Università di Pisa

Dipartimento di Matematica
Corso di Laurea Triennale in Matematica

Local Tate Duality

Candidato

Francesco Minnocci

Relatore

Tamás Szamuely

Anno Accademico 2023/2024

Contents

Introduction

The aim of this work is to provide an exposition of the Local Tate Duality theorem. The main motivation comes from class field theory, which aims to describe the abelian extensions of a field in terms of the arithmetic of the field itself. Historically, this duality theorem was actually proved using class field theory by John Tate, while in this thesis we will go the other way around as is done by J. P. Serre in [Ser97], by proving the existence of a dualizing module to prove the duality theorem and using it to establish local class field theory for p-adic fields.

First we will need to develop some machinery, such as the cohomology of (pro)finite groups and the notion of cohomological dimension, in order to sistematically study the absolute Galois group of a field, which is profinite. Using this machinery and the topological structure of local fields, we will be able to compute the Brauer group and cohomological dimension of a local field, and prove the finiteness of all cohomology groups with finite coefficients in the case of a p-adic field.

Finally, after introducing an appropriate product in cohomology, we will be able to state and prove the Local Duality theorem, which gives a Poincaré-like duality for finite modules over the absolute Galois group of a p-adic field. As an application, we will show that the Galois group of the maximal abelian extension of a p-adic field is isomorphic to the profinite completion of the multiplicative group of the field. The exposition will mainly follow the book [Har20].

Chapter **1**

Cohomology of Finite Groups

1.1 The category of G-Modules

In this chapter, G will always denote a finite multiplicative group. We begin by introducing the notion of a G-module:

Definition 1.1.1 A G-module is an abelian group A (whose operation we denote additively) endowed with a left action of G such that

$$\begin{aligned} A &\longrightarrow A \\ x &\longmapsto g \cdot x \end{aligned}$$

is a homomorphism of groups for all $g \in G$.

Remark 1.1.2 Let $\mathbb{Z}[G]$ be the group ring of G over $\mathbb{Z}$, that is the set of formal sums

$$\sum_{g \in G} n_g \cdot g$$

with $n_g \in \mathbb{Z}$. The action of G on itself by left multiplication induces a G-module structure on $\mathbb{Z}[G]$ by extending linearly.

More generally, a G-module is the same as a (left) module over the ring $\mathbb{Z}[G]$: the action of G extends linearly to multiplication by elements of $\mathbb{Z}[G]$. This does *not* hold for discrete modules on profinite groups, as we will see later on, however many of the results that we prove in this chapter will hold in that context as well, provided we make some additional topological assumptions.

As with any category, we need specify the morphisms between objects:

Definition 1.1.3 A morphism of G-modules is a group homomorphism $A \xrightarrow{f} B$ which commutes with the action of G, that is

$$f(g \cdot x) = g \cdot f(x)$$

for all $g \in G$ and $x \in A$. Again, this is the same as a morphism of $\mathbb{Z}[G]$-modules.

We denote by $\mathrm{Hom}_G(A, B)$ the abelian group of morphisms of G-modules between A and B, which is a subgroup of $\mathrm{Hom}(A, B)$.

Finally, we define the category of G-modules $\mathsf{Mod_G}$, whose objects are G-modules and whose arrows are morphisms of G-modules. By the above discussion, $\mathsf{Mod_G}$ is equivalent to the category

$\mathbb{Z}[G]$-Mod of left $\mathbb{Z}[G]$-modules, and it is thus an **abelian** category which has enough projectives and injectives.

Example 1.1.4 (G-modules)

- Any abelian group A is a G-module with the trivial action $g \cdot x = x$ for all $g \in G$ and $x \in A$.
- If A and B are G-modules, then the group homomorphisms $\operatorname{Hom}(A, B)$ form a G-module with the action
$$(g \cdot f)(x) = g \cdot f(g^{-1} \cdot x)$$
for all $g \in G$, $f \in \operatorname{Hom}(A, B)$ and $x \in A$.
- Let L/K be a finite Galois extension of fields with Galois group $G = \operatorname{Gal}(L/K)$. Then, the additive group L and the multiplicative group $L^\times$ have a natural G-module structure for the action of G on L by field automorphisms. In this situation, an interesting arithmetic submodule is the group of invariants under the Galois action; this is a key motivation for the definition of group cohomology.

Given a subgroup $H < G$ and an H-module A, there are two ways to produce a G-module from A:
$$\operatorname{Ind}_H^G(A) := \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A$$
is the *induced module* of A from H to G, while
$$\operatorname{CoInd}_H^G(A) := \{f : G \to A \mid f(hg) = h \cdot f(g)\ \forall h \in H, g \in G\}$$
is the *coinduced module* of A from H to G, with the action $(g \cdot f)(x) = f(xg)$. If we identify the latter with the G-module
$$\operatorname{Hom}_H(\mathbb{Z}[G], A)$$
on which G acts by right multiplication on the first factor, we see that the two constructions coincide for finite groups: an isomorphism is of G-modules is given by the map
$$\begin{aligned} \operatorname{Hom}_H(\mathbb{Z}[G], A) &\to \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A \\ f &\mapsto \sum_{\overline{g} \in G/H} g \otimes f(g^{-1}). \end{aligned} \tag{1.1}$$

We will be particularly interested in the case H where is the trivial subgroup $\{1\}$, in which case we write $\mathrm{I}_G(A)$ for the G-module $\operatorname{CoInd}_{\{1\}}^G(A)$, called the *induced module* of A. This is because of the following result:

Proposition 1.1.5 *Any G-module A embeds into its induced module $I_G(A)$.*

Proof. The map $A \overset{i}{\hookrightarrow} I_G(A)$ sending a to the function $g \mapsto g \cdot a$ is an injective morphism of G-modules, as if $g \cdot a = 0$ for all $g \in G$, then taking $g = 1$ gives $a = 0$. □

Finally, we observe that the functors $\operatorname{Ind}_H^G(-)$ and $\operatorname{CoInd}_H^G(-)$ are respectively left and right adjoints to the forgetful functor
$$\mathsf{Mod_G} \to \mathsf{Mod_H},$$
which simply restricts the action of G to H. More precisely:

Proposition 1.1.6 *For every G-module A and every H-module B we have isomorphisms of abelian groups*

$$\begin{aligned} \mathrm{Hom}_G\left(A, \mathrm{CoInd}_H^G(B)\right) &\simeq \mathrm{Hom}_H(A,B) \qquad (1.2)\\ \varphi &\mapsto (a \mapsto \varphi(a)(1)) \\ \mathrm{Hom}_G\left(\mathrm{Ind}_H^G(B), A\right) &\simeq \mathrm{Hom}_H(B,A) \qquad (1.3)\\ \varphi &\mapsto (b \mapsto \varphi(1\otimes b)) \end{aligned}$$

For a proof, see Prop. 1.12 and 1.15 of [Har20].

Remark 1.1.7

(a) As the forgetful functor is exact, by the adjunction (1.2) we deduce that the functor

$$\mathrm{CoInd}_H^G(-) : \mathsf{Mod_H} \to \mathsf{Mod_G}$$

preserves injective objects, as in an abelian category an object I is injective if and only if $\mathrm{Hom}(-, I)$ is exact).

(b) Under the identification (1.1), the isomorphism (1.3) becomes

$$\begin{aligned} \mathrm{Hom}_H(B,A) &\to \mathrm{Hom}_G\left(\mathrm{CoInd}_H^G(B), A\right) \\ \psi &\mapsto \left(f \mapsto \sum_{\overline{g}\in G/H} g\cdot\psi(f(g^{-1}))\right). \end{aligned}$$

(c) Since $\mathrm{CoInd}_H^G(-)$ is a right adjoint it preserves all limits, in particular it is left-exact. Analogously, the functor $\mathrm{Ind}_H^G(-)$ is right-exact. By the isomorphism (1.1), we obtain that $\mathrm{CoInd}_H^G(-)$ is exact.

1.2 Group Cohomology

Recall that in an abelian category $\mathcal{A}$ which has enough injectives, an additive left-exact functor $F : \mathcal{A} \to \mathcal{B}$ with $\mathcal{B}$ abelian admits right derived functors $(R^iF)_{i\geq 0}$, which measure the "failure" of F to be right-exact.

Here are some general properties of derived functors:

- in degree 0 we have $R^0F(A) = F(A)$ for all objects A, as follows from the definition via injective resolutions;
- as derived functors are in particular δ-functors ([Wei94] Ch. 2), for any short exact sequence

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

  of objects in $\mathcal{A}$ there are coboundary morphisms $\delta^i : R^iF(C) \to R^{i+1}F(A)$ fitting in a long exact sequence

  $$\ldots \to R^iF(A) \to R^iF(B) \to R^iF(C) \xrightarrow{\delta^i} R^{i+1}F(A) \to \ldots$$

  which are functorial with respect to morphisms of short exact sequences;

- the $(R^i F)_{i \geq 0}$ form a *universal* δ-functor, in the sense that given another δ-functor S equipped with a natural transformation $\alpha^0 : F = R^0 F \to S^0$ there exists a unique natural transformation $(\alpha^i)_{i \geq 0}$ of δ-functors extending α^0, that is a family of natural transformations commuting with the coboundary morphisms.

We will sometimes encounter δ functors which are not necessarily derived functors:

Definition 1.2.1 Let $T : \mathcal{A} \to \mathcal{B}$ be a δ-functor. An object A is T-**acyclic** if $T(A) = 0$ for all $i > 0$.

Definition 1.2.2 A δ-functor T is **effaceable** if for every object A there exists a monomorphism $A \xrightarrow{u} I$ such that $T(u) = 0$.

The following general result ([Gro57], Ex. 2.4.5) will be useful when taking cohomology after applying certain functors:

Proposition 1.2.3 *Let T be a δ-functor. If T is effaceable, then it is universal.*

We now use this generalities to define the cohomology of a group G with coefficients in a G-module A, by considering a very natural sub-G-module of A:

Definition 1.2.4 The G-**invariants** of A are the elements $a \in A$ fixed by the action of G:

$$A^G := \{x \in A \mid g \cdot x = x \ \forall g \in G\}.$$

This yields an additive functor onto the category of abelian groups

$$F : \mathsf{Mod_G} \to \mathsf{Ab}$$

which is left-exact as it coincides with the functor

$$\operatorname{Hom}_G(\mathbb{Z}, -) : \to \mathsf{Ab}$$

where $\mathbb{Z}$ is the trivial G-module: indeed, a morphism of G-modules $\mathbb{Z} \xrightarrow{f} G$ is determined by the image of 1, which must be thus fixed by the action of G, and any choice of $f(1) \in A^G$ gives such a morphism.

We thus define the cohomology groups of G with coefficients in A as the derived functors of F:

Definition 1.2.5 The i-th cohomology group of G with coefficients in A is

$$H^i(G, A) := R^i F(A).$$

From the above general properties of derived functors, we deduce $H^0(G, A) = A^G$, and the fact that we can compute $H^i(G, A)$ as the cohomology of the complex obtained by taking invariants from an injective resolution $I^\bullet$ of A, that is

$$H^i(G, A) = \ker\left[(I^i)^G \to (I^{i+1})^G\right] / \operatorname{im}\left[(I^{i-1})^G \to (I^i)^G\right].$$

Moreover, if G is trivial then $A^G = A$ for all A implies that F is exact, and thus $H^i(G, A) = 0$ for all $i > 0$.

Remark 1.2.6 Since $F = \operatorname{Hom}_G(\mathbb{Z}, -)$, we get $H^i(G, A) = \operatorname{Ext}^i_G(\mathbb{Z}, A)$. By the balancing property of Ext (Theorem 2.7.6 of [Wei94]), we can interpret $H^i(G, A)$ as the *left* derived functors of the (contravariant) right-exact functor $\operatorname{Hom}_G(-, A)$ evaluated at $\mathbb{Z}$, and can be therefore computed using projective resolutions of $\mathbb{Z}$.

Explicit cochain complexes

It is sometimes more practical to have an explicit description of the groups $H^i(G, A)$. By above the remark, we can compute them using projective resolutions of $\mathbb{Z}$; we now construct such a resolution of $\mathbb{Z}$ by free (and therefore projective) $\mathbb{Z}[G]$-modules.

For any $i \geq 0$, let E_i be the set of $(i+1)$-tuples of elements of G, and define L_i to be the free $\mathbb{Z}$-module with basis E_i. Then, the diagonal action of G on E_i

$$h \cdot (g_0, \dots, g_i) := (hg_0, \dots, hg_i)$$

induces a G-module structure on L_i, making it a free $\mathbb{Z}[G]$-module with basis a set of representatives of the orbits of E_i under the action of G, such as the set of tuples of the form $(1, g_1, \dots, g_i)$ (as G acts without fixed points on E_i). The boundary maps of the complex

$$d_i : L_i \to L_{i-1}$$

for $i > 0$ are defined by

$$(g_0, \dots, g_i) \mapsto \sum_{j=0}^{i} (-1)^j (g_0, \dots, \hat{g_j}, \dots, g_i),$$

and $d_0 : L_0 \to \mathbb{Z}$ sending (g) to 1. By a straightforward computation, this is a complex (i.e. $d_{i-1} \circ d_i = 0$ for all $i > 0$). It is also exact: the map

$$\begin{aligned} k_i : L_i &\to L_{i+1} \\ (g_0, \dots, g_i) &\mapsto \begin{cases} (1, g_0, \dots, g_i) & \text{if } i > 0 \\ 1 & \text{otherwise} \end{cases} \end{aligned}$$

satisfies

$$d_{i+1} \circ k_i + k_{i-1} \circ d_i = \mathrm{id}_{L_i},$$

so that if $x \in \ker d_i$ then $d_{i+1}(k_i(x)) = x$. We have thus constructed a projective resolution

$$\dots \to L_2 \to L_1 \to L_0 \to \mathbb{Z} \to 0$$

of $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module.

By applying the functor $\mathrm{Hom}_G(-, A)$ to this resolution, we get

Theorem 1.2.7 *The groups $H^i(G, A)$ can be computed as the i-th cohomology of the complex $K^\bullet := \mathrm{Hom}_G(L_\bullet, A)$ of* homogeneous *cochains. These are the same as functions $G^{i+1} \to A$ commuting with the diagonal action of G, on which the boundary is given by*

$$(d^i f)(g_0, \dots, g_{i+1}) = \sum_{j=0}^{i+1} (-1)^j f(g_0, \dots, \hat{g_j}, \dots, g_{i+1}).$$

For low-degree computations, it's convenient to use *inhomogeneous* cochains instead. These arise from the fact that a function $G^{i+1} \to A$ commuting with the diagonal action of G is determined by its values on elements of the form

$$(1, g_1, \dots, g_i),$$

and define the inhomogeneous i-th cochains as *all* functions $f : G^i \to A$ with a slightly denser formula for the boundary maps:

$$\begin{aligned}(d^i f)(g_1, \dots, g_{i+1}) &= g_1 \cdot f(g_2, \dots, g_{i+1}) \\ &\quad + \sum_{j=1}^{i} (-1)^j f(g_1, \dots, g_j g_{j+1}, \dots, g_{i+1}) + (-1)^{i+1} f(g_1, \dots, g_i).\end{aligned} \tag{1.4}$$

If we denote the resulting complex by $C^\bullet$, there is an isomorphism of complexes

$$K^\bullet \xrightarrow[\sim]{\Phi} C^\bullet$$

sending $f : G^{i+1} \to A$ to

$$\begin{aligned}\Phi(f) : G^i &\to A, \\ (g_1, \dots, g_i) &\mapsto f(1, g_1, g_1 g_2, \dots, g_1 \cdots g_i),\end{aligned}$$

whose inverse sends $f : G^i \to A$ to the function

$$(g_0, \dots, g_i) \mapsto g_0 \cdot f(g_0^{-1} g_1, \dots, g_0^{-1} g_i).$$

As a consequence, we can also compute $H^i(G, A)$ as the i-th cohomology of the complex $(C^\bullet, d)$ of inhomogeneous cochains.

Corollary 1.2.8 *Let G be a finite group. If A is a finite G-module, then $H^i(G, A)$ is a finite abelian group for all i.*

Example 1.2.9 (using inhomogeneous cochains)

- The 1-cocycles $Z^1(G, A) = \ker d^1$ are functions $f : G \to A$ satisfying

  $$f(gh) = g \cdot f(h) + f(g)$$

  for all $g, h \in G$, while the 1-coboundaries $B^1(G, A) = \operatorname{im} d^0$ are functions of the form

  $$g \mapsto g \cdot a - a$$

  for some $a \in A$.

