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 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} = \langle -1 \rangle$, 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 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \simeq (\mathbb{Z}/q\mathbb{Z})^*$, 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 $\mathrm{Gal}(L/\mathbb{Q}) \rightarrow \mathrm{Gal}(L'/\mathbb{Q})$. 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 $i = 1, \dots, g$, 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

$$[L : K] = e\,f\,g.$$

(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*

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

  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* 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*

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

(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* 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*

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

(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 2.12).*

(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

$$\widehat{\mathbb{Z}}^{\times} \simeq \prod_{q} \mathbb{Z}_q^{*}, \tag{1.7}$$

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,

$$\mathrm{Gal}(\mathbb{Q}^{S,\mathrm{ab}}/\mathbb{Q}) \;\cong\; \prod_{q\in S} \mathbb{Z}_q^{\times}, \tag{1.8}$$

under the identification of (1.7).

(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; Mil20]

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

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

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 1.8 (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

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

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 $H_{i,\text{cont}}(G, \mathbb{Z})$ 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 $H_1^{\text{cont}}(G, \mathbb{Z})$ 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.

($\Rightarrow$) 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 Potryagin 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 2.17) 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 pro-finite G. Then the following is true.*

1. *If $H \subset G$ is an open subgroup then it is also closed.*
2. *If $H \subset G$ is a closed subgroup then H is also profinite.*

Proof. For (1) is an easy consequence of the fact that since G is compact any open H is of finite index. In particular, we can write H as the complement of its finitely many non-trivial translates implying it is closed.

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. □

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

Proposition 2.9. *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 2.10. *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 2.10 $G/(S \cap U) \to G/S$ 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 2.11. 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 2.12. *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 2.13. *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 $A_{j_1k_1}, \dots, A_{j_rk_r}$ 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 $A_{j_1k_1} \cap \cdots \cap A_{j_rk_r}$, 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 2.13 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 2.13 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 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 2.14. 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 2.15. *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 2.16. ***(Snake Lemma)*** *Consider a commutative diagram of abelian groups with exact rows:*

$$\begin{tikzcd} & A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' & \end{tikzcd} \tag{2.5}$$

Then there exists a connecting homomorphism

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

such that the following sequence is exact:

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

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 $c \in \mathrm{Ker}(\gamma) \subset C$ 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 $c \in \mathrm{Ker}(\gamma)$, this element will vanish upon applying g' and therefore lie in $\mathrm{Im}(f')$ (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 2.16 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 2.17. An object $M \in \mathrm{Mod}_G$ is said to be *injective* if, for every commutative diagram

$$\begin{tikzcd}
A \arrow[r, "\phi"] \arrow[d, "i"] & M \\
B & ,
\end{tikzcd}$$

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 2.18. 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 2.17, we note that injectivity allows us to deduce the existence of a splitting

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "i"] & B \arrow[r] \arrow[l, bend left, "s"] & C \arrow[r] & 0
\end{tikzcd}$$

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

$$\begin{tikzcd}
0 \arrow[r] & A^G \arrow[r, "i^G"] & B^G \arrow[r] \arrow[l, bend left, "s^G"] & C^G
\end{tikzcd}$$

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 2.16. We now have the following basic fact which tells us that we can always do this.

Exercise 2.19. *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 2.20. 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 2.17. We note that the existence of such a resolution is guaranteed by iteratively applying Exercise 2.19. 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 2.21. 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 2.17, 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

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r] \arrow[d, "f"] & I^0 \arrow[r, "d^0"] \arrow[d, "f^0"] & I^1 \arrow[r, "d^1"] \arrow[d, "f^1"] & \cdots \\ 0 \arrow[r] & N \arrow[r] & J^0 \arrow[r, "d^0"] & J^1 \arrow[r, "d^1"] & \cdots \end{tikzcd} \tag{2.8}$$

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 2.22. *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 2.23 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 2.23. *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*

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d, "f"] & I^0 \arrow[r, "d^0"] \arrow[d, "f^0"] & I^1 \arrow[r, "d^1"] \arrow[d, "f^1"] & \cdots \\
0 \arrow[r] & N \arrow[r] & J^0 \arrow[r, "d^0"] & J^1 \arrow[r, "d^1"] & \cdots
\end{tikzcd}$$

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 2.24. *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 2.22 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 2.16.

Proposition 2.25. *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 2.26. 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 2.27. *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 2.28. 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 2.14.

(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 2.29. 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 2.30.

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

Proposition 2.31. ***(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 2.29. 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 2.29, 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. □

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 2.32. *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

$$\begin{tikzcd} & 0 \arrow[d] \\ A \arrow[r, "f"] & B \end{tikzcd}$$

and the cokernel is the colimit with respect to the diagram

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d] & B \\ 0 & \end{tikzcd}$$

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 2.32, we deduce the following Corollary of Proposition 2.31.

