MATH 223B (GALOIS COHOMOLOGY AND CLASS FIELD THEORY)

LINUS HAMANN

Contents

1. Introduction

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

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

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

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

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

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

One of the basic reasons for wanting to understand the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is that it provides us information about the structure of solutions to the equation $p(x)$. E.g from Galois theory we know that if the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the solutions of $p(x)$ factors through a finite solvable group then the solutions can be computed in terms of the coefficients and radicals. In this way, the group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ together with its action on (1.1) provides some kind of systematic generalization for the notion of solvability of polynomial among radicals.

Another (perhaps more compelling reason) is that it is intimately related to many interesting arithmetic phenomena. For example, let's consider the polynomial $p(x) = x^2 - 5$ again. We may ask ourselves the following basic arithmetic question.

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

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

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

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

is defined for any integer a by

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1. *The extension $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ is Galois with Galois group isomorphic to $(\mathbb{Z}/q\mathbb{Z})^*$ via the mapping*
$$a \mapsto \sigma_a,$$
where $\sigma_a(\zeta_q) = \zeta_q^a$.
2. *The ring of integers of $\mathbb{Q}(\zeta_q)$ is given by $\mathbb{Z}[\zeta_q]$.*
3. *A prime p in $\mathbb{Z}$ is unramified in $\mathbb{Q}(\zeta_q)$ if and only if $p \neq q$.*
4. *If $q \neq p$ then by (1)-(3), we have a factorization as prime ideals $(p)\mathbb{Z}[\zeta_q] = \mathfrak{p}_1 \cdots \mathfrak{p}_g$, and for all $i = 1, \ldots, g$ that $\mathbb{Z}[\zeta_q]/\mathfrak{p}_i \simeq \mathbb{F}_{p^f}$ for some $f \geq 1$ such that*
$$gf = q - 1 \tag{1.4}$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(3) *Consider the reduction map*

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

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

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

(b) *Deduce a group homomorphism*

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

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

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

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

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

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

Deduce in particular that

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

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

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

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

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

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

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

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

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

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

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

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

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

(1) *Show that*

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

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

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

*(*Hint: *Compare discriminants.)*

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

(4) *Deduce that*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(1) *For all finite Galois extensions $K \subset L \subset K^S$, we fix an unramified prime $\mathfrak{P}(L)|\mathfrak{p}$ lying above $\mathfrak{p}$. We consider the conjugacy class of elements $[\mathrm{Frob}_{\mathfrak{p}}(\mathfrak{P}(L))] \subset \mathrm{Gal}(L/K)$ given by Exercise 1.7 6 (b).*
(2) *We choose the prime ideals in (1) such that if we have an inclusion $K \subset L_1 \subset L_2 \subset K^S$, we have that $\mathfrak{P}(L_2)|\mathfrak{P}(L_1)$ then it follows that if we look at the restriction map*

$$\mathrm{Gal}(L_2/K) \to \mathrm{Gal}(L_1/K)$$

that the conjugacy class $[\mathrm{Frob}_{\mathfrak{p}}(\mathfrak{P}(L_2))]$ maps to the conjugacy class $[\mathrm{Frob}_{\mathfrak{p}}(\mathfrak{P}(L_1))]$.
(3) *In light of (2), we may choose a choice of representatives $\{\mathrm{Frob}_{\mathfrak{p}}(\mathfrak{P}(L))\}_{K\subset L\subset K^S} \in \varprojlim_{K\subset L\subset K^S} \mathrm{Gal}(L/K) = \mathrm{Gal}(K^S/K)$ of the conjugacy classes compatible under restriction. One can check that this is well-defined up to conjugacy in $\mathrm{Gal}(K^S/K)$ (cf. the last part of the proof of Proposition 2.12).*
(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]

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

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

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

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

of such a group where $[G, G] \subset G$ denotes the subgroup of commutators. In §1, the interest in the abelianization came from the technical requirement to have well-defined Frobenius elements, as in 1.8 (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

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

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

2.1. **Preliminaries.**

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

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

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

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

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

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

Proof. We prove the two implications separately.

($\Rightarrow$) 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 $(I, \geq)$.

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*
$$A \;\cong\; \mathbb{Q}^{(\kappa)} \;\oplus\; \bigoplus_p \left(\mathbb{Q}_p/\mathbb{Z}_p\right)^{(\lambda_p)},$$
where p varies over all prime numbers.

(Hint: Use that divisible abelian groups are injective objects 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 the study of functorial properties of the cohomology of such 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 $A_{j_1k_1}, \ldots, A_{j_rk_r}$ 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. □

References

[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.