_{M/K} \circ i$ will be equal to $[M : K]$, which is coprime to p which preserves the p-Sylow subgroup S_p. It follows that $\mathrm{Nm}_{M/K}$ surjects onto S_p. Since $r^{\mathrm{ab}}_{L/M}$ is an isomorphism, by the already established case of solvable extensions, we conclude by the commutativity of the diagram (4.17) that $\mathrm{Gal}(L/M)^{\mathrm{ab}}$ surjects onto S_p, as desired. □

Exactly as in the proof of local class field theory, the existence of this isomorphism also gives us some version of the norm limitation theorem (Theorem 3.6).

Corollary 4.30. *For L/K an arbitrary extension of finite subextensions of $\overline{k}/k$, and M the maximal abelian subextension of L/K. We have that $\mathrm{Nm}_{L/K}A_L = \mathrm{Nm}_{M/K}A_M$.*

Proof. We note that there is a tautological inclusion $\mathrm{Nm}_{L/K}A_L \subset \mathrm{Nm}_{M/K}A_M$ so it only remains to establish the converse inclusion. In order to do this, we may replace L/K by its Galois closure L^{Gal}/K and use the tautological inclusion

$$\mathrm{Nm}_{L^{\mathrm{Gal}}/K}A_{L^{\mathrm{Gal}}} \subset \mathrm{Nm}_{L/K}A_L$$

to see that it suffices to show that $\mathrm{Nm}_{M/K}A_M \subset \mathrm{Nm}_{L^{\mathrm{Gal}}/K}A_{L^{\mathrm{Gal}}}$. Therefore, we may assume L/K is Galois. In this case, we look at the commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(L/K)^{\mathrm{ab}} & \xrightarrow{r_{L/K}^{\mathrm{ab}}} & A_K/\mathrm{Nm}_{L/K}A_L \\ \| & & \downarrow \\ \mathrm{Gal}(M/K)^{\mathrm{ab}} & \xrightarrow{r_{M/K}} & A_K/\mathrm{Nm}_{M/K}A_M \end{array}$$

granted by Proposition 4.23 (1). We see that, by Theorem 4.29, every map in the diagram is an isomorphism, which forces the desired equality. □

We also obtain the following.

Corollary 4.31. *Let L_1/K and L_2/K be abelian extensions of finite subextensions of $\overline{k}/k$ then if*

$$\mathrm{Nm}_{L_1/K}A_{L_1} = \mathrm{Nm}_{L_2/K}A_{L_2}$$

we have that $L_1 = L_2$.

Proof. Let $L = L_1L_2$ which is also a finite abelian extension of K. We have an isomorphism

$$\mathrm{Gal}(L/K) \simeq A_K/\mathrm{Nm}_{L/K}A_L$$

by Theorem 4.29. Using the commutative diagram 4.23, we see that the natural quotient maps $\mathrm{Gal}(L/K) \to \mathrm{Gal}(L_1/K)$ and $\mathrm{Gal}(L/K) \to \mathrm{Gal}(L_2/K)$ correspond to the quotient maps $A_K/\mathrm{Nm}_{L/K}A_L \to A_K/\mathrm{Nm}_{L_1/K}A_{L_1}$ and $A_K/\mathrm{Nm}_{L/K}A_L \to A_K/\mathrm{Nm}_{L_2/K}A_{L_2}$ under the reciprocity isomorphisms $r_{L/K}$, $r_{L_1/K}$, and $r_{L_2/K}$. In particular, the equality of norm subgroups forces that $\mathrm{Gal}(L_1/K)$ and $\mathrm{Gal}(L_2/K)$ correspond to the same quotient of $\mathrm{Gal}(L/K)$, which in turn implies that $L_1 = L_2$ by Galois theory. □

Remark 4.32. We note that if we have a subgroup $U \subset A_K$ such that $\mathrm{Nm}_{M/K}A_M \subset U \subset A_K$ for some finite extension M/K of finite extensions of $\overline{k}/k$ then $U = \mathrm{Nm}_{L/K}A_L$ for L/K a finite (even abelian) by Corollary 4.30 subextension of M/K. Indeed, if we look at the image of the subgroup $U/\mathrm{Nm}_{M/K}A_M$ under the reciprocity map

$$\mathrm{Gal}(M/K)^{\mathrm{ab}} \xrightarrow{r_{M/K},\simeq} A_K/\mathrm{Nm}_{M/K}A_M,$$

the resulting fixed field does the job. In particular, we see the key to establishing an analogue of the norm existence theorem is to compute the intersection

$$\cap_{M/K}\mathrm{Nm}_{M/K}A_M \subset A_K$$

for all finite extensions M/K (equivalently abelian extensions by Corollary 4.30). In Proposition 3.32, we showed that this intersection was trivial in the situation of 4.12 (1), which when combined with this reasoning was in enough to gives us the local existence theorem (Theorem 3.2). Without knowing this, we can still use this to give a description of the Galois group $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ of the maximal abelian extension. Indeed, Theorem 4.29 give us an identification

$$\mathrm{Gal}(K^{\mathrm{ab}}/K) = \lim_{M/K}\mathrm{Gal}(M/K) \xrightarrow{r_{M/K},\simeq} \lim_{M/K} A_K/\mathrm{Nm}_{M/K}A_M, \tag{4.18}$$

where we may think of the right hand side as a completion with respect to a certain norm topology on A_K. In particular, we may declare the subgroups $\mathrm{Nm}_{M/K}A_M \subset A_K$ to be a basis of open

subgroups of the identity element, and then the RHS is analogous to the profinite completion operation described in 2.5 (3). In the setting of local class field theory, we know that the norm subgroups are the same as the open finite index ones and this norm completion identified with the profinite completion of K^*, as in Corollary 3.5.

We now introduce our candidate for the subgroups A_K in the case that k is a number field.

4.2. **Adeles, Ideles, and Class Fields.**

4.2.1. *The Basic Definitions.* If one looks at Theorem 1.10, we see that the description of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ involves a product of the rings of integers of the completion of the base field $\mathbb{Q}$ for every prime p in the ring of integers $\mathbb{Z}$. If we compare this with the description of the Galois group of the maximal abelian extension given by (4.18) this leads us to believe that we should take our modules A_K to be similar product of the completions of the number field K. However, we will need to exercise some care when forming this product. Indeed, we note that $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ has the structure of a compact Hausdorff topological group by Proposition 2.2, and this topological structure is important if one wants to capture about the subextensions of $\mathbb{Q} \subset \mathbb{Q}^{\mathrm{ab}}$, as in Theorem 2.17. This leads us to believe that the groups A_K we are looking for should be compact topological groups, so we should be looking for a compact or at least a locally compact group attached to such a product of completions.

In particular, we note that if we simply take the product

$$\prod_p \mathbb{Q}_p$$

of all the completions equipped with its product topology then this is not locally compact. Indeed, a basis of open subgroups of the identity is given by

$$\prod_{p \in S} U_p \times \prod_{p \notin S} \mathbb{Q}_p$$

for $U_p \subset \mathbb{Q}_p$ an open subgroup of $\mathbb{Q}_p$ and S a *finite* set of primes of $\mathbb{Q}$. Since the primes are infinite, we can never arrange that such an open is compact. In order to fix this, we introduce the following notion.

Definition 4.33. Let I be a countable index set. For each $i \in I$, let G_i be a set and let H_i be a subset of G_i. The restricted product, denoted $\prod'_{i \in I}(G_i, H_i)$, of the pairs $\{(G_i, H_i)\}_{i \in I}$ is the union of

$$G_S := \prod_{i \in S} G_i \times \prod_{i \notin S} H_i$$

inside $\prod_{i \in I} G_i$ for $S \subset I$ varying over finite subsets.

We note the following basic facts about this construction.