Corollary 2.33. *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 2.34. *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 2.18 with Proposition 2.31. □

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 2.35. *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 2.34 and 2.33, 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 2.29. 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 2.36. 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 2.37. 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 2.35 and the fact that $H^i(\{e\}, M) = 0$ tautologically for any $i > 0$.

Corollary 2.38. *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 2.38 and 2.27 (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 2.39. *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)

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

Remark 2.40. 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

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

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 2.27 (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 $C^n(G,M)^G$ 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 2.41. Using Exercise 2.27 and in particular Exercise 2.27 (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 2.42. 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

(2.17)
$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d, "\mathrm{id}_M"] & E \arrow[r, "\pi"] \arrow[d] & G \arrow[r] \arrow[d, "\mathrm{id}_G"] & 1 \\
0 \arrow[r] & M \arrow[r] & E' \arrow[r, "\pi'"] & G \arrow[r] & 1.
\end{tikzcd}$$

We note (e.g by the Snake Lemma (Lemma 2.16)) 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 2.9). 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 2.43. *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

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d, "\mathrm{id}_M"] & E \arrow[r] \arrow[d, "\alpha"] & G \arrow[r] \arrow[d, "\mathrm{id}_G"] & 1 \\
0 \arrow[r] & M \arrow[r] & E' \arrow[r] & G \arrow[r] & 1.
\end{tikzcd}$$

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 2.44. ***(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 2.45. *Let $\sigma_1, \dots, \sigma_n$ be distinct automorphisms of a field E. Then if $c_1, \dots, c_n \in E$ 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 2.41 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 2.45,

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

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 2.46. *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 2.41, that one has $H^1(\mathrm{Gal}(L/K), L) = 0$ (Hint: Your replacement for Lemma 2.45 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 2.46 and Theorem 2.44, 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 2.47. 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 2.48. 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 2.49. ***(Wedderburn's Theorem)*** *Let A be a finite dimensional central simple algebra over k then there exists $n \geq 1$ and a finite dimensional divsion 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 2.50 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 2.50. *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 [Mil20, 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 2.51. (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 the 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 2.52. *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 the 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 2.53. *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 2.53.*

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 2.53 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 2.54. 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 2.49). 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 2.55. 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 2.49), 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 the maximal commutative subfield $L \hookrightarrow D$ (cf. Exercise 2.52 (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 2.56. *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 2.51 (3).

Example 2.57. 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

$$A \otimes_K L \simeq M_n(L)$$

[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 2.51 (3)!

(cf. Exercise 2.52 (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

$$(L/K, \phi) \simeq (L/K, \phi')$$

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 2.58. *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 2.59. ***(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 [Mil20, Theorem 2.10]. □

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

We now start with a class in $\mathrm{Br}(L/K)$. By Remark 2.55, 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 2.59, 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 2.59 tells us that we have a surjective map $\mathrm{GL}_n(L) \to \mathrm{Aut}_L(M_n(L))$ 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 2.25 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 2.60. 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 2.61. *Suppose we are in the situation of Definition 2.60 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

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

[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.

where M is regarded as a G'-module via the map $\alpha : G' \to G$. In terms of the description of cohomology given in 2.27 (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.

Example 2.62. Consider a subgroup $H \subset G$. We specialize (2.61) 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 2.31 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 2.35.

We similarly obtain the following dual notion, which comes from the alternative description of the restriction map in 2.62 using Schapiro's Lemma and the adjunction morphisms of Proposition 2.31.

Example 2.63. For M a G-module, we consider the natural map

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

given by Proposition 2.31. By Lemma 2.35, 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 2.64. 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_H^G. 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 2.37), and then looking at the induced map

$$\begin{tikzcd} I_0^H \arrow[r, "(d^0)^H"] \arrow[d, "\mathrm{Nm}_{G/H}"] & I_1^H \arrow[r, "(d^1)^H"] \arrow[d, "\mathrm{Nm}_{G/H}"] & \cdots \\ I_0^G \arrow[r, "(d^0)^G"] & I_1^G \arrow[r, "(d^1)^G"] & \cdots \end{tikzcd}$$

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

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

and considered the induced map on cohomology, which we easily verify is well-defined. One can indeed check this also agrees with CoRes_H^G 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.

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

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

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

Proof. We recall from the proof of Proposition 2.31 that the natural adjunction map

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

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

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

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

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

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 2.62 and 2.63, 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 2.66. *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 2.65 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

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

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

By combining this with Theorem 2.58, we have the following consequence, which is a priori not clear from the definition of the Brauer group (Definition 2.54) and its group structure (Exercise 2.56).

Corollary 2.67. *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.

We now leave off with one more important example of Construction 2.61.

Example 2.68. 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 2.61 yields a map

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

which is known as the inflation map.