- If A is a trivial G-module, then $B^1(G, A)$ is trivial, and $Z^1(G, A)$ consists of functions satisfying $f(gh) = f(g) + f(h)$, which are exactly the group homomorphisms $G \to A$. In conclusion, for a trivial G-module we have

  $$H^1(G, A) = \operatorname{Hom}(G, A).$$

1.3 Functoriality

Given a G-module A and a group homomorphism $G' \xrightarrow{\varphi} G$, we can define a G'-module structure on A by “restriction of scalars”:

$$h \cdot a = \varphi(h) \cdot a.$$

If we denote by $\varphi^* A$ the resulting G'-module, this defines a functor

$$\varphi^* : \mathsf{Mod_G} \to \mathsf{Mod_{G'}}$$

induced by φ, and since $A^G \subseteq (\varphi^* A)^{G'}$, we get a natural transformation

$$\varphi_0^* : H^0(G, -) \to H^0(G', \varphi^*(-))$$

which extends by universality to a morphism of δ-functors

$$\varphi_i^* : H^i(G, -) \to H^i(G', \varphi^*(-)).$$

From now on, we will just write A instead of $\varphi^* A$ when there is no ambiguity.

We also have functoriality with respect to A, provided that we only consider morphisms which are compatible with the action under consideration:

Definition 1.3.1 Let A and φ be as above, and let B be a G'-module. We say that a group homomorphism $A \xrightarrow{f} B$ is **compatible** with φ if

$$f(\varphi(g) \cdot a) = g \cdot f(a)$$

for all $g \in G'$ and $a \in A$. This means exactly that f is a morphism of G'-modules $\varphi^* A \to B$. In particular, for each $i \geq 0$ we get a homomorphism

$$f_* : H^i(G, \varphi^* A) \to H^i(G', B),$$

and by precomposing with φ_i^* we get a homomorphism

$$H^i(G, A) \to H^i(G', B).$$

associated with the pair (φ, f) which commutes with the coboundaries. On the level of cochains, it sends $\alpha : G^i \to A$ to

$$f \circ \alpha \circ \varphi^{(i)} : (G')^i \to B,$$

where $\varphi^{(i)} := (\varphi, \ldots, \varphi) : (G')^i \to G^i$.

Here are some important examples of the above construction:

Definition 1.3.2

(a) Let A be a G-module, and H a subgroup of G. The inclusion homomorphism $H \hookrightarrow G$ induces a homomorphism known as the **restriction** map

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

for all $i \geq 0$. Using (1.3.1) we see that Res sends a cocycle $\alpha : G^i \to A$ to the restriction of α to H^i, from which the name.

(b) Let A be a G-module, and N a normal subgroup of G. Then, the quotient G/N acts naturally on A^N, and the inclusion of A^N in A is compatible with the projection $\pi : G \to G/N$. This induces the **inflation** map

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

On cochains, this amounts to precomposing a function $(G/N)^i \to A^N$ with the homomorphism $\pi^{(i)} : G^i \to (G/N)^i$.

(c) Functoriality is useful even when there is no "change of group": if A is G-module, given any element s in G consider the associated automorphism of A

$$\begin{aligned} f : A &\to A \\ a &\mapsto s \cdot a. \end{aligned}$$

Then, f is compatible with the inner automorphism σ of G associated with s^{-1}:

$$f(\sigma(g) \cdot a) = f(s^{-1}gs \cdot a) = g \cdot f(a),$$

and for all $i \geq 0$ we get a map

$$\sigma_s : H^i(G,\, A) \to H^i(G,\, A).$$

The above homomorphism is actually the identity, as we will see in Proposition 1.3.6.

We will use the following lemma in the construction of the Hochschild-Serre spectral sequence:

Lemma 1.3.3 *Let G be a finite group, and H a subgroup. Then, the forgetful functor*

$$\mathsf{Mod_G} \to \mathsf{Mod_H}$$

preserves injective objects.

Proof. Let A be a G-module. As in the proof of the fact that the category of modules over a ring has enough injectives, we can embed A in a huge injective G-module

$$A \hookrightarrow I := \prod_{\mathrm{Hom}_G(A,Q)} Q,$$

where Q is the injective G-module $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \mathbb{Q}/\mathbb{Z})$ (recall that direct products preserve injectives).

Now, suppose that A is an injective G-module. Then, A is a direct factor of I: to find a retraction, use the injectivity of A applied to the diagram

$$\begin{tikzcd} A \arrow[r, hook] \arrow[d, equal] & I \arrow[dl, dashed, "\exists"] \\ A. & \end{tikzcd}$$

Therefore, it's enough to show that I is injective as an H-module. As direct products preserve injectives, it's enough to show that Q is injective as an H-module, and since $\mathbb{Z}[G]$ is a free $\mathbb{Z}[H]$-module generated by a finite set of right coset representatives of H in G, we have

$$Q = \mathrm{I}_G(\mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Z}[G] \otimes \mathbb{Q}/\mathbb{Z} = \left(\bigoplus_{G/H} \mathbb{Z}[H] \right) \otimes \mathbb{Q}/\mathbb{Z} = \bigoplus_{G/H} \mathbb{Z}[H] \otimes \mathbb{Q}/\mathbb{Z} = \bigoplus_{G/H} \mathrm{I}_H(\mathbb{Q}/\mathbb{Z}),$$

and the result follows from the fact that $\mathrm{I}_H(-)$ preserves injectives (Remark 1.1.7 (a)). □

Shapiro's Lemma

We now prove an important result which relates the cohomology of a subgroup to that of the whole group:

Theorem 1.3.4 *Let H be a subgroup of G and B an H-module. Then, for every $i \geq 0$ there is a canonical isomorphism*

$$\mathrm{Sh} : H^i(G,\, \mathrm{CoInd}_H^G(B)) \simeq H^i(H,\, B).$$

Proof. We claim that the functors

$$H^i(G,\, \mathrm{CoInd}_H^G(-)) : \mathsf{Mod_H} \to \mathsf{Ab}$$

form a universal δ functor: it's a δ functor since $\mathrm{CoInd}_H^G(-)$ is exact by Remark 1.1.7 (c), and it's effaceable because we can embed B in an injective H-module I, and $\mathrm{CoInd}_H^G(I)$ is injective by Remark 1.1.7 (a). The claim then follows from Proposition 1.2.3.

Moreover, we can construct a homomorphism

$$\mathrm{Sh} : H^i(G,\, \mathrm{CoInd}_H^G(B)) \to H^i(H,\, B)$$

by functoriality, using the map

$$\begin{aligned} \mathrm{CoInd}_H^G(B) &\to B \\ f &\mapsto f(1) \end{aligned}$$

which is compatible with the inclusion $H \hookrightarrow G$.

By universality, it's enough to show that this is an isomorphism for $i = 0$. However, an element $f : G \to B$ of $(\mathrm{CoInd}_H^G(B))^G$ must be constant as

$$f(x) = (g \cdot f)(x) = f(xg)$$

for all $g, x \in G$. Finally, by definition of coinduced module it must also satisfy

$$f(h) = h \cdot f(1)$$

for all $h \in H$, which means that $f(1) \in B^H$. □

As a special case of Shapiro's Lemma, we deduce that $\mathrm{I}_G(A)$ is cohomologically trivial: this allows us to prove statements about group cohomology by a technique know as *dimension shifting* (as in Proposition 1.3.6 below), which is a concrete incarnation of the universality of derived functors.

Corollary 1.3.5 *Let A be a G-module. Then, the cohomology groups of G with coefficients in the induced module $\mathrm{I}_G(A)$ are all zero except for $H^0(G,\, \mathrm{I}_G(A)) \simeq A$.*

Proposition 1.3.6 *The homomorphism σ_s defined in 1.3.2 (c) is the identity in each degree.*

Proof. We prove this by dimension shifting: for $i = 0$, by construction σ_s sends $a \in A^G$ to $s \cdot a = a$.

For $i > 0$, we proceed by induction on i: embed A into $\mathrm{I}_G(A)$, and let $B := \mathrm{Coker}(A \hookrightarrow \mathrm{I}_G(A))$. The exact sequence

$$0 \to A \to \mathrm{I}_G(A) \to B \to 0$$

gives rise to a long exact sequence in cohomology, and by the compatibility of σ_s with the coboundaries and Corollary 1.3.5 we get a commutative diagram with exact rows

$$\begin{tikzcd}
H^i(G, I) \arrow[r] \arrow[d, "\sigma_s"] & H^i(G, B) \arrow[r] \arrow[d, "\sigma_s"] & H^{i+1}(G, A) \arrow[r] \arrow[d, "\sigma_s"] & 0 \\
H^i(G, I) \arrow[r] & H^i(G, B) \arrow[r] & H^{i+1}(G, A) \arrow[r] & 0.
\end{tikzcd}$$

By induction, the middle vertical map is the identity, and it follows that the last one is the identity as well. □

Corollary 1.3.7 *Let A be a G-module, and assume that N is a normal subgroup of G. Then, there is an action of G/N on $H^i(G, A)$ for all i.*

Proof. Since N is normal, G acts by conjugation on $H^i(N, A)$ as described in the above example, and by the previous proposition any $n \in N$ acts trivially, so that the action of G/N is well-defined. □

Corestriction

Let H be a subgroup of G, and A a G-module. We want to define a **corestriction** map which goes in the opposite direction of the restriction: in degree 0, it's given by the "norm" homomorphism

$$\begin{aligned} \mathrm{N}_{G/H} : A^H &\longrightarrow A^G \\ a &\longmapsto \sum_{g \in G/H} g \cdot a. \end{aligned}$$

Remark 1.3.8 This comes from field theory, as we can reinterpret the norm map relative to a tower of finite field extensions $K \subset F \subset L$: in this case $A = L^\times$, $G = \mathrm{Gal}\,(L/K)$ and $H = \mathrm{Gal}\,(L/F)$, and

$$\mathrm{N}_{G/H} = N_{F/K} : F^\times \to K^\times$$

is given by

$$x \mapsto \prod_{\sigma \in G/H} \sigma(x).$$

In general, we can extend this to a map

$$\mathrm{Cor} : H^i(H, f^*(A)) \to H^i(G, A)$$

where $f : H \to G$ is the inclusion homomorphism, because the $H^i(H, f^*(-))$ form a universal δ-functor: indeed, it's effaceable since we can embed A in an injective G-module I, and $f^*(I)$ is injective by Lemma 1.3.3.

Remark 1.3.9 We can also define the corestriction using Shapiro's Lemma: the surjection

$$\begin{aligned} \pi : \mathrm{CoInd}_G^H\,(A) &\to A \\ f &\mapsto \sum_{g \in G/H} g \cdot f(g^{-1}) \end{aligned}$$

induces a map

$$\pi^* : H^i(G, \mathrm{CoInd}_G^H\,(A)) \to H^i(G, A),$$

and if we precompose with $\mathrm{Sh}^{-1} : H^i(H, A) \to H^i(G, \mathrm{CoInd}_G^H\,(A))$ the resulting map is the corestriction, as is easily checked in degree 0 (and the general case follows by universality).

The composite (Cor ∘ Res) is as simple as it gets:

Theorem 1.3.10 *Let H be a subgroup of G, and A a G-module. Then, the composite*

$$H^i(G,\,A) \xrightarrow{\mathrm{Res}} H^i(H,\,A) \xrightarrow{\mathrm{Cor}} H^i(G,\,A)$$

is multiplication by the index $(G:H)$.

Proof. In degree 0, we have

$$A^G \hookrightarrow A^H \to A^G,$$

which sends $a \in A^G$ to

$$\sum_{g\in G/H} g\cdot a = (G:H)\cdot a.$$

The result then follows from universality, as the homomorphism in question is an endomorphism of the universal δ-functor $H^i(G,\,-)$. □

This has a number of useful consequences:

Corollary 1.3.11 *Let G be a finite group of order m, and A a G-module. Then, the groups $H^i(G,\,A)$ are m-torsion for all $i>0$. In particular, if m is invertible in A, then $H^i(G,\,A)=0$ for all $i>0$.*

Proof. Chossing H to be the trivial subgroup in Theorem 1.3.10, we get that multiplication by m on $H^i(G,\,A)$ for $i>0$ factors through $H^i(\{1\},\,A)=0$. For the second statement, the additivity of the functor $H^i(G,\,-)$ implies that $H^i(G,\,\cdot n)$ is multiplication by n on $H^i(G,\,A)$. □

Corollary 1.3.12 *If A is a uniquely divisible G-module, then $H^i(G,\,A)=0$ for all $i>0$.*

Proof. By the previous corollary all the groups in question are m-torsion with $m=|G|$, and by assumption $A \xrightarrow{\cdot n} A$ is an isomorphism for any $n>0$, so in particular multiplication by m is an isomorphism in cohomology. □

1.4 The Hochschild-Serre Spectral Sequence

Let G be a group, and N a normal subgroup. The *Hochschild-Serre spectral sequence* is a useful gadget which relates the cohomology of G with coefficients in a G-module A in terms of the cohomology of N with coefficients in A, and of G/N with coefficients in A^N.

We will construct this spectral sequence using the following general result by Grothendieck ([Wei94], Th. 5.8.3):

Theorem 1.4.1 (Spectral Sequence of Composed Functors) *Let $\mathcal{A},\mathcal{B}$ and $\mathcal{C}$ be abelian categories, and assume that $\mathcal{A},\mathcal{B}$ have enough injectives. If $F:\mathcal{A}\to\mathcal{B}$ and $G:\mathcal{B}\to\mathcal{C}$ are left-exact additive functors and F takes injectives to G-acyclic objects, then for any object A in $\mathcal{A}$ there exists a spectral sequence*

$$E_2^{p,q} = R^pG(R^qF(A)) \Longrightarrow R^{p+q}(G\circ F)(A).$$

We want to apply this theorem to the composition

$$\mathsf{Mod_G} \xrightarrow{A\mapsto A^N} \mathsf{Mod}_{G/N} \xrightarrow{B\mapsto B^{G/N}} \mathsf{Ab},$$

which is a factorization of the functor

$$\mathsf{Mod_G} \xrightarrow{A\mapsto A^G} \mathsf{Ab}$$

(since $A^G = (A^N)^{G/N}$). If we denote by F the functor $A \mapsto A^N$, and by G the functor $B \mapsto B^{G/N}$, then by Remark 1.1.7 (a) F preserves injectives, and injective objects are acyclic. This is almost enough to prove the main result:

Theorem 1.4.2 (Hoschild-Serre) *Let G be a group, and N a normal subgroup. Then, for any G-module A there exists a spectral sequence*

$$E_2^{p,q} = H^p(G/N,\, H^q(N,\, A)) \Longrightarrow H^{p+q}(G,\, A).$$

Proof. We only need to check that $H^q(N, -)$, which by Corollary 1.3.7 we can view as a functor $\mathsf{Mod_G} \to \mathsf{Mod}_{G/N}$, is the right derived functor of F. This is true because $R^qF(A)$ is computed using an injective resolution of A as a G-module, and Lemma 1.3.3 shows that this is also an injective resolution of A as an N-module. □

Remark 1.4.3 With some work, one can show that the edge maps of the spectral sequence

$$E_2^{n,0} = H^n(G/N,\, A^N) \longrightarrow H^n(G,\, A)$$

and

$$H^n(G,\, A) \longrightarrow E_2^{0,n} = H^n(N,\, A)^{G/N}$$

are the inflation and restriction maps, respectively.

The convergence of above spectral sequence amounts to the existence, for every $n > 0$, of a finite filtration

$$H^n(G,\, A) = F^0 \supseteq F^1 \supseteq \ldots \supseteq F^n \supseteq F^{n+1} = 0$$

such that

$$F^p/F^{p+1} \simeq E_\infty^{p,n-p}, \tag{1.5}$$

where $E_\infty^{p,n-p}$ is a subquotient (i.e. quotient of a subobject) of $E_2^{p,n-p} = H^p(G/N,\, H^{n-p}(N,\, A))$.