Observations 4.34. *In the situation of Definition 4.33, we observe the following.*

1. *If G_i is a group and each $H_i \subset G_i$ is a subgroup then $\prod'_{i \in I}(G_i, H_i)$ admits a group structure, by restricting the group structure on $\prod_{i \in I} G_i$. Indeed, this later group structure will take G_S and G_T to $G_{S \cup T}$.*
2. *If each G_i is a topological space and H_i is equipped with the subspace topology then $\prod'_{i \in I}(G_i, H_i)$ acquires the structure of a topological space, where we declare a subspace to be open if its intersection with the G_S is open, and G_S has the product topology.*
3. *In the setting of (2), if H_i is a compact open subspace of a locally compact G_i then $\prod'_{i \in I}(G_i, H_i)$ is a locally compact topological space. Indeed, by Tychonoff the subspace $\prod_{i \in S} G_i \times \prod_{i \notin S} H_i$ equipped with its product topology will be locally compact, since S is finite.*

(4) In the setting of (2), we note that the inclusion $\prod'_{i\in I}(G_i, H_i) \to \prod_{i\in I} G_i$ is continuous; however, the topology on the source is strictly finer. In particular, if G_i is Hausdorff then $\prod_{i\in I} G_i$ is easily checked to be Hausdorff and it follows that $\prod'_{i\in I}(G_i, H_i)$ is also Hausdorff.

In light of (3), we see that this fixes the aforementioned problem of taking $\prod_p \mathbb{Q}_p$. This motivates the following.

Definition 4.35. We define the finite adeles $\mathbb{A}_f$ of $\mathbb{Q}$ to be the restricted product

$$\prod{}'_p(\mathbb{Q}_p, \mathbb{Z}_p),$$

As a set, it is the set of (α_p) such that $\alpha_p \in \mathbb{Z}_p$ for all but finitely many p. Similarly, for $K/\mathbb{Q}$ a number field, we define the finite adeles of K to be

$$\prod{}'_{\mathfrak{p}}(K_{\mathfrak{p}}, \mathcal{O}_{K_{\mathfrak{p}}}),$$

where $\mathfrak{p}$ ranges over the prime ideals of K, $K_{\mathfrak{p}}$ denotes the completion at the $\mathfrak{p}$-adic valuation of K, and $\mathcal{O}_{K_{\mathfrak{p}}} \subset K_{\mathfrak{p}}$ is the ring of integers. We refer to the set of prime ideals $\mathfrak{p}$ of K as the finite or non-archimedean places of the number field K.

Remark 4.36. We note, by observations 4.34 (2)-(4) that $\mathbb{A}_{K,f}$ has the naural structure of a *locally compact* Hausdorff topological group.

We will need to refine this a bit further. First, we recall that if we have number field $K/\mathbb{Q}$ of degree n then we may take a primitive element $\alpha \in K$ such that

$$K = \mathbb{Q}(\alpha) \simeq \mathbb{Q}[x]/f(x) \tag{4.19}$$

for some minimal polynomial $f \in \mathbb{Q}[x]$, and we obtain embeddings

$$\tau_i : K \simeq \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C} \tag{4.20}$$

by sending $\alpha \mapsto \alpha_i$ for $i = 1, \ldots, n$, where α_i are the roots of $f(x) \in \mathbb{Q}[x]$ over $\mathbb{C}$. We recall the following.

Definition 4.37. Let $K/\mathbb{Q}$ be a number field of degree n, we define the following.

(1) We set $K_{\mathbb{C}} = K \otimes_{\mathbb{Q}} \mathbb{C}$ and $K_{\mathbb{R}} \otimes_{\mathbb{Q}} \mathbb{R}$. We note that the isomorphism (4.20) induces isomorphisms

$$K \otimes_{\mathbb{Q}} \mathbb{C} \simeq \prod_{i=1}^{n} \mathbb{C} \tag{4.21}$$

and

$$K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \prod_{i=1}^{r} \mathbb{R} \times \prod_{i=1}^{s} \mathbb{C} \tag{4.22}$$

such that $r + 2s = n$. Here we note that the map (4.21) from left to right is defined by applying the embedding τ_i of (4.20) to the first tensor factor and multiplying by an element of $\mathbb{C}$ on the second factor.

(2) We refer to the direct factors of the RHS (4.22) as the archimedean or infinite places v of K. Together with the non-archimedean places of K introduced in Definition 4.35, this gives the collection of the places of a number field K. For an archimedean place v, we let K_v denote the associated field appearing in the RHS of (4.22). If $K_v = \mathbb{R}$ we say v is a real place, and if $K_v = \mathbb{C}$ it is a complex place. We note that in light of point (1) we can identify the archimedean places v with the set of embeddings $\tau_i : \mathbb{Q} \hookrightarrow \mathbb{C}$ modulo the equivalence relationship of complex conjugation. In particular, if $\tau_i = \overline{\tau}_i$ for some i then it gives rise to a real place, and if $\tau_i \neq \overline{\tau}_i$ then the equivalence class of $\{\tau_i, \overline{\tau}_i\}$ gives rise to a complex place.

(3) Let L/K be a finite extension, consider a non-archimedean place w with corresponding equivalence class of embeddings $L \hookrightarrow \mathbb{C}$ as in point (3). We say that w lies over v, denoted $w|v$, if the resulting equivalence class of embeddings $K \hookrightarrow L \hookrightarrow \mathbb{C}$ corresponds to v. We note that in this situation we have an inclusion $K_v \subset L_w$, which is a finite extension of degree 1 or 2.
(4) We write $j_{\mathbb{C}} : K \to \prod_{i=1}^{n} \mathbb{C}$ for the embedding given by sending a to $\tau_i(a)$, where τ_i is as in (4.20). We note that, under the isomorphism (4.21), this identifies with the natural inclusion $K \to K_{\mathbb{C}}$ as the first tensor factor. Similarly, we write $j_{\mathbb{R}} : K \to K_{\mathbb{R}}$ for the inclusion of the first tensor factor.
(5) We equip $K_{\mathbb{C}} \simeq \prod_{i=1}^{n} \mathbb{C}$ with the natural Hermitian inner product

$$\langle z_1, z_2 \rangle := \sum_{i=1}^{n} z_{1,i} \overline{z_{2,i}}.$$

This restricts to a positive definite inner product on $K_{\mathbb{R}} \hookrightarrow K_{\mathbb{C}}$.

Remark 4.38. This definition of archimedean places might seem strange when comparing it with the non-archimedean ones. However, we note that they can be put on equal footing. Indeed, if we have a finite extension L/K and some place v (archimedean or non-archimedean) of K then we always have an isomorphism

$$K_v \otimes_K L \simeq \prod_{w|v} L_w, \tag{4.23}$$

where w is the set of places in L dividing v, by applying the primitive element theorem as in (4.19) to the extension L/K. Here the map from left to right is given by embedding L into its completion L_w and multiplying by element in K_v. For non-archimedean places, this is a fact (See [Mil20b, Proposition 8.2]), where we recall that a non-archimedean place is defined to just be a prime ideal of K. What we did was essentially turn this fact for the non-archimedean places into a definition for the archimedean case.

Remark 4.39. We recall that that the ring of integers $\mathcal{O}_K \subset K$ or more generally any fractional ideal of K is a lattice in $K_{\mathbb{R}}$ (See [Mil20b, Proposition 4.26]) via the embedding $j_{\mathbb{R}}$ of Definition 4.37 (4). In other words, it is a discrete subgroup of $K_{\mathbb{R}}$ with the subspace topology such that its cokernel is compact with the quotient topology (e.g we think of the integral coordinate axes $\mathbb{Z}^n \subset \mathbb{R}^n$ (resp. $\mathbb{Z}^{2n} \subset \mathbb{C}^n$) inside n-dimensional real space (resp. $2n$-dimensional complex space). The fact that this is a lattice is a fundamental point in the proof of the finiteness of the class number of K.