These functors satisfy the following basic compatibilities with one another.

Proposition 2.69. *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*

$$\begin{tikzcd}
H^n(H/N, A^N) \arrow[r, "\mathrm{CoRes}_{H/N}^{G/N}"] \arrow[d, "\mathrm{Inf}_{H/N}^H"'] & H^n(G/N, A^N) \arrow[d, "\mathrm{Inf}_{G/N}^G"] \\
H^n(H, A) \arrow[r, "\mathrm{CoRes}_H^G"'] & H^n(G, A) .
\end{tikzcd}$$

commutes.

(2) *The diagram*

$$\begin{tikzcd}
H^n(H/N, A^N) \arrow[d, "\mathrm{Inf}_{H/N}^H"'] & H^n(G/N, A^N) \arrow[l, "\mathrm{Res}_{H/N}^{G/N}"] \arrow[d, "\mathrm{Inf}_{G/N}^G"] \\
H^n(H, A) & H^n(G, A) . \arrow[l, "\mathrm{Res}_H^G"']
\end{tikzcd}$$

commutes.

This one may check, by using that all the functors commute with the boundary maps δ_n, as alluded to in Example 2.62, and that the diagram commutes in the case of $n = 0$.

Exercise 2.70. *Show that Proposition 2.69 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 2.39. 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

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

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 2.71. 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 2.19. 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 2.39, 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 2.60. By applying the analogue of Construction 2.61, this gives rise to a directed system

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

We now have the following.

Lemma 2.72. *For $(G_i)_{i\in I}$ and $(M_i)_{i\in I}$ as above, we set $G := \varinjlim_{i\in I} G_i$ and $M = \varprojlim M_i$ 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

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

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 $M \in \text{Mod}_{G,\text{cont}}$, 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 2.68). In particular, we deduce the following from Lemma 2.72.

Corollary 2.73. *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 2.68.

This in particular tells us that we may express the cohomology of any $M \in \text{Mod}_{G,\text{cont}}$ 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 2.73 with Corollary 2.66.

Corollary 2.74. *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 2.11.

We also have the standard interpretations of these groups.

Example 2.75. As one can see directly from the definition (cf. Example 2.41), we have the following for $M \in \text{Mod}_{G,\text{cont}}$.

1. $H^0(G, M) \simeq M^G$ is the set of G-invariants
2. We have an identification
$$H^1(G, M) := \{\phi : G \to M \in C_{\text{cont}}(G, M) \mid h.\phi(g) - \phi(hg) + \phi(h) = 0\}/(\phi_m\ ,\ m \in M)$$
where $\phi_m(g) := g.m - m$.
3. If M is finite then, by arguing as in Example 2.42, 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 2.9.

(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

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

where the inverse limit is over finite Galois extensions L/K. Here the first isomorphism follows from Corollary 2.73, the second isomorphism is Theorem 2.58, 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 2.60. Just as in Construction 2.61, 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 2.76. 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 2.62.

We now turn to the corestriction map.

Example 2.77. Note that the construction in Example 2.63 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 2.64), 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 2.73, 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 2.63, 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 2.69 (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 2.69 (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 2.72, 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 2.65.

Lemma 2.78. *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 2.79. *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 2.12), 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 2.65. In general, we may write H as an intersection of open subgroups containing H and then use Lemma 2.72 to reduce the case of finite index as explained above. □

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

Exercise 2.80. *[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 2.29 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 2.81. 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

$$\mathrm{Hom}_G(M, \mathrm{coInd}_H^G(N)) \simeq \mathrm{Hom}_H(\mathrm{Res}_H^G(M), N), \tag{2.29}$$

for $M \in \mathrm{Mod}_{G,\mathrm{cont}}$ and $N \in \mathrm{Mod}_{H,\mathrm{cont}}$, by analogous argument the proof of Proposition 2.31 and the other induction operation Ind_H^G (which we don't define for simplicity) will satisfy the other adjunction relationship

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

of Proposition 2.31. If $H \subset G$ has finite index (e.g in the finite case of 2.31) then they agree by an analogous argument to Remark 2.29, and we recover a generalization of Proposition 2.31. However, only one of these functors will have the desired categorical properties required for Schapiro's Lemma.

Lemma 2.82. *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 (2.29) and the left exactness of the functor follows from Lemma 2.32 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 2.37)), which one can use to reverse the logic. □

In particular, now by the same argument as in 2.35, we deduce Schapiro's Lemma in the profinite case, where we recall we can argue using injective resolutions in the profinite case using Remark 2.71.

Lemma 2.83. *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 abelinization of profinite groups G^{ab} that we want to see.

References

[Mil20] J.S. Milne. *Class Field Theory (v4.03).* Available at www.jmilne.org/math/. 2020.

[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.