A careful analysis of these filtrations in low degrees yields a 5-term exact sequence relating some of the functorial maps which we have defined:

Corollary 1.4.4 *Let G be a group, N a normal subgroup, and A a G-module. Then, there is a 5-term exact sequence*

$$0 \to H^1(G/N,\, A^N) \overset{\mathrm{Inf}}{\to} H^1(G,\, A) \overset{\mathrm{Res}}{\to} H^1(N,\, A)^{G/N} \to H^2(G/N,\, A^N) \overset{\mathrm{Inf}}{\to} H^2(G,\, A)$$

Moreover, if the cohomology of N with coefficients in A is trivial up to degree $n-1$ we also get a short exact sequence in degree n:

Corollary 1.4.5 *With the notations of the previous corollary, let $n \geq 2$ and suppose that $H^i(N,\, A) = 0$ for all $0 < i < n$. Then, there is a short exact sequence*

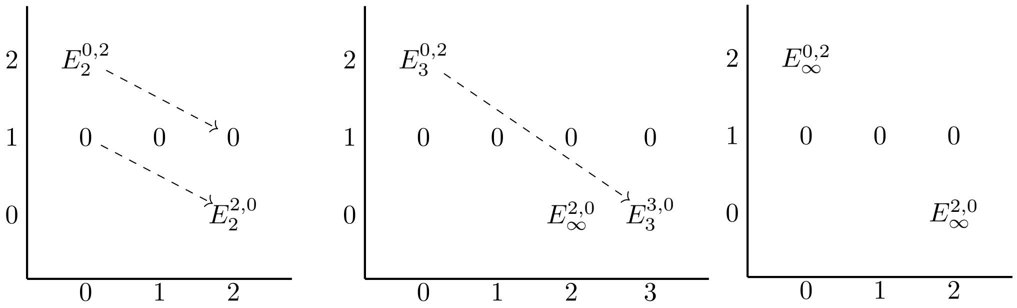
$$0 \to H^n(G/N,\, A^N) \overset{\mathrm{Inf}}{\to} H^n(G,\, A) \overset{\mathrm{Res}}{\to} H^n(N,\, A)^{G/N}.$$

Proof. The triviality assumption implies that $E_2^{p,q} = 0$ for $0 < q < n$. Thus, for $p + q = n$ the only non-trivial terms are $E_\infty^{0,n}$ and $E_\infty^{n,0}$. In this case, we have $E_\infty^{n,0} = E_2^{n,0}$ and $E_\infty^{0,n}$ is a subobject of $E_2^{0,n}$ (as in figure 1.4 for $n = 2$) Moreover, there exists a filtration

$$0 \subset F^n \subset H^n(G,\, A),$$

and by taking cokernels and composing with an inclusion we get the desired short exact sequence: indeed, by (1.5) we have the identifications

$$\begin{aligned} F^n = E_\infty^{n,0} &= H^n(G/N,\, A^N), \\ H^n(G,\, A)/F^n = E_\infty^{0,n} &\subset E_2^{0,n} = H^n(N,\, A)^{G/N}. \end{aligned}$$



□

1.5 Cohomology of Finite Cyclic Groups

Let $G = \{1, s, \dots, s^{n-1}\}$ be a finite cyclic group of order n generated by an element s, and let A be a G-module. To compute the cohomology groups $H^i(G,\, A)$, we consider the following free resolution of $\mathbb{Z}$ as a G-module:

$$\dots \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{s-\mathrm{id}} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{s-\mathrm{id}} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0. \tag{1.6}$$

Here, N denotes the norm map

$$N(x) = \sum_{i=0}^{n-1} s^i \cdot x,$$

ε is the augmentation map

$$\sum_{i=0}^{n-1} a_i s^i \mapsto \sum_{i=0}^{n-1} a_i,$$

and $(s - \mathrm{id})$ is the map

$$x \mapsto s \cdot x - x.$$

As $\mathrm{Hom}_G(\mathbb{Z}[G], A)$ is isomorphic to A through the map $f \mapsto f(1)$, applying the functor $\mathrm{Hom}_G(-, A)$ to the above resolution gives a complex

$$\underset{0}{A} \xrightarrow{s-\mathrm{id}} \underset{1}{A} \xrightarrow{N} \underset{2}{A} \xrightarrow{s-\mathrm{id}} \underset{3}{A} \longrightarrow \dots$$

where the maps on A are defined by the same formulas as above. This computes the cohomology of G with coefficients in A:

$$\begin{cases} H^0(G,\, A) = A^G, \\ H^{2i}(G,\, A) = A^G/N(A) \quad \text{for } i > 0, \\ H^{2i+1}(G,\, A) = \ker(N)/(s - \mathrm{id})A. \end{cases} \tag{1.7}$$

In particular, if A is a trivial G-module, we get

$$\begin{cases} H^0(G,\, A) = A, \\ H^{2i}(G,\, A) = A/nA \quad \text{for } i > 0, \\ H^{2i+1}(G,\, A) = \ker(A \xrightarrow{\cdot n} A). \end{cases} \tag{1.8}$$

Chapter 2

Cohomology of Profinite Groups

In this chapter we extend the notion of group cohomology to profinite groups, which are projective limits of finite groups, and as such have a natural topology. We will see that the cohomology of a profinite group can be reduced to the cohomology of its finite quotients, and how this relates to infinite Galois theory.

2.1 Profinite Groups

Definition 2.1.1 A **profinite group** is a topological group which is isomorphic to the projective limit of a projective system of finite groups.

Here, the topology on the projective limit of a projective system (G_i, φ_{ij}) is the one induced by the product topology on $\prod G_i$, where we endow each finite group with the discrete topology. This makes $\varprojlim G_i$ into a compact, Hausdorff, and totally disconnected topological group (it's a closed subspace of the product). Recall that an explicit description of the projective limit is given by

$$\varprojlim G_i = \left\{ (g_i) \in \prod G_i \mid \varphi_{ji}(g_j) = g_i \text{ for all } i \leq j \right\}.$$

Remark 2.1.2 This actually gives an equivalent characterization: a topological group G is profinite if and only if it is compact, Hausdorff, and totally disconnected ([NSW00], Th. 1.1.3).

In any topological group, the open subgroups are also closed, being the complement of the union of the other cosets. In a profinite group, open subgroups are exactly the closed subgroups of finite index: indeed, if H is a open, then the cosets of H form a finite open cover of G, and by compactness there is a finite subcover which shows the finiteness of G/H; conversely a closed subgroup of finite index is the complement of a finite union of closed sets, hence open.

Note that we can always assume the transition maps φ_{ij} are surjective by restricting them to the image of the natural projections $G \to G_i$ (Cor. 1.1.8 (a) of [RZ10]), and the limit of the corresponding system is isomorphic to G. By compactness, the resulting projections $G \twoheadrightarrow G_i$ are surjective as well (loc. cit. Prop. 1.1.10). An example of such a surjective projective system is given by the finite quotients of the open normal subgroups of G.

Finally, the profinite topology is uniquely determined by the fact that the identity $1 \in G$ admits a basis of open neighborhoods (Γ_i) which are normal in G, and

$$\varprojlim_i G/\Gamma_i \simeq G$$

(we can take the (Γ_i) to be the kernel of $G \to G_i$).

The morphisms under consideration between two profinite groups G, H are the continuous group homomorphisms, which we denote by $\mathrm{Hom}_c(G, H)$.

Example 2.1.3 (Profinite Groups)

- By the characterization of Remark 2.1.2, any finite group is profinite with the discrete topology.
- Let K be a field, and fix a separable closure $\overline{K}$ of K. Then, the absolute Galois group $\mathrm{Gal}\left(\overline{K}/K\right)$ is profinite: indeed, by writing $\overline{K}$ is the inductive limit of the finite Galois extensions (K_i) of K contained in $\overline{K}$ and setting $G_i := \mathrm{Gal}\,(K_i/K)$, we get a surjective projective system of finite groups whose projective limit is $\mathrm{Gal}\left(\overline{K}/K\right)$.

  More generally, given a (possibly infinite) Galois extension L/K, there is a one-to-one correspondence between the closed subgroups $H < \mathrm{Gal}\,(L/K)$ and the intermediate field extensions $K \subset F \subset L$, which is given by $H \mapsto L^H$ and $F \mapsto \mathrm{Aut(L/F)}$. In this correspondence, *normal* subgroups correspond to Galois extensions, and open subgroups to finite extensions (as they the closed subgroups of finite index). The idea of introducing a topology on the Galois group in order to restore the correspondence in the infinite case is originally due to Wolfgang Krull.
- Any closed subgroup H of a profinite group G is profinite. By using a surjective system (G_i, φ_{ij}), one shows that the closed subgroups of G are exactly those of the form $\varprojlim H_i$ for subgroups $H_i < G_i$ such that φ_{ij} restricts to a surjection $H_j \to H_i$ for all $i \leq j$.

We now introduce a notion of index for closed subgroups of a profinite group:

Definition 2.1.4 (Supernatural Number) A **supernatural number** is a formal product of (possibly infinite) prime powers

$$n = \prod_{p \text{ prime}} p^{n_p},$$

where $n_p \in \mathbb{N} \cup \{\infty\}$. There are well-defined notions of multiplication, divisibility and greatest common divisor/lower common multiple which extend the usual ones (e.g. the lcm of a set of supernatural numbers is just the supremum).

Example 2.1.5

- If L/K is an algebraic extension, then the degree $[L : K]$ is a supernatural number, equal to the supremum of the degrees of its finite subextensions.
- If $\overline{\mathbb{F}}_p$ is an algebraic closure of $\mathbb{F}_p$, then

$$[\overline{\mathbb{F}}_p : \mathbb{F}_p] = \prod_{p \text{ prime}} p^{\infty}.$$

Definition 2.1.6 Let G be a profinite group with $G \twoheadrightarrow G_i$. Then, the **index** of a closed subgroup $H = \varprojlim H_i$ of G is the supernatural number

$$[G : H] := \sup[G_i : H_i],$$

which coincides with $\mathrm{lcm}\,[G/U : {}^{H}/_{H \cap U}]$ for U ranging over all open normal subgroups of G.

The **order** of G is the index $[G : \{1\}]$, or equivalently

$$|G| := \sup |G_i| = \mathrm{lcm}\,[G : U].$$

For finite groups, this notion of index coincides with the usual one, and it's "multiplicative" in the sense that $[G:H]=[G:K][K:H]$ for closed subgroups $H<K<G$.

Example 2.1.7

- $|\mathbb{Z}_p| = p^\infty$.
- $|\widehat{\mathbb{Z}}| = \prod_p p^\infty$.

One of the properties shared with finite groups is the existence of p-Sylow subgroups:

Definition 2.1.8 A pro-p-group is a profinite group G such that $|G|$ is a power of p. Given a profinite group G, a **p-Sylow subgroup** is a closed subgroup $H<G$ which is a pro-p group with $[G:H]$ prime to p.

Proposition 2.1.9 *Let G be a profinite group. Then, for any prime p there exists a p-Sylow subgroup of G, and any two p-Sylows are conjugate. Moreover, any pro-p-subgroup of G is contained in a p-Sylow.*

This follows from the analogous statement for finite groups, by a careful passage to the limit.

Example 2.1.10 For any prime p, the ring of p-adic integers $\mathbb{Z}_p$ is a pro-p-group, and it's the unique p-Sylow of $\widehat{\mathbb{Z}}$.

Example 2.1.11 The *profinite completion* of a discrete group G is a profinite group $\widehat{G}$ together with a homomorphism $G\to\widehat{G}$ which is universal with respect to homomorphisms into profinite groups: for any H profinite and for any homomorphism $f:G\to H$, there exists a unique continuous homomorphism $\widehat{f}:\widehat{G}\to H$ making the diagram

$$\begin{tikzcd}
G \arrow[r] \arrow[d] & \widehat{G} \arrow[dl, dashed, "\exists!\widehat{f}"] \\
H &
\end{tikzcd}$$

commute. The profinite completion can be constructed as the projective limit of the quotients G/N for N normal of finite index.

2.2 Discrete G-Modules

We now adapt the definition of a G-module to the case of a profinite group:

Definition 2.2.1 (Discrete G-module) A discrete G-module is an abelian group A equipped with a *continuous* action of G. In other words, for any $a\in A$ the map

$$\begin{aligned} G &\to A \\ g &\mapsto g\cdot a \end{aligned}$$

is continuous, and $a\mapsto g\cdot a$ is a homomorphism for all $g\in G$.

Remark 2.2.2 This is equivalent to

(a) asking that the stabilizer $\mathrm{St}\,(x)$ of any element $x\in A$ is open in G.

(b) requiring that A is the union of the A^U, where U ranges over the set of all open subgroups of G.

The category of discrete G-modules $\mathsf{Mod}_{\mathsf{G}}^{\mathsf{c}}$ is a full abelian subcategory of the category of all $\mathbb{Z}[G]$ modules $\mathsf{Mod}_{\mathsf{G}}$, and it has enough injectives ([Wei94], Prop. 6.11.10).

Remark 2.2.3 If A is a discrete G-module, then A is finitely generated as a $\mathbb{Z}[G]$-module if and only if it is finitely generated as a $\mathbb{Z}$-module. This is because the stabilizer $\mathrm{St}\,(x)$ of any element $x \in A$ is open, and thus of finite index in G.

Example 2.2.4 (Galois Theory) Later, in the case of $G = \mathrm{Gal}\left(\overline{K}/K\right)$ we will consider as discrete G-modules the additive and multiplicative groups $\overline{K}$ and $\overline{K}^{\times}$ respectively, as well as the group of roots of unity $\mu_n \subset \overline{K}^{\times}$ and the trivial module $\mathbb{Z}/n\mathbb{Z}$.

2.3 Passage to the Limit

We now want to define the cohomology of a profinite group G with coefficients in a discrete G-module. As category of discrete G-modules has enough injectives, we are tempted to use the derived functors of $A \mapsto A^G$ again. However, there's a caveat: the abelian category $\mathsf{Mod}_{\mathsf{G}}^{\mathsf{c}}$ *does not* have enough projectives: the main issue is that $\mathbb{Z}[G]$ is not a discrete G-module, as its stabilizers are trivial. Therefore, keeping in mind our application to field theory, we define cohomology through (continuous) cochains directly to reduce to the cohomology of a profinite group to that of its finite quotients.

Definition 2.3.1 Let A be a discrete G-module. We define $C^i(G, A)$ to be the set of all *continuous* functions $G^i \to A$. The coboundary maps $d^i : C^i(G, A) \to C^{i+1}(G, A)$ are defined exactly as in (1.4), and we denote by $H^i(G,\, A)$ the cohomology of the complex $(C^\bullet(G, A), d^\bullet)$.

Theorem 2.3.2 *Suppose that (G_i) is a projective system of profinite groups and (A_i) is an inductive system of discrete G_i-modules such that the transition maps of the two systems are compatible. Then, for any $n \in \mathbb{N}$ the natural map*

$$\varinjlim C^n(G_i, A_i) \to C^n(G, A)$$

induces an isomorphism in cohomology:

$$H^n(G,\, A) \simeq \varinjlim H^n(G_i,\, A_i),$$

where $G := \varprojlim G_i$ and $A := \varinjlim A_i$.

The proof of the theorem is tricky but elementary, and relies on topological arguments using the compactness of each G_i and the fact that continuous functions into a discrete space are locally constant (see [Har20], Th. 4.1.8).

In view of Remark 2.2.2, this implies that we can compute the cohomology of a profinite group by passing to the limit over the cohomology of its finite quotients:

Corollary 2.3.3 *Let A be a discrete G-module. Then,*

$$H^i(G,\, A) = \varinjlim H^i(G/U,\, A^U),$$

where U ranges over all open normal subgroups of G.

As a consequence we find that the cohomology of a profinite group with coefficients in a discrete G-module is always a torsion group, as in the above limit each term is $|G/U|$-torsion by the finite case.

Corollary 2.3.4 *Let A be a discrete G-module. Then, $H^i(G,\, A)$ is a torsion group for all $i > 0$.*

Keeping in mind Remark 2.2.3, writing A as the inductive limit of its finitely generated sub-G-module yields the following corollary:

Corollary 2.3.5 *Let A be a discrete G-module, and write $A = \bigcup B$ where B ranges over the finite type sub-G-modules of A. Then,*

$$H^i(G,\, A) = \varinjlim H^i(G,\, B).$$

Example 2.3.6 If (G_i) is a filtered family of open subgroups of G profinite where we take the transition maps to be inclusions, then

$$G := \varprojlim G_i = \bigcap G_i$$

is closed in G and thus profinite. By Theorem 2.3.2 we get

$$H^i(G,\, A) \simeq \varinjlim H^i(G_i,\, A).$$

for any discrete G-module A.

Remark 2.3.7 The functor $H^i(G,\, -)$ we just defined is a δ-functor, as the functor $C^i(G, -)$ is exact. As in degree zero it coincides with $A \mapsto A^G$, if we show that it is universal then it will be the right derived functor of $A \mapsto A^G$.

Indeed, $H^i(G,\, -)$ is effaceable: if we embed $A \hookrightarrow I$ for an injective object I in $\mathsf{Mod}^c_\mathsf{G}$, we see that I^U is injective as a $\mathbb{Z}[U]$-module for any open normal subgroup U of G, and thus

$$H^i(G,\, I) = \varinjlim H^i(G/U,\, I^U) = 0.$$

Lemma 2.3.8 *Let G be a profinite group and H a closed subgroup. If I is injective object in $\mathsf{Mod}^c_\mathsf{G}$, then I is an injective object in $\mathsf{Mod}^c_\mathsf{H}$.*

The proof ultimately relies on the analogous result for finite groups 1.3.3, and it passes through Baer's criterion for injectivity (see [Har20], Prop. 4.25).