As we will also want to keep track of whether an abelian extension $K/\mathbb{Q}$ is totally real (in the sense that all of its embeddings $\tau_i : K \hookrightarrow \mathbb{C}$ lie inside $\mathbb{R}$ or equivalently that $r = n$ as in Definition 4.37 (1), we will also want to consider completions of K at the archimedean places, which will be captured by the direct factors K_v of $K_{\mathbb{R}} \subset K_{\mathbb{C}}$. Indeed, note that, as in the discussion after Example 2.58, we have an isomorphism $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \simeq \mathbb{R}^*/\mathrm{Nm}_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^*)$, which may view as the very degenerate archimedean version of the local class field theory of §3. The action of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ on the embeddings $K \hookrightarrow \mathbb{C}$ will detect precisely whether a field is totally real. More precisely, we define the following.

Definition 4.40. For $K/\mathbb{Q}$ a number field, we define the adeles of K to be the topological group given by the product

$$\mathbb{A}_K = K_{\mathbb{R}} \times \mathbb{A}_{K,f}$$

equipped with the product topology. Alternatively, we may view this is as the restricted product

$$\prod_v (K_v, \mathcal{O}_v),$$

where v runs over all places of K including the archimedean ones $v|\infty$ introduced in Definition 4.37 and $\mathcal{O}_v := 0$ if $v|\infty$ is archimedean and $\mathcal{O}_v := \mathcal{O}_{K_v}$ is the ring of integers of the completion K_v if v is non-archimedean.

Similarly, if S is a finite set of places of K, we define the finite adelic-S-integers to be the subring $\mathbb{A}_{K,f,S} \subset \mathbb{A}_{K,f}$ of all elements that lie in $\mathcal{O}_{K_\mathfrak{p}}$ for $\mathfrak{p} \notin S$, as in Definition 4.33. We set $\mathbb{A}_{K,S} := \mathbb{A}_{K,f,S} \times K_\mathbb{R}$ and refer to it as the adelic S-integers. We omit the subscript K from this notation if $K = \mathbb{Q}$. If $K = \mathbb{Q}$ then we omit the subscript K from this notation as before.

Remark 4.41. We note that, since $\mathbb{A}_{K,f}$ by Remark 4.36 and $K_\mathbb{R}$ are both locally compact and Hausdorff the same is true for $\mathbb{A}_K$.

This will be our first approximation to the desired groups A_K. In particular, this will essentially be given by the multiplicative version of this known as the ideles. Before moving onto this, we note that, if we want to compare this with $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ as in Remark 4.32, we really want a compact topological group. A hint for how do this is given by Remark 4.39. Indeed, we see that quotienting out by $\mathcal{O}_K \subset K_\mathbb{R}$ has compact cokernel via the embedding $j_\mathbb{R}$. This leads us to think that maybe by embedding $\mathcal{O}_K \subset \mathbb{A}_K$ diagonally that the quotient acquires the structure of a compact group. However, this is too naive; in particular, we are ignoring the p-adic places in the restricted product defining $\mathbb{A}_{K,f}$, where we see something like $\mathbb{Q}_p/\mathbb{Z}_p$, which is not compact since may be identified with an infinite discrete space given by $\bigsqcup_{n\geq 0} p^{-n}\mathbb{Z}_p/\mathbb{Z}_p$. This leads us to consider the bigger subspace

$$\iota_K : K \hookrightarrow \mathbb{A}_K, \tag{4.24}$$

where $\iota_K = j_\mathbb{R} \times \Delta$, where $j_\mathbb{R}$ is as in Definition 4.37 (4) and $\Delta : K \to \mathbb{A}_{K,f}$ is the natural diagonal map given by sending $K \to K_v$ into its v-adic completion at a non-archimedean place. We note that Δ is well-defined since the v-adic valuation at all but finitely many places is trivial for any $a \in K$ (since there are only finitely many terms appearing in the prime factorization of the fractional ideal (a)). We now want to study the properties of this subgroup ι_K. In order to do this, we consider the subgroup $\mathbb{A}_K^* \subset \mathbb{A}_K$ of multiplicative units equipped with the multiplicative structure.

The set $\mathbb{A}_K^*$ of multiplicative units inside $\mathbb{A}_K$ is the set of ideles we are looking for to define our groups A_K. However, we need to be a bit careful. In particular, the exact topology that we want to endow the ideles with is slightly different than the natural subspace topology on $\mathbb{A}_K^*$.

Definition 4.42. For $K/\mathbb{Q}$ a number field, we define the ideles, denoted $\mathbb{I}_K$, to be the restricted product (Definition 4.33)

$$\prod_v{}' (K_v^*, \mathcal{O}_v^*),$$

where $\mathcal{O}_v^* = 0$ if v is archimedean and $\mathcal{O}_v = \mathcal{O}_{K_v}^*$ if $v$is nonarchimedean. Similarly, we set $\mathbb{I}_{K,f}$ to be the analogous restricted product only over the non-archimedean and refer to it as the finite ideles. For S a finite set of places, we write $\mathbb{I}_{K,S}$ (resp. $\mathbb{I}_{K,f,S}$) for the subgroup of elements that lie in $\mathcal{O}_{K_\mathfrak{p}}^*$ for a non-archimedean place $\mathfrak{p} \notin S$ and refer to it as the adelic S-units (resp. finite adelic S-units).

We now have the following precise relationship between $\mathbb{A}_K^* \subset \mathbb{A}_K$ and $\mathbb{I}_K$.

Exercise 4.43. *Let $\mathbb{A}_K^* \subset \mathbb{A}_K$ denote the set of multiplicative units inside $\mathbb{A}_K$ and let $\mathbb{I}_K$ denote the set of ideles. Show that the following is true.*

1. *Show that, as subgroups of $\prod_v K_v$, we have an equality $\mathbb{A}_K^* = \mathbb{I}_K$.*
2. *Show that the subspace topology on $\mathbb{A}_K^* \subset \mathbb{A}_K$ does not agree with the topology on $\mathbb{I}_K$ as a restricted product under the identification of (1), and that the map $\mathbb{I}_K \to \mathbb{A}_K$ is continuous.*
3. *Consider the natural embedding*

$$\begin{aligned} \mathbb{I}_K &\to \mathbb{A}_K \times \mathbb{A}_K \\ x &\mapsto (x, x^{-1}). \end{aligned}$$

Show that the restricted product topology on $\mathbb{I}_K$ is given by the subspace topology for $\mathbb{A}_K \times \mathbb{A}_K$ equipped with the product topologyunder this embedding. Moreover, show that this embedding has closed image.

We now have the following.

Definition 4.44. For each place v of K, we define a norm $|\cdot|_v : K_v \to \mathbb{R}_{\geq 0}$ as follows.

(1) If v is non-archimedean then we define $|\cdot|_v : K_v \to \mathbb{R}_{\geq 0}$ to be the v-adic norm attached to the p-adic field $K_v/\mathbb{Q}_p$, as in (3.3). However, we scale it so that that $|p|_v = p^{-[K_v:\mathbb{Q}_p]}$.
(2) If v is archimedean then we define it as follows.
   (a) We take $|\cdot|_v$ to be usual absolute if $K_v \simeq \mathbb{R}$ is real.
   (b) We take $|z|_v := |z\overline{z}|$ if $z \in K_v \simeq \mathbb{C}$ is complex, where $\overline{(-)}$ denotes complex conjugation.

We set

$$|\cdot|_K : \mathbb{A}_K \to \mathbb{R}_{>0}$$
$$(x_v)_v \mapsto \prod_v |x_v|_v,$$

where we note that the RHS converges as $|x_v|_v \leq 1$ for all but finitely many places v. For notational simplicity, for $x = (x_v)_v \in \mathbb{A}_K$, we will often write $|x|_v$ for $|x_v|_v$.

We also have norm maps between the adeles of different extension.

Definition 4.45. Let L/K be a finite extension of number fields. We define

$$N_{L/K} : \mathbb{A}_L \to \mathbb{A}_K$$
$$(x_w) \mapsto (\prod_{w|v} \mathrm{Nm}_{K_w/K_v}(x_w))_v,$$

where for the archimedean extensions the relevant extension of fields is given in Definition 4.37. We note that this is well-defined in light of 3.2.

This norm map has the following fundamental compatability with the norm map on the number field and the norm on the adeles.