We now state the properties of the cohomology of profinite groups which are carried over by passage to the limit from those developed in the first chapter. The general philosophy is that we have to require subgroups to be closed (open when finiteness of cosets is needed), and maps defined on G to be continuous.

Remark 2.3.9 Let G be a profinite group.

- For any closed subgroup $H < G$ and any discrete G-module A, we can define the coinduced module $\mathrm{CoInd}_H^G A$ as in the finite case, provided we only take continuous functions $G \to A$, and $\mathrm{I}_G(A)$ is still acyclic. However, there is no notion of induced module from H to G, because $\mathbb{Z}[G]$ is not a discrete G-module.

- For any closed subgroup $H < G$, Shapiro's Lemma holds with the same proof: although by the above observation we don't have the isomorphism (1.1), CoInd_H^G is still right exact. Indeed, we can reduce to the case of finite groups because continuous functions $G \to A$ have finite image and thus factor through a finite quotient G/U for some open normal subgroup U of G, as these form a basis of neighborhoods of the identity; more precisely, we have an isomorphism

$$\mathrm{CoInd}_H^G A \simeq \varinjlim \mathrm{CoInd}_{HU/U}^{G/U} \left(A^{U\cap H}\right).$$

  Moreover, the functorial homomorphisms inflation, restriction and "conjugation" are defined as for finite groups.

- If H is closed and normal, the Hochschild-Serre spectral sequence and its consequences are still valid (we can use Lemma 2.3.8 to adapt the previous proof).
- If $U < G$ is open, we can define the corestriction homomorphism
$$\mathrm{Cor} : H^i(U,\, A) \to H^i(G,\, A),$$
and Theorem (1.3.10) continues to hold together with its corollaries.
- Finally, if U is open and A, B are discrete G-modules the isomorphism 1.1.7 (b) is well-defined.

2.4 Cohomological Dimension

In the following, we denote by $A\{p\}$ the p-primary component of an abelian group A, that is the subgroup of elements whose order is a power of p; we instead write $A[n]$ for the n-torsion subgroup of A, i.e. the subgroup of elements killed by n. Finally, we say a non-zero discrete G-module is *simple* if it has no proper non-trivial submodules.

Definition 2.4.1 Let G be a profinite group. For p a prime number, the cohomological p-dimension $\mathrm{cd}_p\,(G)$ of G is the smallest n such that
$$H^i(G,\, A)\{p\} = 0$$
for all $i > n$ and all discrete *torsion* G-modules A. If there is no such n, we set $\mathrm{cd}_p\,(G) = \infty$. Note that the above condition is equivalent to the vanishing of the p-torsion of the corresponding cohomology groups.

The cohomological dimension of G is then defined as the supremum of the cohomological p-dimensions over all prime numbers:
$$\mathrm{cd}\,(G) := \sup_p \mathrm{cd}_p\,(G).$$

Remark 2.4.2 If the order of G is not divisible by some prime p, then the cohomological p-dimension of G is 0, as by Corollary 2.3.3 the cohomology groups in question are inductive limits of torsion groups whose order is not divisible by p.

We now develop a few helpful criterions for computing cohomological dimension:

Theorem 2.4.3 *Let G be a profinite group. For p prime and $n \in \mathbb{N}$, the following are equivalent:*

(a) $\mathrm{cd}_p\,(G) \leq n$.

(b) $H^i(G,\, A) = 0$ *for all $i > n$ and all p-primary discrete G-modules A.*

(c) $H^{n+1}(G,\, A) = 0$ *for all discrete G-modules which are p-torsion and simple as $\mathbb{Z}[G]$-modules.*

Proof. The implications (a)⇒(b) and (b)⇒(c) are clear. Moreover, (b)⇒(a) as for any $i > 0$ we have
$$H^i(G,\, A)\{p\} = H^i(G,\, A\{p\})$$
and cohomology commutes with direct sums (this follows from Theorem 2.3.2).
For the implication (c)⇒(b), we first show that $H^{n+1}(G,\, A) = 0$ for all finite p-primary G-modules by induction on $n := |A|$. Without loss of generality, assume A is non-zero. If A is

simple, then by assumption $H^{n+1}(G,\, A) = 0$. Otherwise, it has a proper non-trivial submodule B, and there is an exact sequence

$$0 \to B \to A \to A/B \to 0$$

with $|A/B|, |B| < |A|$, and we conclude by induction using the long exact sequence in cohomology. To remove the finiteness assumption, we can write any p-primary A as the inductive limit of its finitely generated sub-G-modules B_i, and since each B_i is a finitely generated torsion group, it must be finite. Therefore, $H^{n+1}(G,\, A) = 0$ for any p-primary discrete G-module A.

To get the result for every $i > n$, we argue by dimension shifting using the short exact sequence

$$0 \to A \to \mathrm{I}_G(A) \to \mathrm{I}_G(A)/A \to 0$$

and the fact that $\mathrm{I}_G(A)$ is p-primary, since continuous functions $G \to A$ are locally constant and thus have finite image by compactness. □

Lemma 2.4.4 *Let G be a finite p-group, and A a finite p-primary G-module. Then, $A^G \neq 0$.*

Proof. If $A_1, \ldots, A_k$ are the orbits of $A \setminus A^G$, then p divides $|A_i|$ and the formula

$$|A| = |A^G| + \sum_i |A_i|$$

shows that p divides $|A^G|$. □

This implies a practical characterization for the cohomological dimension of a pro-p-group:

Theorem 2.4.5 *Let G be a pro-p-group, and n a natural number. Then,*

$$\mathrm{cd}_p\,(G) \leq n \iff H^{n+1}(G,\, \mathbb{Z}/p\mathbb{Z}) = 0.$$

Proof. For the non-trivial implication, by Theorem 2.4.3 we need to show that $H^{n+1}(G,\, A) = 0$ for any simple p-torsion G-module A. We claim that any such module is isomorphic to $\mathbb{Z}/p\mathbb{Z}$: the G-module generated by any non-zero $a \in A$ is finitely generated and torsion, and by simplicity it must be all of A, so A must be finite. Therefore, the union of its stabilizers V is open in G, and its core

$$U := \bigcap_{s \in G/V} s^{-1}Vs$$

is a normal open subgroup which acts trivially on A, so we can view A as a simple G/U-module. By Corollary 2.3.3 we are down to the case of a finite p-group, where $A^G \neq 0$ by Lemma 2.4.4 and as A is simple we find $A = A^G$, so the action is trivial. Finally, any non-zero element $a \in A$ generates A by simplicity and it has order p, so $A \simeq \mathbb{Z}/p\mathbb{Z}$ as an abelian group. □

Example 2.4.6 If G is the group of p-adic integers $\mathbb{Z}_p$, by Theorem 2.3.2 we can compute

$$H^2(G,\, \mathbb{Z}/p\mathbb{Z}) = \varinjlim_n H^2(\mathbb{Z}/p^n\mathbb{Z},\, \mathbb{Z}/p\mathbb{Z})$$

where each term is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ by 1.8, and the transition maps are given by inflation:

$$H^2(\mathbb{Z}/p^n\mathbb{Z},\, \mathbb{Z}/p\mathbb{Z}) \overset{\mathrm{Inf}}{\to} H^2(\mathbb{Z}/p^{n+1}\mathbb{Z},\, \mathbb{Z}/p\mathbb{Z}). \tag{2.1}$$

Since the inflation has an explicit expression in terms of the resolution of $\mathbb{Z}$ by inhomogeneous cochains, we can compute it by extending $\mathrm{id}_{\mathbb{Z}}$ to a map between the resolutions of $\mathbb{Z}$ as a $\mathbb{Z}/p^{n+1}\mathbb{Z}$-module and a $\mathbb{Z}/p^n\mathbb{Z}$-module respectively constructed in 1.6 by Theorem 2.2.6 of [Wei94] (which says that such a lifting is unique up to chain homotopy), as $\mathbb{Z}[\mathbb{Z}/p^n\mathbb{Z}]$ is also a $\mathbb{Z}/p^{n+1}\mathbb{Z}$-module and they are thus both projective resolutions in the category of $\mathbb{Z}/p^{n+1}\mathbb{Z}$-modules. Carrying out this computation up to degree 2 of the aforementioned resolutions and denoting by s^p and s the generators of $\mathbb{Z}/p^n\mathbb{Z}$ and $\mathbb{Z}/p^{n+1}\mathbb{Z}$, we get the following diagram:

$$\begin{tikzcd}
\mathbb{Z}[\mathbb{Z}/p^{n+1}\mathbb{Z}] \arrow[r, "N"] \arrow[d, "s\mapsto ps^p"] & \mathbb{Z}[\mathbb{Z}/p^{n+1}\mathbb{Z}] \arrow[r, "s-\mathrm{id}"] \arrow[d, "s\mapsto s^p"] & \mathbb{Z}[\mathbb{Z}/p^{n+1}\mathbb{Z}] \arrow[r, "\varepsilon"] \arrow[d, "s\mapsto s^p"] & \mathbb{Z} \arrow[d, equal] \\
\mathbb{Z}[\mathbb{Z}/p^{n}\mathbb{Z}] \arrow[r, "N"] & \mathbb{Z}[\mathbb{Z}/p^{n}\mathbb{Z}] \arrow[r, "s^p-\mathrm{id}"] & \mathbb{Z}[\mathbb{Z}/p^{n}\mathbb{Z}] \arrow[r, "\varepsilon"] & \mathbb{Z}
\end{tikzcd}$$

Applying $\mathrm{Hom}(-,\mathbb{Z}/p\mathbb{Z})$ to the above diagram, we deduce that the transition maps (2.1) are induced by multiplication by p on $\mathbb{Z}/p\mathbb{Z}$, and are thus all zero. As a consequence, $H^2(G,\,\mathbb{Z}/p\mathbb{Z}) = 0$ and thus $\mathrm{cd}_p\,(\mathbb{Z}_p) \leq 1$ by Theorem 2.4.5. For the other inequality, note that

$$H^1(\mathbb{Z}_p,\,\mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}_c(\mathbb{Z}_p, \mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z} \neq 0,$$

as any homomorphism $\mathbb{Z}_p \to \mathbb{Z}/p\mathbb{Z}$ factors through $\mathbb{Z}_p/p\mathbb{Z}_p$. Therefore, $\mathrm{cd}_p\,(\mathbb{Z}_p) = 1$.

Lemma 2.4.7 *Let G be a profinite group, A a discrete G-module and p a prime number. If H is a closed subgroup of G of index prime to p, then the restriction map is injective on the p-primary component:*

$$H^i(G,\,A)\{p\} \overset{\mathrm{Res}}{\hookrightarrow} H^i(H,\,A)$$

for all $i > 0$.

Proof. By definition of index, can reduce to the case where $(G:H)$ is finite via Corollary 2.3.3. Then, the claim follows from the formula $\mathrm{Cor}\circ\mathrm{Res} = \cdot(G:H)$ of Theorem 1.3.10. □

Lemma 2.4.8 *Let G be a pro-p group of finite cohomological dimension n. Then, if A is a non-zero finite p-primary G-module, we have*

$$H^n(G,\,A) \neq 0.$$

Proof. Let $A' \subset A$ be a proper maximal sub-G-module of A. Then, ${}^{A}\!/_{A'}$ is a non-zero finite p-primary module, so by Lemma 2.4.4 the order of $({}^{A}\!/_{A'})^G$ is divisible by p, and in particular $\mathbb{Z}/p\mathbb{Z} \subset {}^{A}\!/_{A'}$, which implies $A' \subsetneq \pi^{-1}(\mathbb{Z}/p\mathbb{Z}) \subset A$. By maximality of A', we obtain $A/A' = \mathbb{Z}/p\mathbb{Z}$, and the exact sequence

$$0 \to A' \to A \to \mathbb{Z}/p\mathbb{Z} \to 0$$

induces a long exact sequence in cohomology which concludes the proof:

$$H^n(G,\,A) \to H^n(G,\,\mathbb{Z}/p\mathbb{Z}) \to 0 = H^{n+1}(G,\,A').$$

□

Proposition 2.4.9 *Let G be a profinite group. Then, for any closed subgroup H of G we have*

$$\mathrm{cd}_p\,(H) \leq \mathrm{cd}_p\,(G).$$

Furthermore, we have equality in the following cases:

- *if $p \nmid (G : H)$;*
- *if H is open and $\operatorname{cd}_p(G) < \infty$.*

Proof. The inequality follows from Shapiro's Lemma (1.3.4), which reduces the cohomology of any p-primary H-module A to that of the p-primary G-module $\operatorname{CoInd}_H^G A$.

If p does not divide $(G : H)$, then we can use Lemma 2.4.7 to reduce the cohomology of any p-primary G-module to its cohomology as an H-module, which implies the equality.

If H is open, we can reduce to the case of a pro-p-group: take a p-Sylow H_p of H and a p-Sylow G_p of G containing H_p; then, H_p is open in G_p because $G_p \cap H = H_p$. Now assume G is a pro-p-group, and set $n := \operatorname{cd}_p(G)$. Applying Shapiro's Lemma, we get

$$H^n(H, \mathbb{Z}/p\mathbb{Z}) \simeq H^n(G, \operatorname{CoInd}_H^G(\mathbb{Z}/p\mathbb{Z})) \neq 0$$

by Lemma 2.4.8 as $\operatorname{CoInd}_H^G(\mathbb{Z}/p\mathbb{Z}))$ is finite of order $p^{(G:H)}$, so $\operatorname{cd}_p(H) \geq n$ by Theorem 2.4.5 and we are done. □

Corollary 2.4.10 *If G_p is a p-Sylow of G, then*

$$\operatorname{cd}_p(G) = \operatorname{cd}_p(G_p) = \operatorname{cd}(G_p).$$

Example 2.4.11 By the above corollary and Example 2.4.6, we get $\operatorname{cd}_p(\widehat{\mathbb{Z}}) = \operatorname{cd}_p(\mathbb{Z}_p) = 1$ for any prime p, which implies $\operatorname{cd}(\widehat{\mathbb{Z}}) = 1$.

Proposition 2.4.12 *Let G be a profinite group, and $H \triangleleft G$ a normal and closed subgroup. Then, for any prime number p*

$$\operatorname{cd}_p(G) \leq \operatorname{cd}_p(H) + \operatorname{cd}_p(G/H).$$

Proof. Let $m := \operatorname{cd}_p(H)$ and $n := \operatorname{cd}_p(G/H)$, and assume that $m, n < \infty$. The claim then follows from the Hochschild-Serre spectral sequence: if A is a p-primary discrete G-module, we want to show that the cohomology of G with coefficients in A vanishes in degree greater than $\operatorname{cd}_p(H) + \operatorname{cd}_p(G/H)$. The spectral sequence reads

$$E_2^{i,j} = H^i(G/H, H^j(H, A)) \Rightarrow H^{i+j}(G, A),$$

and $E_2^{i,j}$ vanishes for $i > \operatorname{cd}_p(G/H)$ or $j > \operatorname{cd}_p(H)$ by assumption. Thus, if $i + j$ is greater than $\operatorname{cd}_p(H) + \operatorname{cd}_p(G/H)$, we have $H^{i+j}(G, A) = 0$ as it admits a filtration by successive quotients of subquotients of the terms on the left hand side. □

2.5 Galois Cohomology

In this chapter, we denote by $\overline{K}$ the separable closure of a field K, and by Γ_K the absolute Galois group $\operatorname{Gal}(\overline{K}/K)$. If M is a discrete Γ_K-module and L/K is a Galois extension, fixing an inclusion $\overline{K} \overset{\iota}{\hookrightarrow} \overline{L}$ which extends $K \hookrightarrow L$ produces a continuous homomorphism

$$\varphi : \Gamma_L \to \Gamma_K$$

and by functoriality a homomorphism

$$\varphi^* : H^i(\Gamma_K, M) \to H^i(\Gamma_L, M).$$

If we change the inclusion ι, this changes φ by an inner automorphism of Γ_K, which by Proposition 1.3.6 induces the identity in cohomology, and therefore φ^* is independent of the choice of ι. This shows that different separable closures of K yield *canonically* isomorphic cohomology groups. For this reason, we are led to adopt the following notation:

$$H^i(K,\,M) := H^i(\Gamma_K,\,M).$$

The additive group is cohomologically trivial:

Proposition 2.5.1 *Let L/K be a finite Galois extension of fields with group $G = \mathrm{Gal}\,(L/K)$. Then,*

$$H^i(G,\,L) = 0$$

and

$$H^i(K,\,\overline{K}) = 0$$

for all $i > 0$.

Proof. By the Normal Basis Theorem, we know that L is isomorphic to $K[G] \simeq K \otimes_{\mathbb{Z}} \mathbb{Z}[G]$ as a G-module, and since G is finite we can use the isomorphism (1.1) to conclude that L is the induced module $\mathrm{I}_G(K)$, which is cohomologically trivial by Corollary 1.3.5.

The second claim then follows by Corollary 2.3.3:

$$H^i(K,\,\overline{K}) = \varinjlim_{\substack{L/K \\ \text{fin. Galois}}} H^i(\mathrm{Gal}\,(L/K),\,L) = 0.$$

□

Proposition 2.5.2 (Artin-Schreier) *Let K be a field of characteristic $p > 0$, and consider the map $\Phi(x) := x^p - x$ from $\overline{K}$ to itself. Then,*

$$H^1(K,\,\mathbb{Z}/p\mathbb{Z}) \simeq {}^{K}\!/_{\Phi(K)}$$

and $H^i(K,\,\mathbb{Z}/p\mathbb{Z}) = 0$ for $i > 1$.

Proof. Note that Φ is additive because we are in characteristic p, and it is surjective because $\overline{K}$ is separably closed and the polynomial $X^p - X - a$ is separable for any $a \in \overline{K}$. The kernel of Φ is the prime subfield of K, which is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ as a Γ_K-module. The result then follows from the short exact sequence of Γ_K-modules

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \overline{K} \overset{\Phi}{\to} \overline{K} \to 0,$$

from which we get a long exact sequence in cohomology

$$\begin{aligned} 0 \to \mathbb{Z}/p\mathbb{Z} \to K \xrightarrow{\Phi} K \to & H^1(K,\,\mathbb{Z}/p\mathbb{Z}) \to 0 = H^1(K,\,\overline{K}) \\ & \longrightarrow 0 \to H^2(K,\,\mathbb{Z}/p\mathbb{Z}) \to 0 \to \dots \end{aligned}$$

□

Hilbert 90

We now consider the multiplicative group of a field as a discrete module with the Galois action:

Theorem 2.5.3 (Hilbert 90) *Let L be a finite Galois extension of K with Galois group G. Then, $H^1(G,\, L^\times) = 0$ and $H^1(K,\, \overline{K}^\times) = 0$.*

Proof. The second claim follows from the first, as by Corollary 2.3.3

$$H^1(K,\, \overline{K}^\times) = \varinjlim H^1(\mathrm{Gal}\,(L/K),\, L^\times)$$

where the limit is taken over all finite Galois extensions L/K.

Now let $(s \mapsto a_s) \in Z^1(G, L^\times)$ be a cocycle. The cocycle condition translates to

$$a_{st} = a_s \cdot s(a_t) \iff s(a_t) = a_s^{-1} a_{st}.$$

By Dedekind's Theorem on independence of characters, there is some $c \in L^\times$ such that

$$b := \sum_{t \in G} a_t \cdot t(c) \in L^\times$$

is non-zero. Then, for any $s \in G$ the computation

$$s(b) = \sum_{t \in G} s(a_t) \cdot (st)(c) = \sum_{t \in G} a_s^{-1} a_{st} \cdot (st)(c) = a_s^{-1} b$$

shows that $(s \mapsto a_s)$ is a coboundary: $a_s = {}^{s(b^{-1})}/_{b^{-1}}$. □

Kummer Theory

Let K be a field which contains a primitive n-th root of unity. Then, Kummer theory classifies the abelian extensions of K whose exponent divides n: it states that any such an extension is obtained by adjoining n-roots, that is roots of polynomials of the form $X^n - a$ for some $a \in K^\times$. For instance, if $\overline{a}$ has order m in $K^\times$ modulo the n-th powers $K^{\times n}$, then $K(\sqrt[n]{a})$ is a cyclic extension of degree m.

We can reinterpret this result using group cohomology:

Proposition 2.5.4 *Let K be a field and assume that n is invertible in K. If μ_n is the group of all n-th roots of unity in $\overline{K}$, then we have an isomorphism*

$$H^1(K,\, \mu_n) \simeq {}^{K^\times}/_{K^{\times n}}.$$

Proof. As the map $x \mapsto x^n$ is surjective on $\overline{K}^\times$, we have a short exact sequence

$$1 \to \mu_n \to \overline{K}^\times \xrightarrow{\cdot n} \overline{K}^\times \to 1$$

which gives rise to a long exact sequence in cohomology:

$$0 \to \mu_n(K) \to K^\times \xrightarrow{\cdot n} K^\times \to H^1(K,\, \mu_n) \to 0$$

Here $\mu_n(K)$ is the group of n-th roots of unity contained in K, and the last term vanishes by Hilbert 90. By exactness, we conclude that $H^1(K,\, \mu_n) \simeq {}^{K^\times}/_{K^{\times n}}$. □

Remark 2.5.5 When K contains a primitive n-th root of unity, the action of Γ_K on μ_n is trivial, so we can identify $H^1(K,\, \mu_n)$ with

$$H^1(K,\, \mathbb{Z}/n\mathbb{Z}) = \mathrm{Hom}_c(\Gamma_K, \mathbb{Z}/n\mathbb{Z}).$$

For any such homomorphism $\Gamma_K \xrightarrow{f} \mathbb{Z}/n\mathbb{Z}$, the kernel of f is a closed normal subgroup, to which we can associate (by Galois theory) an abelian extension L of K:

$$\mathrm{Gal}\,(L/K) \simeq {}^{\Gamma_K}/_{\ker f} \hookrightarrow \mathbb{Z}/n\mathbb{Z}.$$

We thus recover the Kummer correspondence for cyclic extensions of degree diving n.

Brauer Group of a Field

Definition 2.5.6 Let K be a field. The *Brauer group* of K is

$$\mathrm{Br}\,(K) := H^2(K,\, \overline{K}^\times).$$

Given an extension L/K, by functoriality we have a map $\mathrm{Br}\,(K) \to \mathrm{Br}\,(L)$, which is well-defined by the the discussion at the beginning of the chapter.

Remark 2.5.7 The Brauer group of a field K can also be described as the group of equivalence classes of finite-dimensional central simple algebras over K. This is a very rich theory which allows one to do explicit computations, as we will see in the next chapter. However some of the properties of the Brauer group are more easily derived via the cohomological approach (such as the fact that it is a torsion group). For the equivalence between the two definitions, see [GS06] §4.4.

Proposition 2.5.8 *Let n be a positive integer which is invertible in K. Then, the n-torsion of the Brauer group is the cohomology of the group μ_n of n-th roots of unity:*

$$\mathrm{Br}\,(K)[n] = H^2(K,\, \mu_n).$$

If moreover K contains μ_n, then the action of Γ_K on μ_n is trivial, and we deduce

$$\mathrm{Br}\,(K)[n] \simeq H^2(K,\, \mathbb{Z}/n\mathbb{Z})$$

by choosing a generator of μ_n.

Proof. This follows from the Kummer exact sequence

$$1 \to \mu_n \to \overline{K}^\times \xrightarrow{\cdot n} \overline{K}^\times \to 1,$$

by inspecting the long exact sequence in cohomology and using Hilbert 90:

$$H^1(K,\, \overline{K}^\times) = 0 \to H^2(K,\, \mu_n) \to \mathrm{Br}\,(K) \xrightarrow{\cdot n} \mathrm{Br}\,(K) \to 0.$$

□

Example 2.5.9

(a) Let K be a separably closed field. Then, $\Gamma_K = 0$ and thus $\mathrm{Br}\,(K) = 0$.

(b) The Brauer group of a finite field $\mathbb{F}_q$ is trivial, because $\mathrm{Gal}\,(\overline{\mathbb{F}_q}/\mathbb{F}_q) = \widehat{\mathbb{Z}}$ has cohomological dimension 1 by Example 2.4.11.

(c) Using the cohomology of cyclic groups, we can compute the Brauer group of $\mathbb{R}$:

$$\mathrm{Br}\,(\mathbb{R}) = H^2(\mathrm{Gal}\,(\mathbb{C}/\mathbb{R}),\, \mathbb{C}^\times) \overset{1.7}{=} \mathbb{R}^\times/\mathbb{R}_{>0} \simeq \mathbb{Z}/2\mathbb{Z},$$

where we used the fact that the norm map $N(x) = x\overline{x}$ has image $\mathbb{R}_{>0}$.

Cohomological Dimension of a Field

Definition 2.5.10 Let K be a field with absolute Galois group Γ_K and fix a prime number p. If the characteristic of K is different from p or K is perfect of char $K = p$, then the **cohomological dimension** of K is

$$\mathrm{cd}\,(K) := \mathrm{cd}\,(\Gamma_K).$$

The above restriction on the characteristic of K is justified by the following fact:

Proposition 2.5.11 *If K is a field of positive characteristic p, then $\mathrm{cd}_p\,(K) \leq 1$.*

Proof. Consider a p-Sylow subgroup G_p of Γ_K. Then, G_p is of the form $\mathrm{Aut}_L\,(\overline{K})$ for some intermediate extension $K \subset L \subset \overline{K}$. By Corollary 2.4.10, $\mathrm{cd}\,(K) = \mathrm{cd}\,(G_p)$, and thanks to the criterion 2.4.5 it's enough to show

$$H^2(L,\, \mathbb{Z}/p\mathbb{Z}) = 0,$$

which follows from Artin-Schreier (2.5.2) as L is a field of characteristic p. □

Proposition 2.5.12 *Let K be a field and p a prime different from the characteristic of K. Then, the following are equivalent:*

(a) $\mathrm{cd}_p\,(K) \leq 1$,

(b) $\mathrm{Br}\,(L)[p] = 0$ *for any algebraic separable extension L/K.*

(c) $\mathrm{Br}\,(L)[p] = 0$ *for any finite separable extension L/K.*

Proof. Suppose (a), and let L be a separable algebraic extension of K. By Galois theory, L corresponds to a closed subgroup H of Γ_K, and by Proposition 2.4.9 we have

$$\mathrm{cd}_p\,(L) \leq \mathrm{cd}_p\,(K) \leq 1.$$

Therefore, by Proposition 2.5.8 we get $\mathrm{Br}\,(L)[p] = H^2(L,\, \mu_p) = 0$. The implication (b)⇒(c) is immediate.

Finally, if (c) holds, consider a p-Sylow G_p of Γ_K and set $K_p := \overline{K}^{G_p}$. Then, the p-th roots of unity of $\overline{K}$ are contained in K_p: indeed, the degree $[K_p(\mu_p) : K_p]$ is a power of p by Galois correspondence, but it must divide $p-1$; therefore, $H^2(K,\, \mathbb{Z}/p\mathbb{Z}) = H^2(K_p,\, \mu_p)$. Now, given a finite separable extension $K \subset E \subset K_p$ which contains μ_p, by hypothesis we have $\mathrm{Br}\,(E)[p] = 0$. Since we can write K_p as the union of such extensions, we deduce

$$\bigcap_{\substack{E \text{ fin. sep. over } K \\ \mu_p \subset E \subset K_p}} \mathrm{Gal}\,(\overline{K}/E) = \Gamma_{K_p},$$

and by Example 2.3.6 we can compute

$$H^2(K_p,\, \mathbb{Z}/p\mathbb{Z}) = H^2(K_p,\, \mu_p) = \varinjlim_E H^2(E,\, \mu_p) = \varinjlim_E \mathrm{Br}\,(E)[p] = 0.$$

Using the criterion 2.4.5 and Corollary 2.4.10, we conclude that $\mathrm{cd}_p\,(K) = \mathrm{cd}_p\,(K_p) \leq 1$. □

Chapter 3

Local Fields

In this chapter we are going to recall some notions of algebraic number theory over local fields, that is fields which are complete with respect to a discrete valuation with finite residue field. These fields turn out to be isomorphic to a finite extension of either the p-adic numbers $\mathbb{Q}_p$ or the Laurent series $\kappa((t))$ over a finite field κ.

We will see how to describe the structure of local fields by looking at certain filtrations of their units, how the extensions of their residue field is related to unramped extensions of the field itself, and compute their Brauer group. The exposition of these topics will mainly follow [Ser79].

3.1 Complete Discretely Valued Fields

Let A be a *discrete valuation ring* (or DVR), that is a local principal ideal domain of Krull dimension 1. If $\mathfrak{m}$ is its maximal ideal we denote by κ its residue field; a generator π of $\mathfrak{m}$ is said to be a *uniformizer* of A. Since A is local, the group of invertible elements $A^\times$ is just $A \setminus \mathfrak{m}$.

It follows that every non-zero element x of A can be written uniquely as

$$x = u \cdot \pi^n \tag{3.1}$$

for some $u \in A^\times$ and $n \in \mathbb{N}$; by setting $v(x) := n$ and $v(0) := \infty$ we get a **valuation** on A, that is a map $v : K := \mathrm{Frac}\,(A) \to \mathbb{Z} \cup \{\infty\}$ which satisfies

- $v(x) = \infty$ if and only if $x = 0$,
- $v(xy) = v(x) + v(y)$,
- $v(x + y) \geq \min\{v(x), v(y)\}$.

(to extend the valuation to the field of fractions K of A we just set $v(x/y) = v(x) - v(y)$).

In this situation, A is said to be the *ring of integers* of K, that is the subring of K consisting of elements with non-negative valuation. Note that $A^\times$ consists of the elements of A whose valuation is zero.

Remark 3.1.1 If K has positive characteristic p, then the residue field κ has to be a finite field of characteristic p. In the same way, if κ has characteristic 0 then the characteristic of K is necessarily 0. These are the *equal characteristic* cases; however, there are important examples where $\mathrm{char}\, K = 0$ but $\mathrm{char}\, \kappa = p$ (the *mixed characteristic* case):

Example 3.1.2 (Discrete Valuation Rings)

- If p is a prime number, then the localization $\mathbb{Z}_{(p)}$ of $\mathbb{Z}$ at the ideal (p) is a discrete valuation ring, with maximal ideal (p), fraction field $\mathbb{Q}$ and residue field $\mathbb{Z}/p\mathbb{Z}$. The valuation is induced by the p-adic valuation on $\mathbb{Z}$, which assigns to a non-zero integer x the largest integer n such that p^n divides x.

- The ring of *p-adic integers* $\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ is a discrete valuation ring with maximal ideal (p) and residue field $\mathbb{Z}/p\mathbb{Z}$. It is the completion of $\mathbb{Z}_{(p)}$ with respect to its maximal ideal, and its units are the elements $u = (u_n)$ with $u_1 \neq 0$. The valuation of a non-zero element $x = (x_n)$ is 0 if $x \in \mathbb{Z}_p^\times$, and the largest n such that $x_n = 0$ otherwise. Its fraction field $\mathbb{Q}_p$ is called the field of *p-adic numbers.*

- The ring of formal power series $\kappa[[t]$ with coefficients in a field κ is a discrete valuation ring, with the valuation of a non-zero power series $\sum_{n\geq 0} a_n t^n$ being the smallest n such that $a_n \neq 0$. Its residue field is $\kappa = \kappa[[t]]/(t)$, and its fraction field is the field of *Laurent series* $\kappa((t))$.

Let a be a real number between 0 and 1. Given a discrete valuation ring A, the valuation v on its fraction field K defines an **ultrametric absolute value** on K by setting $|x| = a^{v(x)}$ for $x \in K$ (and $|0| = 0$). This absolute value satisfies the following properties, and makes K into a totally disconnected metric space with the distance $d(x, y) = |x - y|$:

- $|x| = 0 \iff x = 0$,
- $|xy| = |x| \cdot |y|$,
- $|x + y| \leq \max\{|x|, |y|\}$.

We can now talk about *local fields*:

Definition 3.1.3 A **local field** is a field K which is complete with respect to a discrete valuation and has a finite residue field.

The following proposition (Prop. 1 of [Ser79], Ch. II) motivates this definition:

Proposition 3.1.4 *A discretely valued field K is locally compact with respect to the topology induced by the above distance if and only if it is complete and its residue field is finite. In this case, its ring of integers A is compact, and therefore $(A, +)$ is a profinite abelian group by 2.1.2.*

Example 3.1.5

- If κ is a field, then $\kappa((t))$ is complete, and it's locally compact if and only if κ is a finite field.

- The fraction field $\mathbb{Q}$ of $\mathbb{Z}_{(p)}$ from Example 3.1.2 is not complete with respect to the p-adic valuation: its completion is the local field $\mathbb{Q}_p$.

Extensions

Let now K be a field complete with respect to a discrete valuation v, A its ring of integers and $\kappa = A/\mathfrak{m}$ its residue field. Given a finite extension L of K, the integral closure B of A in L is a discrete valuation ring and free A-module of rank $[L : K]$, whose induced topology on L makes it complete. Moreover, there exists a unique discrete valuation w on L inducing the same topology of v on K.