Lemma 4.46. *Let L/K be a finite extension of number fields. Then the diagram*

$$\begin{array}{ccccc} L & \xrightarrow{\iota_L} & \mathbb{A}_L & \xrightarrow{|\cdot|_L} & \mathbb{R}_{\geq 0} \\ \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle N_{L/K}} & & \| \\ K & \xrightarrow{\iota_K} & \mathbb{A}_K & \xrightarrow{|\cdot|_K} & \mathbb{R}_{\geq 0} \end{array}$$

commutes.

Proof. In general, note that if we have a finite extension L/K and a place v, we have an identity

$$\mathrm{Nm}_{L/K}(x) = \prod_{w|v} \mathrm{Nm}_{L_w/K_v}(x).$$

Indeed, this follows from the isomorphism and (4.23) by taking products over all places v recalling that the norm may be viewed as the determinant of the K-linear map given by multiplication of the element $x \in L$. This implies commutativity of the left square by varying over all places w of L

For the right square, we claim that for all places w of L lying over $v \in K$, we have an equality

$$|\mathrm{Nm}_{L_w/K_v}(x)|_v = |x|_w.$$

Indeed, we note that if we evaluate on $x \in K_v$, this equation becomes

$$|x|_v^{[K_w:L_v]} = |x|_w,$$

which was precisely how we setup our normalization. By varying over all places w of L, this implies the desired claim. □

We now have the following fundamental property of this norm.

Proposition 4.47. ***(The Product Formula)*** *The subgroup $\iota_K(K^*) \subset \mathbb{A}_K^*$ lies in the kernel of the norm map $|\cdot|_K$.*

Proof. We first do the case where $K = \mathbb{Q}$. Let $x \in \mathbb{Q}$ if $|x|_\infty = \prod_p p^{n_p}$ is the prime factorization of the absolute value. Then we have

$$|x|_\infty \prod_p |x|_p = (\prod_p p^{n_p})(\prod_p p^{-v_p(x)}) = (\prod_p p^{n_p})(\prod_p p^{-n_p}) = 1,$$

which implies the claim. In general, we note that by applying 4.46 to the case of the extension $K/\mathbb{Q}$, we may reduce to this case. □

We can verify the following useful consequence, which hints at our expectation that the principal adeles $\iota_K : K \hookrightarrow \mathbb{A}_K$ is a kind of lattice.

Exercise 4.48. *Let K be a number field, and let $\mathbb{A}_K$ denote its ring of adèles. Show that the diagonal embedding*

$$\iota_K : K \hookrightarrow \mathbb{A}_K$$

has discrete image in the natural topology on $\mathbb{A}_K$. (Hint: Use the product formula. Try to find an open neighborhood U of $0 \in A_K$ such that $U \cap K = \{0\}$)

In a similar vein to the reasoning used in the proof of Lemma 4.46, we also have the following.

Lemma 4.49. *Let L/K be a finite extension of number fields. Then we have an isomorphism of topological rings*

$$\mathbb{A}_K \otimes_K L \xrightarrow{\simeq} \mathbb{A}_L$$
$$a \otimes b \mapsto a\iota_L(b).$$

Here the RHS is equipped with the topology coming from its presentation as the restricted product $\prod_v'(K_v \otimes_K L, \mathcal{O}_v \otimes_{\mathcal{O}_K} \mathcal{O}_L)$ (Note that tensor product as a left adjoint to Hom commutes with all colimits in light of Lemma 2.79 and the restricted product may be presented as a union = colimit of subgroups) and $\mathcal{O}_v$ is as in Definition 4.40. Moreover, this fits into a commutative diagram

$$\begin{array}{ccc} K \otimes_K L & \xrightarrow{\simeq} & L \\ \downarrow{\scriptstyle \iota_K \otimes_K L} & & \downarrow{\scriptstyle \iota_L} \\ \mathbb{A}_K \otimes_K L & \xrightarrow{\simeq} & \mathbb{A}_L, \end{array}$$

where the top arrow is the obvious isomorphism given by $a \otimes b \mapsto ab$.

Proof. As already noted, $\mathbb{A}_K \otimes_K L$ is isomorphic to the restricted product $\prod_v'(K_v \otimes_K L, \mathcal{O}_v \otimes_{\mathcal{O}_K} \mathcal{O}_L)$, which we note in light of (4.23) identifies with $\prod_v' \prod_{w|v}(L_w, \mathcal{O}_w)$. We may easily rewrite this in terms of $\prod_w'(L_w, \mathcal{O}_w) = \mathbb{A}_L$, as desired. It is easy to see that this has the claimed properties. □

In particular, we deduce the following consequence of this.

Corollary 4.50. *For L/K a finite Galois extension of a global field of degree n, we have an isomorphism*

$$\mathbb{A}_L \simeq \oplus_{i=1}^n \mathbb{A}_K$$

of topological K-vector spaces (where $\mathbb{A}_K$ is regarded as a K-module via ι_K), and on the principal ideles this restricts to the isomorphism $L \simeq \bigoplus_{i=1}^n K$ of K-vector spaces.

We now want to understand to what extent the quotient $\mathbb{A}_K/\iota_K(K)$ is compact, which together with Exercise 4.48 will justify our heuristic in Remark 4.39 that $\iota_K(K) \subset \mathbb{A}_K$ should be a lattice. Corollary 4.50 will reduce us to considering the case where $K = \mathbb{Q}$. To solve the problem in this case, we recall the following weak approximation theorem specialized to the case where $K = \mathbb{Q}$, which (up to formal manipulations) is essentially the Chinese remainder theorem.

Lemma 4.51. ***(Weak Approximation for $\mathbb{Q}$)*** *Let $p_1, p_2, \dots, p_n$ be distinct primes. Let $c_i \in \mathbb{Q}_{p_i}$ for be an element for each $i = 1, \dots, n$. Then, for every $\varepsilon > 0$, there exists an $\alpha \in \mathbb{Q}$ such that the p_i-adic norm satisfies*

$$|\alpha - c_i|_{p_i} < \varepsilon$$

for all $1 \leq i \leq n$. Furthermore, α may be chosen so that, for all $q \neq p_i$, we have that $|\alpha|_q \leq 1$; in other words, we have that $\alpha \in \mathbb{Z}_q$.

Proof. We first note, by uniformly scaling the c_i so that they lie in $\mathbb{Z}_{p_i}$, and using that we may choose ε to be as small as we want, we may reduce to the case where all the $c_i \in \mathbb{Z}_{p_i}$. Now, since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, we may replace $c_i \in \mathbb{Z}_p$ by $c_i' \in \mathbb{Z}$. Now we are asked with finding a $\alpha \in \mathbb{Z}$ such that α is congruent to the fixed c_i modulo some arbitrarily high powers n_i of p_i. By the Chinese remainder theorem, we may find a unique solution to this system of equations modulo $\prod_{i=1}^n p_i^{n_i}$, which gives the desired claim by choosing $x \in \mathbb{Z}$ lifting this solution. □

We now deduce the following corollary of this claim.

Corollary 4.52. *A fundamental domain for $\mathbb{A}/\iota(\mathbb{Q})$ is given by*

$$D := [0,1) \times \prod_p \mathbb{Z}_p \subset \mathbb{R} \times \mathbb{A}_f = \mathbb{A}.$$

More precisely, the projection $[0,1) \times \prod_p \mathbb{Z}_p \to \mathbb{A} \to \mathbb{A}/\iota(\mathbb{Q})$ is a bijection.