If $\mathfrak{n}$ is the maximal ideal of B, then $\mathfrak{m}B = \mathfrak{n}^e$ for some $e > 0$, called the *ramification index* of the extension. The degree of the field extension $f := [B/\mathfrak{n} : \kappa]$ is the *residual degree* of the extension, and we have the following relations:

- $[L:K]=e\cdot f$
- $w(x)=e\cdot v(x)$ for all $x\in K$.

Definition 3.1.6 With the above notation, the extension L/K is said to be *unramified* if $e=1$ and $B/\mathfrak{n}$ is separable over κ (for instance when κ is perfect), and *totally ramified* if $f=1$.

Example 3.1.7

- Let κ be a field. Then, the finite unramified extensions of $\kappa((t))$ are of the form $\kappa'((t))$ for κ' a finite separable extension of κ.
- The fields $\kappa((t^{1/n}))$ for some $n>0$ give examples of totally ramified extensions of $\kappa((t))$

Galois Theory

After discussing extensions, we present the Galois theory of a complete discretely valued field, under the additional assumption that its residue field is perfect. The main result is summarized by the following Theorem (Thm. 2 of [Ser79], Ch. III):

Theorem 3.1.8 *Let K be a field complete for a discrete valuation with perfect residue field κ, and fix a separable closure $\overline{K}$ of K. Then,*

- *for any finite extension κ' of κ, there exists a unique (up to isomorphism) finite unramified extension $L\subset\overline{K}$ of K with residue field κ', which is Galois if and only if k/k' is.*
- *Let $\overline{\kappa}$ be an algebraic closure of κ, and define $K_{nr}\subset\overline{K}$ to be the inductive limit of the unramified extensions of K which correspond to finite subextensions of $\overline{\kappa}$. Then, K_{nr} is a Galois extension of K with Galois group $\mathrm{Gal}\,(K_{nr}/K)\simeq\mathrm{Gal}\,(\overline{\kappa}/\kappa)$.*

The field K_{nr} is called the *maximal unramified extension* of K. If $\overline{K}$ is a separable closure of K, the subgroup

$$I:=\mathrm{Gal}\,(\overline{K}/K_{\mathrm{nr}})<\mathrm{Gal}\,(\overline{K}/K)$$

is called the *inertia group* I of K.

Example 3.1.9 If K is a local field with residue field $\kappa=\mathbb{F}_q$, then for any integer $n>0$, there is a unique extension of κ of degree n, which is cyclic with Galois group $\mathbb{Z}/n\mathbb{Z}$ (namely $\mathbb{F}_{q^n}$). It follows that

$$\mathrm{Gal}\,(K_{\mathrm{nr}}/K)\simeq\mathrm{Gal}\,(\overline{\kappa}/\kappa)\simeq\widehat{\mathbb{Z}}.$$

In particular, there is an automorphism of K_{nr} which corresponds to the Frobenius automorphism $x\mapsto x^q$ of $\overline{\kappa}$.

3.2 Structure of Local Fields

The following theorem gives a classification of local fields based on their characteristic (see Thm. 2 and 4 of [Ser79], Ch. II):

Theorem 3.2.1 *Let K be a field complete with respect to a discrete valuation with finite residue field κ of characteristic $p>0$. Then,*

- *if K has characteristic 0, it is isomorphic to a finite extension of $\mathbb{Q}_p$ (which we call a **p-adic field**),*

- *if K has characteristic p, it is isomorphic to the field of Laurent series $\kappa((t))$.*

Now, let K be a complete discretely valued field with ring of integers $\mathcal{O}_K$ and residue field κ; we are interested in the structure of multiplicative group $K^\times$. However, it's enough to determine the structure of the group of units $U_K := \mathcal{O}_K^\times$, since after fixing an uniformizer (3.1) yields an isomorphism $K^\times \simeq \mathbb{Z} \times U_K$, or equivalently a splitting for the the following exact sequence:

$$1 \to U_K \to K^\times \xrightarrow{v} \mathbb{Z} \to 0. \tag{3.2}$$

Note that $\mathcal{O}_K$ has a basis of closed neighborhoods of 0 given by the subgroups $\mathfrak{m}^n$ for $n \in \mathbb{N}$, where $\mathfrak{m}$ is the maximal ideal of $\mathcal{O}_K$. Analogously, the group of units $U_K := \mathcal{O}_K^\times$ has a basis of closed neighborhoods of 1 given by the subgroups

$$U_K^j := 1 + \mathfrak{m}^j,$$

as they define a filtration $U_K = U_K^0 \supset U_K^1 \supset U_K^2 \supset \dots$ of U_K with $\bigcap_j U_K^j = \{1\}$. Furthermore, since U_K is closed in $K^\times$ and thus complete, we have $U_K = \varprojlim_j U_K/U_K^j$.

Now, the reduction map $U_K \to \kappa^\times$ induces a short exact sequence

$$1 \to U_K^1 \to U_K \to \kappa^\times \to 1, \tag{3.3}$$

so that U_K/U_K^1 is isomorphic to the multiplicative group $\simeq \kappa^\times$. Analogously, the surjective map

$$\begin{aligned} U_K^n &\to \kappa \\ 1 + u\pi^n &\mapsto \overline{u} \end{aligned}$$

induces a short exact sequence

$$1 \to U_K^{n+1} \to U_K^n \to \kappa \to 0,$$

which shows that the successive quotients U_K^n/U_K^{n+1} are isomorphic to the additive group κ.

Suppose now that K is a local field with residue field κ of characteristic $p > 0$. Then, the subgroups $(\mathfrak{m}^n)$ and (U_K^j) are open in $\mathcal{O}_K$ and U_K respectively; in particular, U_K is a profinite group, and the group of *principal units* $U_K^1 = \varprojlim_{j \geq 1} U_K^1/U_K^j$ is thus a pro-p group. Moreover, the exact sequence 3.3 splits thanks to (a version of) **Hensel's lemma**:

Proposition 3.2.2 *Let K be a field complete for a discrete valuation, with A its ring of integers and residue field κ. Given a polynomial $f \in A[x]$, any simple root of its reduction $f \in \kappa[x]$ lifts uniquely to a root of f.*

Indeed, as $\kappa^\times$ is cyclic of order m prime to p, by Hensel's lemma the polynomial $x^m = 1$ has m distinct roots in U_K, which gives the desired section; we get an isomorphism

$$U_K \simeq U_K^1 \times \kappa^\times. \tag{3.4}$$

In the case of a p-adic field, we can finally explicit the structure of $K^\times$:

Theorem 3.2.3 *If K is a p-adic field with $[K : \mathbb{Q}_p] = n$ and ramification index e over $\mathbb{Q}_p$, then*

$$U_K^m \subset K^p$$

for all $m > \frac{e}{p-1}$. Moreover, we have the following decomposition of the group of principal units:

$$U_K^1 \simeq \mathbb{Z}_p^n \times F,$$

where F is a finite cyclic group of order a power of p. By (3.2) and (3.4), this determines the structure of $K^\times$:

$$\begin{aligned} K^\times &\simeq \mathbb{Z} \times U_K \\ &\simeq \mathbb{Z} \times \mathbb{Z}_p^n \times F \times \kappa^\times. \end{aligned}$$

We omit the proof, which is a direct consequence of [Ser79], Ch. XIV, Prop. 9 and 10.

Using this result, we can show that the n-th powers in $K^\times$ are open:

Corollary 3.2.4 *Let K be a p-adic field. Then, for any $n > 0$ the subgroup $K^{\times n} < K^\times$ of n-th powers is open.*

Proof. If n is not divisible by p, then we can use Hensel's lemma to show that $K^{\times n}$ contains the principal units U_K^1, which are open in $K^\times$: for any $a \in U_K^1$, the polynomial $x^n - a$ reduces to $x^n - 1$ in $\kappa[x]$. Since 1 is a root of the latter and n is invertible in κ, we can lift it to a root of $x^n - a$ in $K^\times$.

As for the case $n = p^k$, since U_K^m is open in $K^\times$ for any m, it's enough to show that $(U_K^m)^{p^k}$ is open in U_K^m. Then, using Prop. 9 of loc. cit. again we find that for $m > \frac{e}{p-1}$ the map $x \mapsto x^{p^k}$ is an isomorphism of U_K^m onto U_K^{m+ke}, which concludes. □

Remark 3.2.5 If K is a local field of characteristic $p > 0$, then K^{*p} cannot be not open in $K^\times$, otherwise it would contain U_K^m for m large enough and then $x^p = \pi^m + 1$ would give $(x-1)^p = \pi^m$, which yields a contradiction whenever $(m, p) = 1$. However, if n is prime to p then $K^{\times n}$ is still open in $K^\times$ by Hensel's lemma, as in the previous corollary.

3.3 The Brauer Group of a Local Field

We now explain how to compute the Brauer group of a local field, following §6.3 of [GS06]. Recall from Remark 2.5.7 the interpretation of the Brauer group as equivalence classes of central simple algebras, which is crucial in the following. We first reduce to the relative Brauer group of the maximal unramified extension K_{nr} of K, for which we only need κ to be perfect:

Proposition 3.3.1 *Let K be a complete discretely valued field with perfect residue field κ, and K_{nr} its maximal unramified extension with Galois group $G = \mathrm{Gal}\,(K_{nr}/K)$. Then, the inflation map*

$$H^2(G,\, K_{nr}^\times) \to H^2(K,\, \overline{K}^\times) = \mathrm{Br}\,(K)$$

is an isomorphism.

Proof. (Sketch) Since G is the quotient of the absolute Galois group Γ_K of K by the inertia group $\mathrm{Gal}\,(\overline{K}/K_{\mathrm{nr}})$, the Hochschild-Serre spectral sequence yields the inflation-restriction exact sequence

$$0 \to H^2(G,\, K_{\mathrm{nr}}^\times) \to H^2(K,\, \overline{K}^\times) \to H^2(K_{\mathrm{nr}},\, \overline{K}^\times).$$

It's enough to show that the last term is trivial, but $H^2(K_{\mathrm{nr}},\, \overline{K}^\times) = \mathrm{Br}\,(K_{\mathrm{nr}})$ is zero by Corollary 2.9.4 of [GS06], which shows the existence of an unramified splitting field for any central simple algebra over K, using the reduced norm to extend the valuation of K to a central division algebra D equivalent to A, and showing that D has a maximal (and thus splitting) unramified subfield. □

As the valuation of K extends uniquely to a valuation on K_{nr}, we have a exact sequence of G-modules which splits as in (3.2):

$$1 \to U_{\mathrm{nr}} \to K_{\mathrm{nr}}^{\times} \to \mathbb{Z} \to 1,$$

with U_{nr} the group of units of K_{nr}. This induces a split exact sequence in cohomology, which in degree 2 reads

$$1 \to H^2(G,\, U_{\mathrm{nr}}) \to H^2(G,\, K_{\mathrm{nr}}^{\times}) \to H^2(G,\, \mathbb{Z}) \to 1. \tag{3.5}$$

Let's compute each term: using the long exact sequence in cohomology associated with the short exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

and by Corollary 1.3.12, we have an isomorphism of $H^2(G,\, \mathbb{Z})$ with $H^1(G,\, \mathbb{Q}/\mathbb{Z})$, which are just the continuous homomorphisms from G to $\mathbb{Q}/\mathbb{Z}$. Recall from Example 3.1.9 of the previous section that $G = \mathrm{Gal}\,(\overline{\kappa}/\kappa) \simeq \widehat{\mathbb{Z}}$, and so

$$H^2(G,\, \mathbb{Z}) = \mathrm{Hom}\,(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Q}/\mathbb{Z}.$$

Morever, using the profinite structure of the group of principal units U_K^1 one shows (as in Proposition 6.3.1 of [GS06]) that $H^2(G,\, U_{\mathrm{nr}})$ is isomorphic to the Brauer group of the residue field $\mathrm{Br}\,(\kappa) = H^2(\kappa,\, \overline{\kappa}^{\times})$.

Finally, the content of the previous proposition is that the middle term is isomorphic to $\mathrm{Br}\,(K)$, so that (3.5) becomes

$$1 \to \mathrm{Br}\,(\kappa) \to \mathrm{Br}\,(K) \to \mathbb{Q}/\mathbb{Z} \to 1.$$

The first term is trivial by Example 2.5.9 (b), and we get a canonical isomorphism

$$\mathrm{Br}\,(K) \simeq \mathbb{Q}/\mathbb{Z}. \tag{3.6}$$

We also need the following compatibility of the Brauer group isomorphism:

Proposition 3.3.2 *Let K be a local field and L/K a finite separable extension. Then, the restriction map*

$$\mathrm{Res} : \mathrm{Br}\,(K) \to \mathrm{Br}\,(L)$$

corresponds to multiplication by $[L : K]$ on $\mathbb{Q}/\mathbb{Z}$, and the corestriction map

$$\mathrm{Cor} : \mathrm{Br}\,(L) \to \mathrm{Br}\,(K)$$

corresponds to the identity of $\mathbb{Q}/\mathbb{Z}$.

Proof. (Sketch)

The second statament follows from the first, thanks the formula $\mathrm{Cor} \circ \mathrm{Res} = [L : K]$ (Theorem 1.3.10).

The first statement can be shown by considering an unramified extension of K contained in L, as the procyclic structure absolute Galois group of its residue field makes the computation of the corestriction straightforward (see Proposition 6.3.7 of [GS06]). □

Corollary 3.3.3 *In the situation of the previous proposition, if $n = [L : K]$ then an element $a \in \mathrm{Br}\,(K)$ has trivial image in $\mathrm{Br}\,(L)$ if and only if $n \cdot a = 0$.*

3.4 Cohomological Dimension

We now use these results to compute the cohomological dimension of Γ_K:

Proposition 3.4.1 *Let K be a local field, and L an algebraic separable extension of K. If $l^\infty \mid [L : K]$ for some prime l, then $\mathrm{cd}_l\,(\Gamma_L) \leq 1$ and $\mathrm{Br}\,(L)\{l\} = 0$.*

Proof. If $l = \mathrm{char}\,K$, then we have seen that $\mathrm{cd}_l\,(\Gamma_L) \leq 1$ automatically (Proposition 2.5.11). Otherwise, by Proposition 2.5.12 it's enough to show that $\mathrm{Br}\,(L)\{l\} = 0$ (we should check it for any algebraic separable extension of L, but the degree of any such extension is again divisible by l^∞). Now, as in Example 2.3.6 we can write the Brauer group of L as the inductive limit of the Brauer groups of its finite subextensions

$$\mathrm{Br}\,(L) = \varinjlim_{\substack{K \subset E \subset L \\ E \text{ finite}}} \mathrm{Br}\,(E),$$

where the transition maps are given by restriction. Given such an intermediate field E and an element $\alpha \in E$ killed by l^m for some $m > 0$, we can find a finite extension F of E such that $l^m \mid [F : E]$ (since $l^\infty \mid [L : E]$). In other words, α is killed by the degree of F over E, so by Corollary 3.3.3 it has trivial image in $\mathrm{Br}\,(F)$, and a fortiori in $\mathrm{Br}\,(L)$.

□

Corollary 3.4.2 *The cohomological dimension of the inertia group $I := \mathrm{Gal}\,(\overline{K}/K_{nr})$ of K is at most 1.*

Proof. We just apply the previous proposition to the maximal unramified extension K_{nr} of K: as $\mathrm{Gal}\,(K_{\mathrm{nr}}/K) \simeq \widehat{\mathbb{Z}}$, we have that $l^\infty \mid [K_{\mathrm{nr}} : K]$ for any prime l. □

Theorem 3.4.3 *If l is a prime different from the characteristic of K, then the cohomological l-dimension of K equals 2. In particular, $\mathrm{cd}\,(K) = 2$.*

Proof. This is a consequence of the inequality 2.4.12: we have

$$\mathrm{cd}_l\,(K) \leq \mathrm{cd}_l\,(I) + \mathrm{cd}_l\,(\Gamma_K/I) \leq 2$$

as $\mathrm{cd}_l\,(I) \leq 1$ by the previous corollary, and $\mathrm{cd}_l\,(\Gamma_K/I) = 1$ by Example 2.4.11 because Γ_K/I is the absolute Galois group of the residue field κ.

Moreover, if $l \neq \mathrm{char}\,K$, then Proposition 2.5.8 implies $H^2(K,\, \mu_l) = \mathrm{Br}\,(K)[l]$, which is non-trivial by (3.6). Therefore, $\mathrm{cd}_l\,(K) = 2$ by the usual criterion for cohomological dimension. □

3.5 Cohomological Finiteness

We now specialize to the case of a p-adic field K, by first showing that the cohomology groups of μ_n are all finite:

Theorem 3.5.1 *Let K be a p-adic field and n a positive integer. Then,*

- *$H^1(K,\, \mu_n) \simeq K^\times/K^{\times n}$ is a finite group,*
- *$H^2(K,\, \mu_n) \simeq \mathbb{Z}/n\mathbb{Z}$, and*
- *$H^i(K,\, \mu_n) \simeq 0$ for $i \geq 3$.*

In particular, $H^i(K,\, \mu_n)$ is finite for all i (for $i = 0$ it's just the invariants of μ_n).