Proof. It suffices to show that every element $x \in \mathbb{A}$ may be expressed uniquely as $d + \iota(q)$ for $d \in D$ and $q \in \mathbb{Q}$. Fix $(x_v) \in \mathbb{A}$ let $p_1, \dots, p_n$ be the finite set of primes such that $x_{p_i} \notin \mathbb{Z}_{p_i}$, set $c_i = x_{p_i}$, and $\varepsilon = 1$. Then, applying Lemma 4.51, we obtain $\alpha \in \mathbb{Q}$ such that $|x_p - \alpha|_p \leq 1$ for all $p = p_i$. For $t \in \mathbb{R}$, let $[t]$ denote the greatest integer not exceeding t. We have that

$$x_p - \alpha - [x_\infty - \alpha] \in \mathbb{Z}_p,$$

for all p, since $|x_p - \alpha|_p \leq 1$ for $p = p_i$, and $\alpha, x \in \mathbb{Z}_p$ for $p \neq p_i$. Moreover, we have that

$$x_\infty - \alpha - [x_\infty - \alpha] \in [0,1).$$

This shows existence, by setting $q \in \mathbb{Q} = -\alpha - [x_\infty - \alpha]$. For uniqueness, suppose there exists $q' \in \mathbb{Q}$ and $d' \in D$ such that $x + \iota(q) = d'$. This implies that $\iota(q - q') = d - d'$. However, this implies that $q - q' \in \mathbb{Q}$ is p-adic integer for all non-archimedean places p, and therefore it must be an integer. Similarly, we have that $-1 < q - q' < 1$ at the archimedean places. Combining, this forces $q - q' = d - d' = 0$, as desired. □

Theorem 4.53. *Let K be a number field. Then the quotient $\mathbb{A}_K/\iota_K(K)$ equipped with the quotient topology (where $\iota_K(K)$ has the discrete topology in light of 4.48) is compact.*

Proof. Using Corollary 4.50, we may reduce to the case where $K = \mathbb{Q}$ then we have that $\mathbb{A}/\iota(\mathbb{Q})$ identifies with the topological group

$$S^1 \times \prod_p \mathbb{Z}_p,$$

where S^1 is the circle viewed as the quotient space $[0,1]/(0 \sim 1)$ of the interval with its points identified and is equipped with the additive group structure. By Tychonoff, this is clearly a compact topological space. □

Remark 4.54. Perhaps more transparently, we see that by combining the proof of Theorem 4.53 with Corollary 4.50 that we obtain for a number field $K/\mathbb{Q}$ of degree n, an isomorphism of topological groups

$$\mathbb{A}_K/\iota_K(K) \simeq (S^1)^n \times \prod_{\mathfrak{p}} \mathcal{O}_{K_\mathfrak{p}},$$

where the product ranges over prime ideals, which is clearly a compact topological space by Tychonoff.

This has the following very beautiful consequence.

Exercise 4.55. *Recall the Potryagin duality functor $(-)^\vee$ from Exercise 2.6. Let $K/\mathbb{Q}$ be a number field. Show the following.*

(1) Show that we have an isomorphism

$$(\mathbb{A}/\iota(\mathbb{Q}))^\vee \simeq \mathbb{Q}$$

of abelain groups (Hint: use the explicit description of the LHS provided in class and embed $\mathbb{Q}/\mathbb{Z}$ into S^1 as nth roots of unity).

(2) Use Part (1) and Lemma 4.49, to show that we have an isomorphism

$$(\mathbb{A}_K/\iota_K(K))^\vee \simeq K$$

of abelian groups.

We now want to think of $\mathbb{A}_K/\iota_K(K)$ as a topological space with finite volume. To make this precise, we discuss the notion of a Haar measure.

4.2.2. *Aside on Haar Measures.* Let G be a locally compact Hausdorff topological group. We recall that σ-algebra on G is a collection of subsets of G closed under complement, countable unions, and intersections. We can consider the σ-algebra generated by the open subsets. This is known as the Borel algebra of G, which we will denote by Σ. We refer to an element $S \in \Sigma$ as a Borel set. We may form the left and right translates gS and Sg. We now have the following fundamental result of Haar.

Theorem 4.56. ***(Haar's Theorem)*** *For G any locally compact topological group, there exists a unique (up to positive multiplicative constant) measure (See Remark 4.57) $\mu : \Sigma \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ satisfying the following.*

(1) The measure μ is left-translation invariant $\mu(gS) = \mu(S)$.

(2) The measure μ is finite on every compact set $K \in \Sigma$.

(3) The measure μ is outer regular. In particular, we have that

$$\mu(S) := \inf_U \{\mu(U) | S \subset U, U \subset G \text{ open }\}.$$

(4) The measure μ is inner regular. In particular, for all open subests $U \subset G$, we have that

$$\mu(U) = \sup_K \{\mu(K) | K \subset U, K \text{ compact }\}.$$

This is referred to as a left Haar measure.

Remark 4.57. Recall that a measure $\mu : \Sigma \to \mathbb{R}_{>0} \cup \{\infty\}$ is a function such that

(1) $\mu(\emptyset) = 0$

(2) For all countable collections of sets $\{E_k\}_{k=1}^\infty$ of pairwise disjoint sets in Σ, we have countable additivity. Namely, that

$$\mu(\bigcup_{k=1}^\infty E_k) = \sum_{k=1}^\infty \mu(E_k).$$

Remark 4.58. Similarly, by insisting on right-translation invariance we obtain right Haar measures. If G is commutative then these obviously agree and we refer to the output of this Theorem just as a Haar measure, but in general they are different.

We may apply Theorem 4.56 to obtain the following.

Construction 4.59. *For $K/\mathbb{Q}$ a number field of degree n, we consider the additive group $(\mathbb{A}_K, +)$. This is a locally compact Hausdorff topological group (Remark 4.41). In particular, it has a unique Haar measure μ_K by Theorem 4.56 up to a positive multiplicative constant We fix a more precise choice of μ_K as follows.*

1. *For each place v of K, we fix a Haar measure (μ_v, K_v) on the locally compact Hausdorff group $(K_v, +)$ normalized as follows.*
   - (a) *If v is non-archimedean μ_v is a Haar measure on $(K_v, +)$ such that $\mu_v(\mathcal{O}_v) = 1$*
   - (b) *If v is archimedean and real $\mu_v(-) = \mu_{\mathbb{R}}(-)$, where $\mu_{\mathbb{R}}$ is the Lebesgue measure on $\mathbb{R}$. In particular, $\mu_v([0,1]) = 1$.*
   - (c) *If v is non-archimedean and complex $\mu_v(-) = 2\mu_{\mathbb{C}}(-)$ where $\mu_{\mathbb{C}}(-)$ is the Lesbegue measure on $\mathbb{C} \simeq \mathbb{R}^2$. Note that this is compatible with the choice of measure on $K_{\mathbb{R}} \to K_{\mathbb{C}}$ induced by the inner products in Definition 4.37 (5).*
2. *We note that the Borel algebra of $\mathbb{A}_K$ is generated by products $\prod_v B_v$, where $B_v = \mathcal{O}_v$ for all but finitely many v and $\mu_v(B_v) < \infty$ for all v. In particular, we may define a measure μ_K on $\mathbb{A}_K$ by the formula:*

$$\mu_K(\prod_v B_v) = \prod_v \mu_v(B_v),$$

where the RHS converges by virtue of the fact that $\mu_v(\mathcal{O}_v) = 1$ if v is non-archimedean. This is easily verified to be a Haar measure since μ_v for all v is a Haar measure.

Remark 4.60. Let's consider the Haar measure μ_p on $\mathbb{Q}_p$, as in the above the construction, and take $a \in \mathbb{Q}_p$. We note that $\mu_p(a \cdot (-))$ is also easily checked to be a Haar measure. In particular, by the uniqueness part of Theorem 4.56, we have an equality

$$c_a \mu_p(-) = \mu_p(a \cdot (-))$$

for some non-zero constant $c_a \in \mathbb{R}_{>0}$. Suppose that $a = p^k a_u$ for some $a_u \in \mathbb{Z}_p^*$ and $k \geq 0$ and evaluate the previous equation on the compact open subset $\mathbb{Z}_p \subset \mathbb{Q}_p$. Then we obtain

$$c_a = c_a \mu_p(\mathbb{Z}_p) = \mu(a\mathbb{Z}_p) = \mu(p^k \mathbb{Z}_p),$$

where we have used that $\mu_p(\mathbb{Z}_p) = 1$ by the given choice of normalization. However, now we note that we have

$$\mathbb{Z}_p = \sqcup_{i=0}^{p^k - 1} i + p^k \mathbb{Z}_p.$$

In particular, by the countable additivity of the measure (Remark 4.57) and the translation invariance of the Haar measure this implies that

$$1 = \mu(\mathbb{Z}_p) = p^k \mu(p^k \mathbb{Z}_p),$$

so that $\mu(p^k \mathbb{Z}_p) = p^{-k}$. In other words, $c_a = |a|_p$ and we have that

$$\mu_p(a \cdot (-)) = |a|_p \mu_p(-).$$

Similarly, for v any place of a number field K, and $a_v \in K_v$, one may verify by similar arguments that

$$\mu_v(a_v \cdot (-)) = |a_v|_v \mu_v(-).$$

In turn, by construction of the measure μ_K as a product of the μ_v, one then deduces for any $a = (a_v) \in \mathbb{A}_K$, one has an identity

$$\mu_K(a \cdot (-)) = |a|_K \mu_K(-), \tag{4.25}$$

where $|\cdot|_K$ is the norm constructed in Definition 4.44.

4.2.3. *Strong Approximation on the Adeles.* We can use Theorem 4.53 together with the Haar measure of Construction 4.59 to deduce a "strong approximation result" that will be useful for our incoming study of the ideles.

Proposition 4.61. ***(Strong Approximation for the Adeles)*** *Let $K/\mathbb{Q}$ be a number field. There then exists a positive constant $B_K > 0$ such that, for any $a \in \mathbb{A}_K$ with $|a|_K > B_K$, there exists a nonzero principal adele $x \in K^* \subset \mathbb{A}_K$ for which $|x|_v \leq |a|_v$ for all places v of K.*

Proof. We let b_0 be the measure of the fundamental region of $\mathbb{A}_K/K$ under the Haar measure of Construction 4.59. This is finite by virtue of the fact that the quotient $\mathbb{A}_K/K$ is compact (Theorem 4.53) the measure μ_K is finite on compact subsets and translation invariant (Theorem 4.56 (1)-(2)). Now we define

$$b_1 := \mu_K(\{z \in \mathbb{A}_K \mid |z|_v \leq 1 \text{ for all } v \text{ and } |z|_v \leq \frac{1}{4} \text{ if } v \text{ is archimedean}\}). \tag{4.26}$$

Then, by construction of μ_K (Construction 4.59), this will be finite since there are only finitely many archimedean places. We then set $B_K := b_0/b_1$ to be the desired constant. Suppose $a \in A_K$ satisfies $|a|_K > B_K$. We consider now the subset

$$T := \{t \in \mathbb{A}_K \mid |t|_v \leq |a|_v \text{ for all } v \text{ and } |t|_v \leq \frac{1}{4}|a|_v \text{ if } v \text{ is archimedean }\},$$

which we note is just given by multiplying the set appearing on the RHS (4.26) by a. In particular, in light of Remark 4.60, we have the following inequality.

$$\mu(T) = b_1|a|_K > b_1 B_K = b_0$$

Since $\mu(T) > b_0$, the set T is not contained in the fundamental region of $\mathbb{A}_K/K$ by countable additivity of the measure. In particular, there must be distinct $t_1, t_2 \in T$ with the same image in $\mathbb{A}_K/K$. In other words, $x := t_1 - t_2$ is a nonzero element of $K \subset \mathbb{A}_K$. By definition of T, we have that

$$|t_1 - t_2|_v \leq \max(|t_1|_v, |t_2|_v) \leq |a|_v$$

if v is non-archimedean by the ultrametric inequality. Moreover, we have that

$$|t_1 - t_2|_v \leq |t_1|_v + |t_2|_v \leq 2\frac{1}{4}|a|_v \leq |a|_v$$

if v is real archimedean by the triangle inequality, and

$$|t_1 - t_2|_v \leq 2|t_1|_v + 2|t_2|_v \leq 4\frac{1}{4}|a|_v \leq |a|_v,$$

if v is complex (Recall that we defined the norm at a complex place (4.44) to be twice the usual norm). In particular, $|x|_v \leq |a|_v$ for all places v of K, as desired. □

4.2.4. *The Structure of the Ideles.* As already discussed, while the adeles are very nice, for actual class field theory we will be more interested in the multiplicative notion (i.e the ideles introduced in 4.42). We may attempt to perform a similar kind of analysis now for the quotient $\mathbb{I}_K/\iota_K(K^*)$ and conjecture that $\iota_K(K^*)$ is a lattice. The first indication of this is the following.

Remark 4.62. It is easy to see that $\iota_K(K^*) \subset K^*$ is a discrete subgroup, by using Exercise 4.48, together with the fact that the map $\mathbb{I}_K \to \mathbb{A}_K$ is continuous (Exercise 4.43 (2)) and that the preimage of $\iota_K(K)$ under this map is $\iota_K(K^*)$. Indeed, note that to show it is discrete one simply needs to exhibit an open subset of $\mathbb{I}_K$ with trivial intersection with K^*.

However, the problem is that the quotient $\mathbb{I}_K/\iota_K(K^*)$ is not compact, so even though $\iota_K(K^*) \subset \mathbb{I}_K$ is discrete it is not a lattice. Indeed, we have the following.

Exercise 4.63. *Show that a fundamental domain for $\mathbb{I}/\iota(\mathbb{Q}^*)$ is given by*

$$D^* := \mathbb{R}_{>0} \times \prod_p \mathbb{Z}_p^*.$$

(Hint: follow the basic structure of the analogous proof for the adeles; however, note that the analogue of weak approximation is very easy in this case!).

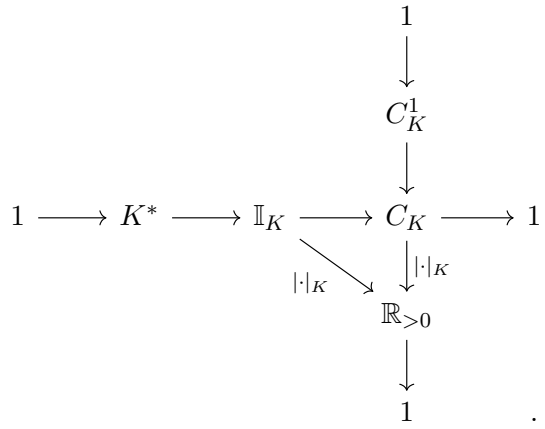
In particular, if we want to see a comapct topological group that will match up with the Galois group of the maximal abelain extension, we need to fix this. To do this, we first fix some notation.

Definition 4.64. We define the following.

(1) We define the idele class group $C_K := \mathbb{I}_K/\iota_K(K^*)$. We note, by Proposition 4.47, that the norm map $|\cdot|_K$ factors through the quotient $\mathbb{I}_K \to C_K$ and in turn defines a map

$$|\cdot|_K : C_K \to \mathbb{R}_{>0}. \tag{4.27}$$

(2) We define $C_K^1 \subset C_K$ to be the kernel of (4.27) and equip it with the subspace topology. By definition, it sits in the following diagram of exact sequences

(4.28)


Similarly, we define $\mathbb{I}_K^1 \subset \mathbb{I}_K$ to be the kernel of $|\cdot|_K : \mathbb{I}_K \to \mathbb{R}_{>0}$ so that $C_K^1 \simeq \mathbb{I}_K^1/K^*$.

Let's give some flavor for this object.

Example 4.65. We note that the composition of

$$D^* \to \mathbb{I} \xrightarrow{|\cdot|_K} \mathbb{R}_{>0}$$

identifies simply with the projection

$$D^* = \mathbb{R}_{>0} \times \prod_p \mathbb{Z}_p^* \to \mathbb{R}_{>0},$$

by virtue of the fact that the p-adic valuation of every element in $\mathbb{Z}_p^*$ is 1. In particular, in light of Exercise 4.63, we deduce an isomorphism

$$C_K^1 \simeq \prod_p \mathbb{Z}_p^*.$$

We note that, by Theorem 1.10, this also identifies with

$$C_K^1 \simeq \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}).$$

In particular, this is seeing precisely the kind of groups that we want to see in global class field theory!