Proof. The first isomorphism follows from Kummer Theory (Proposition 2.5.4). We can show that $K^\times/_{K^{\times n}}$ is finite using the structure theorem for local fields 3.2.3:

$$\begin{aligned} K^\times/K^{\times n} &\simeq \mathbb{Z}/n\mathbb{Z} \times \times \mathbb{Z}_p^{[K:\mathbb{Q}_p]}/n\mathbb{Z}_p^{[K:\mathbb{Q}_p]} \times F/F^n \times \kappa^\times/_{\kappa^{\times n}} \\ &\simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times F/F^n \times \kappa^\times/_{\kappa^{\times n}}. \end{aligned}$$

Since both $\kappa^\times$ and F are finite groups, we are done.

For second isomorphism, $H^2(K,\, \mu_n)$ is equal to the n-torsion of $\mathrm{Br}\,(K)$ by Proposition 2.5.8, which is isomorphic to $\mathbb{Q}/\mathbb{Z}$, so that

$$H^2(K,\, \mu_n) = \mathrm{Br}\,(K)[n] \simeq \tfrac{1}{n}\mathbb{Z}/\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}.$$

Finally, we have shown in the previous section that the absolute Galois group of a p-adic field has cohomological dimension 2, and since μ_n is torsion we are done. □

Remark 3.5.2 If K is a local field of characteristic $p > 0$, the groups $H^1(K,\, \mathbb{Z}/p\mathbb{Z}) = K/\Phi(K)$ and $K^\times/K^{\times p}$ are both infinite. However, for all n prime to p the group $H^1(K,\, \mu_n)$ is finite, asthe n-th powers are open in $K^\times \simeq \mathbb{Z} \times U_K$ by Remark 3.2.5 and U_K is profinite. For such n, we can apply proposition 2.5.8 and thus Theorem 3.5.1 continues to hold; analogously, the following corollary also holds in positive characteristic if the order of M is prime to p:

Corollary 3.5.3 *If K is a p-adic field and M is a finite Γ_K-module, then $H^i(K,\, M)$ is finite for all i.*

Proof. Let $M = \{m_1, \ldots, m_n\}$. Then, the union of the stabilizers of the m_i is an open subgroup U of Γ_K which acts trivially on M, as does its core $V = \bigcap_{s \in \Gamma_K/U} s^{-1}Us$. By Galois theory, V corresponds to a finite extension L', so that the absolute Galois group of $L \coloneqq L'(\mu_n)$ acts trivially on both M and μ_n. By the structure theorem for finite abelian groups, M is isomorphic (as a Γ_L-module) to the direct sum of finitely many μ_k, with $k \mid n$.

However, by the previous theorem $H^i(L,\, \mu_k)$ is finite for all i, so $H^i(L,\, M)$ is finite as well by additivity. Now, using the Hochschild-Serre spectral sequence (1.4.2):

$$E_2^{pq} = H^p(\mathrm{Gal}(L/K),\, H^q(L,\, M)) \Rightarrow H^{p+q}(K,\, M)$$

we see that $H^i(K,\, M)$ is finite, as it has a finite filtration whose successive quotients are subquotients of the finite groups E_2^{pq} (which are finite as cohomology groups of a finite module, since $\mathrm{Gal}(L/K)$ is finite). □

Chapter **4**

Local Duality

In this chapter we are going to define a product on cohomology, the *cup product*, and work through its properties and compatibility with various pairings.

Using the cup product and the previous results on the structure of local fields, we'll prove Tate's local duality theorem for finite modules over the absolute Galois group Γ of a p-adic field, for which we'll need to show the existence of a dualizing module for G, which represents the Pontryagin dual of a specific cohomology functor.

We will then apply all of this machinery by computing the abelianization of the absolute Galois group of a p-adic field, which describes the finite abelian extensions of K.

4.1 Cup Product

Let G be a profinite group. Given two G-modules A and B, we consider their tensor product $A \otimes B$ (over $\mathbb{Z}$) with the natural G-module structure

$$g \cdot (a \otimes b) = g \cdot a \otimes g \cdot b,$$

which extends to a bi-additive map on *homogeneous* cochains

$$\begin{aligned} K^p(G, A) \times K^q(G, B) &\xrightarrow{\cup} K^{p+q}(G, A \otimes B) \\ (a, b) &\mapsto a \cup b, \end{aligned}$$

by setting

$$(a \cup b)(g_0, \ldots g_{p+q}) = a(g_0, \ldots, g_p) \otimes b(g_p, \ldots, g_{p+q}).$$

This extends to a map on cohomology groups:

Theorem 4.1.1 *The cup product induces a bi-additive map*

$$\begin{aligned} \cup : H^p(G,\, A) \times H^q(G,\, B) &\longrightarrow H^{p+q}(G,\, A \otimes B) \\ (\alpha, \beta) &\longmapsto \alpha \cup \beta. \end{aligned}$$

Proof. We only need to prove that the cup product is well-defined, i.e. that it sends pairs of cocycles of $Z^p(G, A) \times Z^q(G, B)$ in cocycles of $Z^{p+q}(G, A \otimes B)$, and that changing one of such representatives by a coboundary doesn't change the cohomology class of the image. It's enough to prove the following formula:

$$d(a \cup b) = da \cup b + (-1)^p a \cup db, \tag{4.1}$$

whose computation follows readily from the definition of the coboundary morphisms, by cancelling out terms with opposite signs in the right hand side. □

Remark 4.1.2 Note that for $p = 0$, the cup product with a fixed element $a \in H^0(G, A) = A^G$ is a map

$$H^q(G, B) \to H^q(G, A \otimes B)$$

induced by

$$\begin{aligned} B &\longrightarrow A \otimes B \\ b &\longmapsto a \otimes b, \end{aligned}$$

as is readily checked on cocycles.

In the case $p = q = 0$, we get that the cup product on invariants is just the tensor product

$$A^G \otimes B^G \to (A \otimes B)^G.$$

Definition 4.1.3 A *pairing* of G-modules is a bi-additive map $\varphi : A \times B \to C$ which is G-equivariant, i.e. such that

$$\varphi(g \cdot a, g \cdot b) = g \cdot \varphi(a, b)$$

for all $a \in A$, $b \in B$, and $g \in G$.

Since any such pairing induces a map $\overline{\varphi} : A \otimes B \to C$, we can use the cup product to define a pairing on cohomology, which we will denote by the same symbol by a slight abuse of notation:

$$\begin{tikzcd}
H^p(G, A) \times H^q(G, B) \arrow[rr, "\cup"] \arrow[dr] & & H^{p+q}(G, C) \\
& H^{p+q}(G, A \otimes B) \arrow[ur, "\overline{\varphi}^*"'] &
\end{tikzcd}$$

In order to prove the duality theorem, we will need the following compatibility of the cup product with exact sequences:

Proposition 4.1.4 *Suppose we have exact sequences of G-modules*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0, \qquad 0 \longrightarrow A' \longrightarrow B' \longrightarrow C' \longrightarrow 0$$

and a pairing $\varphi : B \times B' \to D$ that sends $A \times A'$ to 0, so that it induces pairings

$$\varphi' : A \times C' \to D$$

and

$$\varphi'' : A' \times C \to D.$$

Then, the cup products associated with φ', φ'' are compatible (up to sign) with the coboundaries of the long exact sequences in cohomology:

$$\delta\gamma \cup \gamma' + (-1)^p(\gamma \cup \delta\gamma') = 0$$

for all $\gamma \in H^p(G, C)$ and $\gamma' \in H^{q-1}(G, C')$.

Proof. We need explicit the connecting homomorphisms: lift γ and γ' to cocycles c and c', and lift those respectively to $b \in K^p(B)$ and $b' \in K^{q-1}(B')$. Their images db and db' then come from some $a \in K^{p+1}(A)$ and $a' \in K^q(A')$ respectively, which are representatives for $\delta\gamma$ and $\delta\gamma'$.

Now, by (4.1) the *coboundary* $d(b \cup b')$ is equal to

$$db \cup b' + (-1)^p b \cup db' = a \cup c' + (-1)^p c \cup a',$$

which is thus zero in cohomology. □

4.2 Dualizing Modules

In this section we introduce the dualizing module, a type of object which is central in the study of any duality. While it can be defined explicitly (as done in e.g. [NSW00]), we are going to prove its existence by homological methods and only compute it for the absolute Galois group of a p-adic field, which suffices to prove the duality theorem. We start by introducing the type of duality we are interested in:

Pontryagin Duality

If A is an abelian group, we define the *Pontryagin dual* of A as

$$A^* := \mathrm{Hom}_c(A, \mathbb{Q}/\mathbb{Z}).$$

If A is torsion, $A^* = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ is profinite with the compact-open topology.

Remark 4.2.1 The functor $A \mapsto A^*$ induces an equivalence of categories

$$\{\text{Torsion abelian groups}\}^{\mathrm{op}} \cong \{\text{Profinite abelian groups},\}$$

as a special case of Pontryagin duality for locally compact abelian groups. For a finite abelian group A, the structure theorem yields a (non-canonical) isomorphism $A \xrightarrow{\sim} A^*$, and by cardinality considerations we have the canonical isomorphism

$$\begin{aligned} A &\xrightarrow{\sim} A^{**} \\ b &\mapsto (f \mapsto f(b))\,. \end{aligned}$$

Generalizing to torsion abelian groups, we can write such an A as the inductive limit of its finite subgroups A_i to get

$$A^* = \mathrm{Hom}(\varinjlim_i A_i, \mathbb{Q}/\mathbb{Z}) = \varprojlim_i A_i^*,$$

which is a profinite group. Viceversa, if G is an abelian profinite group, we can write it as the projective limit of its finite quotients G_i, and then

$$G^* = \mathrm{Hom}_c(\varprojlim_i G_i, \mathbb{Q}/\mathbb{Z}) = \varinjlim_i G_i^*$$

is a torsion group. One checks that this actually induces an equivalence of categories, for which we refer to [RZ10], §2.9.

Existence

Now, given a profinite group G of finite cohomological dimension $\mathrm{cd}\,(G) = n$, denote by $\mathsf{Mod}_{\mathsf{G}}^f$ the category of finite discrete G-modules. Then, by the previous remark we have a contravariant left-exact functor

$$\mathsf{Mod}_{\mathsf{G}}^f \to \mathsf{Ab} \tag{4.2}$$
$$A \mapsto H^n(G,\, A)^* : \tag{4.3}$$

indeed, * is an exact functor because it induces an equivalence, and using the long exact sequence we see that the n-th cohomology functor is right-exact, so their composition is left-exact by contravariance of *.

The dualizing module is defined through the following theorem, which gives sufficient conditions to the representability of this functor:

Theorem 4.2.2 *Let G be a profinite group of finite cohomological dimension $\mathrm{cd}\,(G) = n$ such that $H^n(G,\, A)$ is finite for all $A \in \mathsf{Mod}^f_{\mathsf{G}}$.*

Then, the functor (4.2) on $\mathsf{Mod}^f_{\mathsf{G}}$ is representable by an object of the category $\varinjlim \mathsf{Mod}^f_{\mathsf{G}}$ of torsion modules: there exists a discrete torsion G-module I together with a natural isomorphism

$$\mathrm{Hom}_G\,(-, I) \simeq H^n(G,\, -)^* \tag{4.4}$$

of functors $\mathsf{Mod}^f_{\mathsf{G}} \to \mathsf{Ab}$.

Definition 4.2.3 In the situation of Theorem 4.2.2, I is called the *dualizing module* of G.

The proof uses a lemma from homological algebra, for which we give a basic definition:

Definition 4.2.4 A category $\mathcal{C}$ is *Noetherian* if:

- it is *essentially small* (i.e. it's equivalent to a category whose objects form a set), and
- every object C of $\mathcal{C}$ is *Noetherian* (i.e. every ascending chain of subobjects of C stabilizes).

Lemma 4.2.5 *Let $\mathcal{C}$ be a Noetherian Abelian category, and $F : \mathcal{C} \to \mathsf{Ab}$ a contravariant left-exact functor. Then, F is* Ind*-representable: there exists a filtered inductive system (I_j) of objects in $\mathcal{C}$ such that F is naturally isomorphic to the functor*

$$A \mapsto \varinjlim_j \mathrm{Hom}(A, I_j).$$

We first show how this implies the existence of the dualizing module:

Proof of Theorem 4.2.2. We apply Lemma 4.2.5 to the functor $H^n(G,\, -)^*$, which we have already shown to be left-exact; the category $\mathsf{Mod}^f_{\mathsf{G}}$ is Noetherian as it is small and its objects are finite. Thus, we obtain an inductive system (I_j) and a natural isomorphism

$$H^n(G,\, -)^* \simeq \varinjlim_j \mathrm{Hom}(-, I_j).$$

Now, set $I := \varinjlim_j I_j$. This is a discrete torsion G-module, and since A is finite we conclude:

$$\begin{aligned} \mathrm{Hom}_G(A, I) &\simeq \varinjlim_j \mathrm{Hom}(A, I_j) \\ &= H^n(G,\, A)^*. \end{aligned}$$

□

Remark 4.2.6 We can generalize Theorem 4.2.2 to discrete torsion G-modules, just by writing such an A as the inductive limit of its finite submodules $A = \varinjlim_{\substack{B \subset A \\ B \text{ finite}}} B$:

$$\begin{aligned} H^n(G,\, A)^* &= \varprojlim H^n(G,\, B)^* \\ &\simeq \varprojlim \mathrm{Hom}_G(B, I) \\ &= \mathrm{Hom}_G(A, I). \end{aligned}$$

Remark 4.2.7 If we only consider profinite groups of finite p-cohomological dimension n, the analogue of Theorem 4.2.2 holds with the same proof, provided we further restrict ourselves to p-primary torsion modules (as the n-th cohomology functor is right-exact on the corresponding subcategory)

Let us now embark on the proof of Lemma 4.2.5, which is due to Grothendieck (in the case of an Artinian category, see [Gro61] §3):

Proof. A pair (A, x), for A in $\mathcal{C}$ and x in $F(A)$, is called **minimal** if $x \notin F(B)$ for each surjection $B \twoheadrightarrow A$ with a non-trivial kernel. This makes sense as for F left-exact we can view $F(B)$ as a subobject of $F(A)$; we shall use this repeatedly in the following.

Given two pairs (A, x) and (B, y), we say that (A, x) **dominates** (B, y) if there is a morphism $p : A \to B$ such that $F(p)(y) = x$.

Using the Noetherian hypothesis, we can show that every pair (A, x) is dominated by a minimal pair: to construct it, consider the poset Σ of all subjobects $A_0 \subset A$ such that $(A/A_0, y)$ dominates (A, x) for some $y \in F(A/A_0)$ through the projection morphism $p : A \twoheadrightarrow A/A_0$. Taking $A_0 = 0$ and $y = x$ shows that Σ is non-empty: indeed, $p = \mathrm{id}_A$ and $F(p)(y) = \mathrm{id}_{F(A)}(y) = x$. Then, by the Noetherian condition Σ admits a maximal element A_0, and we show that $(A/A_0, y)$ is a minimal pair: given $p' : B \twoheadrightarrow A_0$ with $\ker(p') \neq 0$, if y is in $F(B)$ we can consider the pair (B, y) and the morphism $q := p' \circ p : A \twoheadrightarrow B$. Then, (B, y) dominates (A, x) since

$$F(q)(y) = F(p)(F(p')(y)) = F(p)(y),$$

but then $B = (A/A_0)/\ker(p')$ is a quotient of A which contradicts the maximality of A_0.

Furthermore, if (A, x) is dominated by a minimal pair (B, y), we claim that there is a *unique* morphism $p : A \to B$ such that $F(p)(y) = x$. Indeed, let $q : A \to B$ be a morphism with $F(q)(y) = x$, then

$$F(p - q)(y) = 0.$$

Moreover, the surjection $A \twoheadrightarrow \mathrm{im}(p - q)$ induces an injective morphism $F(\mathrm{im}(p - q)) \hookrightarrow F(A)$, and composing it with the inclusion $i : \mathrm{im}(p - q) \hookrightarrow A$ we get a morphism

$$F(B) \overset{F(i)}{\to} F(\mathrm{im}(p - q)) \hookrightarrow F(A)$$

which sends y to 0, and conclude that $x \in \ker(F(i))$.