As the previous example suggests, we have the following.

Theorem 4.66. *The group $C_K^1 := \mathbb{I}_K^1/K^*$ equipped with its natural quotient topology is compact.*

Proof. We first show the following Lemma.

Lemma 4.67. *The group $\mathbb{I}_K^1 \subset \mathbb{A}_K$ is a closed subspace. In particular, since the map $\mathbb{I}_K \to \mathbb{A}_K$ is continuous (4.43 (2)), $\mathbb{I}_K^1$ is closed in $\mathbb{I}_K$ as well. Moreover, the subspace topology on $\mathbb{I}_K^1$ induced from the inclusions into $\mathbb{I}_K$ and $\mathbb{A}_K$ agree.*

Proof. Consider any $x \in \mathbb{A}_K \setminus \mathbb{I}_K^1$. It suffices to construct an open neighborhood U_x of x in $\mathbb{A}_K$ that is disjoint from $\mathbb{I}_K^1$. For any finite set of places S of K, any $x \in \mathbb{A}_K$, and a tuple $\varepsilon > 0$, we define

$$U_\varepsilon(x, S) := \{u \in \mathbb{A}_K \mid |u - x|_v < \varepsilon \text{ for } v \in S \text{ and } |u|_v \leq 1 \text{ for } v \notin S\} \tag{4.29}$$

which is a basis of open neighborhoods of x in $\mathbb{A}_K$. By the assumption that $|x|_K \neq 1$, there are two cases.

Case 1: $|x|_K < 1$

By the assumption that $|x| < 1$ and that $|x|_v \leq 1$ for all but finitely many v, we may find a suitably large finite set S of places of K containing the archimedean places and all v for which $|x|_v > 1$ and such that $\prod_{v \in S} |x|_v < 1$.

By taking ε to be sufficiently small, we claim that the set $U_x := U_\varepsilon(x, S)$ is disjoint from $\mathbb{I}_K^1$. This is because every $y \in U_x$ must satisfy $|y|_K \leq \prod_{v \in S} |y|_v$, by definition of $U_\varepsilon(x, S)$, and, by choosing ε sufficiently small, we can make the difference between $\prod_{v \in S} |y|_v$ and $\prod_{v \in S} |x|_v < 1$ arbitrarily small guaranteeing that $|y|_K \leq \prod_{v \in S} |y|_v < 1$ (e.g via the triangle inequality $|y|_v = |y - x + x|_v \leq |x - y|_v + |x|_v$ and taking the product over all $v \in S$).

Case 2: $|x|_K > 1$

Let B be twice the product of the finitely many $|x|_v > 1$. Let S be the finite set containing the archimedean places of K and all non-archimedean v with residue field cardinality less than $2B$ and all v for which $|x|_v > 1$. By choosing ε to be sufficiently small, we claim that $U_x = U_\varepsilon(x, S)$ is an open neighborhood of x disjoint from $\mathbb{I}_K^1$. This follows, since for every $y \in U_x$, either $|y|_v = 1$ for all $v \notin S$ in which case we may arrange that $|y|_K = \prod_{v \in S} |y|_v > 1$ (e.g by using the triangle inequality in the form $|y|_v \geq |x|_v - |x - y|_v$ and taking the product over all v). Otherwise, there exists $v \in S$ such that $|y|_v < 1$ for some $v \notin S$ and this implies that $|y|_v < \frac{1}{2B}$ since v is nonarchimedean and does not include those with valuations with residue field less than $2B$. By choosing $\varepsilon > 0$ sufficiently small, we may conclude that $|y|_K \leq \frac{1}{2B} \prod_{v \in S} |y|_v \leq \frac{1}{2B} 2|x|_K = \frac{1}{2} < 1$, giving the desired claim.

It remains to show the claim that the subspace topologies agree. Given $x \in \mathbb{I}_K^1$, a basis of open neighborhoods in $\mathbb{I}_K$ is given by

$$V_\varepsilon(x, S) := \{u \in \mathbb{A}_K | |u - x|_v < \varepsilon \text{ for } v \in S \text{ and } |u|_v \leq 1 \text{ for } v \notin S\}$$

for $\varepsilon > 0$ sufficiently small and S any sufficiently large finite set of finite places. We need to show that we can arrange that $V_\varepsilon(x, S) \cap \mathbb{I}_K^1 = \mathbb{I}_K^1 \cap U_\epsilon(x, S)$ for $\varepsilon > 0$ and S any sufficiently large finite set of finite places. However, this can be arranged by choosing S so that it contains all the archimedean places and the finitely many non-archimedean places such that $|x|_v \neq 1$. In this case, we may arrange that $u \in \mathbb{I}_K^1 \cap U_\varepsilon(x, S)$ automatically satisfies $|u|_v = 1$ for all $v \notin S$ and $\varepsilon > 0$ sufficiently small, so that $\mathbb{I}_K^1 \cap U_\varepsilon(x, S) = \mathbb{I}_K^1 \cap V_\varepsilon(x, S)$, as desired. □

To prove that C_K^1 is compact, it suffices to exhibit a compact set $W \subset \mathbb{A}_K$ for which $W \cap \mathbb{I}_K^1$ surjects onto C_K^1. In particular, this follows by the Lemma. The inclusion $\mathbb{I}_K^1 \subset \mathbb{A}_K$ is closed so that the intersection $W \cap \mathbb{I}_K^1$ is closed in the compact W, and therefore also compact with respect to the subspace topology coming from $\mathbb{A}_K$ and in turn the subspace topology coming from $\mathbb{I}_K$ again by the Lemma. To construct W, we first choose $a \in A_K$ such that $|a| > B_K$, where B_K is as in Proposition 4.61 and let

$$W = \{x \in \mathbb{A}_K \mid |x|_v \leq |a|_v \text{ for all places } v \text{ of } K\}.$$

Now consider any $u \in \mathbb{I}_K^1$, we have that $|u|_K = 1$ so $|\frac{a}{u}|_K = |a|_K > B_K$. By Proposition 4.61, there exists $x \in K^* \subset \mathbb{A}_K$ for which $|x|_v \leq |\frac{a}{u}|_v$ for all places v. Therefore, $xu \in L(a)$. Thus, every $u \in \mathbb{I}_K^1$ can be written as $u = x^{-1}xu$ with $x^{-1} \in K^*$ and $xu \in W \cap \mathbb{I}_K^1$. Thus $W \cap \mathbb{I}_K^1$ is the desired set. □

While we arrived at Theorem 4.66 by formal considerations involving point-set topology and abstract measure theory on topological groups, it actually captures a tremendous amount of information. To get at this, we first recall the following.

Definition 4.68. We define the following.

(1) We write I_K for the set of fractional ideals of K. In other words, it is the subset of $I \subset K$ of non-zero $\mathcal{O}_K$-submodules of K such that there exists a non-zero $d \in \mathcal{O}_K$ such that $dI \subset \mathcal{O}_K$ is an ideal of $\mathcal{O}_K$. We endow this with the group structure given by taking the product (I, J) of the $\mathcal{O}_K$-submodules inside K.
(2) We write $P_K \subset I_K$ for the subgroup of principal fractional ideals. I.e those generated by a single element $a \in K^*$.
(3) We write $\mathrm{Cl}(K) := P_K/I_K$ for the quotient group and refer to it as the class group of K.

We now note that there is a natural homomorphism

$$\mathbb{I}_{K,f} \to I_K$$
$$(x_\mathfrak{p})_\mathfrak{p} \mapsto \prod_p \mathfrak{p}^{v_\mathfrak{p}(x_\mathfrak{p})},$$

which, by precomposing with the natural projection $\mathbb{I}_K \to \mathbb{I}_{K,f}$, induces a natural map

$$\mathbb{I}_K \to I_K, \tag{4.30}$$

which will send $K^* \subset \mathbb{I}_K$ to P_K. In particular, this fits into a map of short exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^* & \xrightarrow{\iota_K} & \mathbb{I}_K & \longrightarrow & C_K & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & P_K & \longrightarrow & I_K & \longrightarrow & \mathrm{Cl}(K) & \longrightarrow & 1 \end{array} \tag{4.31}$$

Remark 4.69. We note that, by prime factorization of fraction ideals the map (4.30), is surjective. Moreover, it is continuous with respect to the discrete topology on I_K, by noting that the $\pi_v^n \mathcal{O}_v^*$ for all $n \in \mathbb{Z}$ is an open subset of K_v^*. Moreover, by construction, the subgroup $K_\mathbb{R}^* \subset \mathbb{I}_K$ (i.e the contribution from the infinite places) lies in the kernel.

Similarly, $K^* \to P_K$ is surjective and $K^* \subset \mathbb{I}_K$ is a discrete subgroup by Remark 4.62. In particular, it follows that the map

$$C_K \to \mathrm{Cl}(K) \tag{4.32}$$

appearing in (4.32) is a continous surjection where the source has the quotient topology and the target has the discrete topology.

This gives us the following familiar consequence of Theorem 4.53.

Corollary 4.70. ***(Finiteness of Class Number)*** *For $K/\mathbb{Q}$ a number field of degree n, the class group $\mathrm{Cl}(K)$ is finite.*

Proof. As noted in Remark 4.69, the map $C_K \to \mathrm{Cl}(K)$ is continous and surjective where the target has the discrete topology. Moreover, its precomposition with $\mathbb{I}_K \to C_K$ has $K_\mathbb{R}$ inside the kernel. Up to scaling an element in $\mathbb{I}_K$ by an appropriate element inside $K_\mathbb{R}$ we can always arrange that it lies in $\mathbb{I}_K^1$ (cf. Example 4.65). In particular, it follows that the map

$$C_K^1 := \mathbb{I}_K^1/\iota_K(K^*) \to \mathrm{Cl}(K)$$

is also surjective where the target has the quotient topology and the target has the discrete topology. However, if $\mathrm{Cl}(K)$ were infinite, then by taking the preimage along this map we could exhibit an infinite open covering of C_K^1 by disjoint sets, which would contradict the compactness of C_K^1 (Theorem 4.66). □

In particular, one of the main finiteness results of algebraic number theory is encoded in the compactness of C_K^1. Remarkably, the the same is true of the other major finiteness theorem; namely, Dirchlet's unit theorem.

Corollary 4.71. ***(Dirichlet's Unit Theorem)*** *Let $K/\mathbb{Q}$ be a number field and let S denote the set of archimedean places of K. Then we have a short exact sequence*

$$0 \to \mu_K \to \mathcal{O}_K^* \to \mathbb{Z}^{|S|-1} \to 0,$$

where μ_K is the finite cyclic group of roots of unity of K. In particular, recalling the definition of the archimedean places (Definition 4.37 (2)) we have that $|S| = r + s$, where r is the number of real places and s is the number of complex places, and we conclude the ring of units $\mathcal{O}_K^*$ is generated up to torsion by $r + s - 1$ elements.

Proof. We consider the surjective map

$$\log : \mathbb{I}_{K,S} \to \mathbb{R}^{|S|}, \tag{4.33}$$

by taking the log of the absolute value on the norm of each archimedean component defined by a place $v \in S$. This carries $\mathcal{O}_K^* \subset \mathbb{I}_{K,S}$ into the trace zero hyperplane H in $\mathbb{R}^{|S|}$ by the product formula (Proposition 4.47). It is easy to check that any element of $\mathcal{O}_K^*$ with trivial norm at all infinite places must be root of unity (See [Mil20b, Corollary 5.6]), and therefore the kernel of

$$\mathcal{O}_K^* \to H$$

is equal to μ_K (This is sometimes known as Kronecker's Theorem). To show the desired claim, it therefore suffices to show that if W is the span of the image of $\mathcal{O}_K^*$ in H_S it is equal to H. Indeed, this will imply $\mathcal{O}_K^*$ is a lattice in H and has rank equal to $\dim(H) = |S| - 1$. We note that we have a continuous (since the norm and logarithm maps are continuous) and surjective (note by definition $\mathbb{I}_{K,S}^1$ is just the preimage of H_S under (4.33)) map

$$\mathbb{I}_{K,S}^1/\iota_K(\mathcal{O}_K^*) \to H/W, \tag{4.34}$$

and it suffices to show it is zero. The obvious open inclusion $\mathbb{I}_{K,S} \subset \mathbb{I}_K$ restricts to an open inclusion $\mathbb{I}_{K,S}^1 \subset \mathbb{I}_K^1$ on the norm one parts, and therefore we get an open inclusion of subgroups

$$\mathbb{I}_{K,S}^1/\iota_K(\mathcal{O}_K^*) = \mathbb{I}_{K,S}^1/\iota_K(K^* \cap \mathbb{I}_{K,S}^1) \hookrightarrow \mathbb{I}_K^1/\iota_K(K^*) = C_K^1$$

(Recall that for quotients of topological groups by topological subgroups, the quotient map is open). Since this is the open inclusion of a subgroup it is also closed (by arguing as in 2.8), and therefore since C_K^1 is compact by Theorem 4.66. it follows that $\mathbb{I}_{K,S}^1/\iota_K(\mathcal{O}_{K,S}^*)$ is compact. Therefore, (4.34) is a continuous surjection of compact group onto some copies of the real line. This must be 0, since otherwise we would arrive at a contradiction. □

We have now come full circle. Indeed, we started by introducing the adeles and ideles, as some way of approximating the topological group given by the Galois group of the maximal abelian extension. Using our knowledge that the Galois group of the maximal abelian extension were compact Hausdorff, we sought to modify it by quotienting out by certain lattices namely $\iota_K(K)$ and $\iota_{K^*}(K^*)$ partially motivated by Minkowski Theory (Remark 4.39), and, at the end, we have built a machine sophisticated enough to capture the basic theorems of algebraic number theory. With the significance of these objects now illuminated, we turn to a cohomological analysis of these objects and isolate the most important inputs for the proof of global class field theory.

References

[CF10] J. W. S. Cassels and A. Fröhlich, eds. *Algebraic number theory*. Papers from the conference held at the University of Sussex, Brighton, September 1–17, 1965, Including a list of errata. London Mathematical Society, London, 2010, pp. xxiv + 366. ISBN: 978-0-95027-342-6.

[Ked] Kiran Kedlaya. "Sheaves, Stacks, and Shtukas". In: *Online Notes* (). Arizona Winter School Notes.

[Ked02] Kiran S. Kedlaya. *Notes on Class Field Theory*. `https://kskedlaya.org/cft/preface-1.html`. Lecture notes, revised version available online. 2002.

[Mil20a] J.S. Milne. *Class Field Theory (v4.03)*. Available at www.jmilne.org/math/. 2020.

[Mil20b] James S. Milne. *Algebraic Number Theory (v3.08)*. Available at `https://www.jmilne.org/math/CourseNotes/ANT.pdf`. Online course notes, University of Michigan, 2020.

[Neu99] Jürgen Neukirch. *Algebraic number theory*. Vol. 322. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. Springer-Verlag, Berlin, 1999, pp. xviii+571. ISBN: 3-540-65399-6. DOI: `10.1007/978-3-662-03983-0`. URL: `https://doi-org.ezp-prod1.hul.harvard.edu/10.1007/978-3-662-03983-0`.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*. 2nd ed. Vol. 323. Grundlehren der mathematischen Wissenschaften. Berlin, Heidelberg: Springer, 2008. ISBN: 978-3-540-37888-4.

[Ser94] Jean-Pierre Serre. *Cohomologie galoisienne*. Fifth. Vol. 5. Lecture Notes in Mathematics. Springer-Verlag, Berlin, 1994, pp. x+181. ISBN: 3-540-58002-6. DOI: `10.1007/BFb0108758`. URL: `https://doi.org/10.1007/BFb0108758`.

[Wei80] Claudia Weill. *It's My Turn*. Motion picture. 1980.