Finally, taking C to be the cokernel of $(p - q)$ yields an exact sequence

$$0 \to \mathrm{im}(p - q) \overset{i}{\to} B \to C \to 0 \tag{4.5}$$

which in turn induces an exact sequence

$$0 \to F(C) \to F(B) \to F(\mathrm{im}(p - q)),$$

which shows that $\ker(F(i)) = F(C)$, so x is contained in $F(C)$. However, by minimality of (B, y) the second map in (4.5) is an isomorphism, which means that $p = q$.

The set of minimal pairs can be ordered by setting $(A, x) \leq (B, y)$ if (A, x) dominates (B, y). This defines an inductive system (I_j, x_j), as any two minimal pairs (I_j, x_j) and (I_k, x_k) are dominated by their direct sum $(I_j \oplus I_k, (x_j, x_k))$, which is itself dominated by a minimal pair.

We thus get a canonical element $x := (x_j)$ of $F(I) := \varprojlim_j F(I_j)$, which we use to define a functorial homomorphism

$$\phi : \varinjlim_j \mathrm{Hom}(A, I_j) \longrightarrow F(A),$$

by sending $f \coloneqq (f_j)$ to $F(f)(x)$. This is well defined because Hom preserves limits, and so

$$F(f) \in \varinjlim_{j} \operatorname{Hom}(F(I_j), F(A)) = \operatorname{Hom}(F(I), F(A)).$$

Finally, we show that ϕ is an isomorphism: if (f_j) is sent to 0, then for any j the two morphisms

$$F(f_j), F(0): \ F(I_j) \to F(A)$$

both send x_j to 0. Since (I_j, x_j) is a minimal a pair which dominates $(A, 0)$, we deduce that f_j must be the zero morphism, and by arbitrariness of j we get injectivity.

For surjectivity, given any $y \in F(A)$ we know that (A, y) is dominated by a minimal pair (I_j, x_j), so there is a unique $f_j : A \to I_j$ satisfying $F(f_j)(x_j) = y$. Then, the limit of the f_j is sent by ϕ to y, and we are done. □

Remark 4.2.8 In light of Remark 4.2.6, for any discrete torsion G-module A we can view the functorial isomorphism (4.4) as a **perfect pairing**

$$\langle -, - \rangle_A : \operatorname{Hom}_G(A, I) \times H^n(G,\, A) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

between the discrete torsion group $H^n(G,\, A)$ and the profinite group $\operatorname{Hom}_G(A, I)$ endowed with the compact-open topology. This in particular applies to $A = I$ itself.

For any G-module A, consider the abelian group

$$A' \coloneqq \operatorname{Hom}_{\mathbb{Z}}(A, I),$$

which we make into a G-module by setting

$$(\sigma \cdot f)(a) = \sigma(f(\sigma^{-1} \cdot a)). \tag{4.6}$$

This action induces a pairing of G-modules

$$\begin{aligned} A' \times A &\to I \\ (f, a) &\mapsto f(a), \end{aligned}$$

and thus a cup product

$$H^0(G,\, A') \times H^n(G,\, A) \xrightarrow{\cup} H^n(G,\, I)$$

which is related to the dual of cohomology by

$$H^0(G,\, A') = \operatorname{Hom}_G(A, I).$$

Indeed, the group $H^0(G,\, A')$ consists of the G-invariants of $A' = \operatorname{Hom}_{\mathbb{Z}}(A, I)$, and so

$$H^0(G,\, A') = (\operatorname{Hom}_{\mathbb{Z}}(A, I))^G = \operatorname{Hom}_G(A, I),$$

where for the last equality note that on $\operatorname{Hom}_G(A, I)$ the action was defined as

$$(g \cdot f)(a) = g \cdot (f(g^{-1} \cdot a)).$$

We will need the following compatibility of the cup product with the duality pairing:

Lemma 4.2.9 *In the situation of the previous definition, the pairing $\langle -, - \rangle_A$ factors through the cup product and the homomorphism $i := \langle \mathrm{id}_I, - \rangle_I : H^n(G,\, I) \to \mathbb{Q}/\mathbb{Z}$, i.e. the following diagram commutes:*

$$\begin{tikzcd}
H^0(G,\, A') \times H^n(G,\, A) \arrow[r, "\cup"] \arrow[dr, "\langle -,- \rangle_A"'] & H^n(G,\, I) \arrow[d, "i"] \\
& \mathbb{Q}/\mathbb{Z}.
\end{tikzcd}$$

Proof. Any morphism $f \in \mathrm{Hom}_G(A, I)$ induces a homomorphism in cohomology

$$f^* : H^n(G,\, A) \to H^n(G,\, I),$$

and by composition on the left a homomorphism

$$f^* : \mathrm{Hom}_G(I, I) \to \mathrm{Hom}_G(A, I).$$

Now, writing out the functorality of the dualizing module gives the following commutative diagram:

$$\begin{tikzcd}
\mathrm{Hom}_G(A, I) & \times & H^n(G,\, A) \arrow[dd, "f^*"] \arrow[dr, "\langle -,- \rangle_A"] & \\
& & & \mathbb{Q}/\mathbb{Z} \\
\mathrm{Hom}_G(I, I) \arrow[uu, "f^*"] & \times & H^n(G,\, I) \arrow[ur, "\langle -,- \rangle_I"'] &
\end{tikzcd}$$

As remarked in 4.1.2, here the cup product of $f \in H^0(G,\, A')$ with some $\alpha \in H^n(G,\, A)$ is given by $f^*(\alpha)$. Since f^* clearly sends id_I to f, the above diagram implies that

$$\langle f, \alpha \rangle_A = \langle \mathrm{id}_I, f^*(\alpha) \rangle_I = i(f \cup \alpha).$$

□

Corollary 4.2.10 *It follows that the pair (I, i) is unique up to unique isomorphism.*

Before moving on to the computation of the dualizing module of the absolute Galois group of a p-adic field, we need a lemma about dualizing modules of open subgroups:

Lemma 4.2.11 *Let G be a profinite group of finite cohomological dimension n such that $H^n(G,\, A)$ is finite for all $A \in \mathsf{Mod}_\mathsf{G}^f$. If $U \subset G$ is an open subgroup and I is the dualizing module of G, then I (viewed as an U-module) is the dualizing module of U, and the homomorphism*

$$H^n(U,\, A) \to H^n(G,\, A)$$

defined by dualizing the inclusion $i : \mathrm{Hom}_G(A, I) \hookrightarrow \mathrm{Hom}_U(A, I)$ is simply the corestriction.

Proof. As U is open and $\mathrm{cd}\,(G) < \infty$, Proposition 2.4.9 implies $\mathrm{cd}\,(U) = \mathrm{cd}\,(G)$. By uniqueness of the dualizing module, it's enough to show that $H^n(U,\, -)^* \simeq \mathrm{Hom}_U(-, I)$, and then the first claim follows from the functorial isomorphisms

$$\begin{aligned}
H^n(U,\, A)^* &\simeq H^n(G,\, \mathrm{CoInd}_G^U(A)) && \text{(Shapiro)} \\
&\simeq \mathrm{Hom}_G(\mathrm{CoInd}_G^U(A),\, I) && (I \text{ is the dualizing module of } G) \\
&\simeq \mathrm{Hom}_U(A,\, I) && \text{(by Remark (1.1.7) (b)).}
\end{aligned}$$

For the second claim, recall from remark 1.3.9 that the corestriction homomorphism is induced by the surjective morphism of G-modules

$$\begin{aligned} \mathrm{CoInd}_G^U(A) &\xrightarrow{\pi} A \\ f &\longmapsto \sum_{g\in G/U} g\cdot f(g^{-1}). \end{aligned}$$

On the other hand, π induces a morphism of modules $\mathrm{Hom}_G(A, I) \xrightarrow{\pi_*} \mathrm{Hom}_G(\mathrm{CoInd}_G^U(A), I)$. Using the functoriality of the dualizing module and the Shapiro isomorphism Sh (1.3.4), we get the following commutative diagram:

$$\begin{tikzcd}
\mathrm{Hom}_U(A, I) \arrow[r, "\Phi"] & \mathrm{Hom}_G(\mathrm{CoInd}_G^U(A), I) \arrow[r] & H^n(G,\, \mathrm{CoInd}_G^U(A))^* \arrow[r, "(-)^*"] & H^n(G,\, \mathrm{CoInd}_G^U(A)) \arrow[r, "\mathrm{Sh}"] \arrow[d, "\pi^*"] & H^n(U,\, A) \arrow[dl, "\mathrm{Cor}"] \\
& \mathrm{Hom}_G(A, I) \arrow[ul, "i"'] \arrow[u, "\pi_*"] \arrow[r] & H^n(G,\, A)^* \arrow[u, "\pi_n^*"] \arrow[r, "(-)^*"] & H^n(G,\, A) &
\end{tikzcd}$$

Here, Φ is the isomorphism of Remark 1.1.7 (b), which makes the leftmost triangle commute as

$$\pi_*(\varphi)(f) = \varphi\left(\sum\nolimits_{g\in G/U} g\cdot f(g^{-1})\right) = \sum\nolimits_{g\in G/U} g\cdot\varphi(f(g^{-1})) = (\Phi\circ i)(\varphi)(f)$$

for any $\varphi \in \mathrm{Hom}_G(A, I)$ and $f \in \mathrm{CoInd}_G^U(A)$. □

Computation for p-adic Fields

Finally, we apply the theory of dualizing modules to the absolute Galois group Γ of a p-adic field K: by 3.4.3 we know that $\mathrm{cd}\,(\Gamma) = 2$, and by 3.5.3 the groups $H^2(K,\, A)$ are finite for any finite Γ_K-module A. Thus, Γ has a dualizing module I by Theorem 4.2.2, which we now compute explicitly.

Proposition 4.2.12 *The dualizing module of Γ is canonically isomorphic to the Γ-module of roots of unity $\mu \subset \overline{K}^{\times}$.*

Proof. Let $I_n := I[n]$ be the kernel of multiplication by n on I, and take an open subgroup $U \subset \Gamma$. By Lemma 4.2.11, the dualizing module of U is the same as that of Γ.

The computation of the cohomology of μ_n (Theorem 3.5.1) shows that $H^2(U,\, \mu_n) \simeq \mathbb{Z}/n\mathbb{Z}$, and by Proposition 3.3.2 the corestriction $\mathrm{Br}\,(K^U) \to \mathrm{Br}\,(K)$ is the identity of $\mathbb{Q}/\mathbb{Z}$.

Thus, if $U \subset V$ are open subgroups of Γ, the second part of Lemma 4.2.11 yields the following commutative diagram:

$$\begin{tikzcd}
\mathrm{Hom}_V(\mu_n, I_n) \arrow[r] \arrow[d] & H^2(V,\, \mu_n)^* \arrow[r, "\sim"] \arrow[d, "\mathrm{Cor}^* = \mathrm{id}"] & \mathbb{Z}/n\mathbb{Z} \arrow[d, equal] \\
\mathrm{Hom}_U(\mu_n, I_n) \arrow[r] & H^2(U,\, \mu_n)^* \arrow[r, "\sim"] & \mathbb{Z}/n\mathbb{Z}.
\end{tikzcd}$$

This shows that $\mathrm{Hom}_U(\mu_n, I_n)$ doesn't depend on U, and by Remark 2.2.2 (b) we get

$$\mathrm{Hom}_{\mathbb{Z}}(\mu_n, I_n) = \bigcup_{\substack{U\subset\Gamma \\ U \text{ open}}} \mathrm{Hom}_U(\mu_n, I_n) \simeq \mathbb{Z}/n\mathbb{Z}$$

In particular, taking U to be Γ tells us that Γ acts trivially on $\mathrm{Hom}_{\mathbb{Z}}(\mu_n, I_n)$, or equivalently that any homomorphism $\mu_n \to I_n$ is Γ-equivariant.

Let f_n be the canonical generator of $\mathrm{Hom}_{\mathbb{Z}}(\mu_n, I_n)$ associated with $1 \in \mathbb{Z}/n\mathbb{Z}$. Then f_n is injective because it has order n, and surjective because otherwise any element outside its image wouldn't be reached by any element of $\langle f_n \rangle = \mathrm{Hom}_{\mathbb{Z}}(\mu_n, I_n)$, but since I_n has exponent n there exist homomorphisms $\mu_n \to I_n$ sending a generator of μ_n to any element of I_n.

By writing $\mu = \bigcup_n \mu_n$ and $I = \bigcup_n I[n]$, we get an isomorphism of Γ-modules

$$f \coloneqq \varinjlim_n f_n : \mu \xrightarrow{\sim} I,$$

which is well defined thanks to the functoriality of the dualizing module, and canonical since the map $H^2(\Gamma, \mu_m) \to H^2(\Gamma, \mu_n)$ induces the canonical injection $\mathbb{Z}/m\mathbb{Z} \hookrightarrow \mathbb{Z}/n\mathbb{Z}$ if m divides n. □

4.3 Tate Duality

We now define yet another kind of duality, this time for modules:

Definition 4.3.1 Given a field K, let Γ be its absolute Galois group and μ the group of all the roots of unity in $\overline{K}^\times$. For any finite Γ -module M whose torsion is prime to the characteristic of K, we define the **Cartier dual** of M as

$$M' = \mathrm{Hom}_{\mathbb{Z}}(M, \overline{K}^\times) = \mathrm{Hom}_{\mathbb{Z}}(M, \mu),$$

with the action of Γ given by

$$(\sigma \cdot f)(m) = \sigma(f(\sigma^{-1} \cdot m)),$$

just as we did in (4.6). This yields an obvious pairing

$$\begin{aligned} M' \times M &\to \mu \\ (f, m) &\mapsto f(m), \end{aligned}$$

and thus a cup product. Notice that, with the above action, the dual of $M' = \mathrm{Hom}_{\mathbb{Z}}(\mu_n, \mu_n)$ of $M = \mu_n$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ as a Γ-module.

Theorem 4.3.2 *Let K be a p-adic field, and M a finite Γ-module. Then, for $i = 0, 1, 2$ the cup product induces a perfect pairing of finite groups*

$$H^i(K, M) \times H^{2-i}(K, M') \to H^2(K, \mu) \simeq \mathbb{Q}/\mathbb{Z}.$$

Proof. We have already proved the finiteness of the groups involved in 3.5.3, so we only need to show that the pairing is perfect. We start from $i = 2$, where our computation of the dualizing module pays off: indeed, the content of Lemma 4.2.9 in this situtation consists of the following commutative diagram

$$\begin{tikzcd} H^0(K, M') \times H^2(K, M) \arrow[r, "\cup"] \arrow[dr, "\langle -,- \rangle_M"'] & H^2(K, \mu) \arrow[d, "i"] \\ & \mathbb{Q}/\mathbb{Z}, \end{tikzcd}$$

where

$$i = \langle \mathrm{id}_\mu, - \rangle_\mu : H^2(K, \mu) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

is the Brauer group isomorphism by the computation 4.2.12 of the dualizing module together with the uniqueness of the pair (I, i). Since $\langle -, - \rangle_M$ is a perfect pairing, we are done.

The case $i = 0$ then follows by symmetry, as any finite M can be identified with its double dual M''. We are now left with $i = 1$: here it's enough to show that the map

$$H^1(K,\, M) \overset{\cup}{\to} H^1(K,\, M')^*$$

induced by the cup product is injective, as then applying the same argument to M' gets us surjectivity, since we are working with finite groups. To prove injectivity, we first find a finite Γ-module B fitting in an exact sequence

$$0 \to M \to B \to C \to 0 \tag{4.7}$$

such that the induced map

$$H^1(K,\, M) \to H^1(K,\, B)$$

is zero: as usual, we start by injecting M in the induced module $\mathrm{I}_\Gamma(M)$ which is torsion, and by the fundamental property 2.3.2 we have

$$0 = H^1(K,\, \mathrm{I}_\Gamma(M)) = \varinjlim_{\substack{B \subset \mathrm{I}_\Gamma(M) \\ B \text{ finite}}} H^1(K,\, B),$$

which implies the existence of a finite submodule B on which $H^1(K,\, M) \to H^1(K,\, B)$ is 0. As M is finite, we can find such a B which also contains M. Then, the quotient $C = B/M$ is finite and we can relate the long exact cohomology sequences associated with the short exact sequence (4.7) and its dual using the cup product. Note that the dual sequence is also exact, as Pontryagin duality is exact for finite groups (it's clearly left exact, and right-exactness follows from the injectivity of $\mathbb{Q}/\mathbb{Z}$).

This gets us the following commutative diagram (up to a sign, by 4.1.4) with exact rows:

$$\begin{tikzcd}
H^0(K,\, B) \arrow[r] \arrow[d, "\cup"] & H^0(K,\, C) \arrow[r] \arrow[d, "\cup"] & H^1(K,\, M) \arrow[r] \arrow[d, "\cup"] & 0 \\
H^2(K,\, B')^* \arrow[r] & H^2(K,\, C')^* \arrow[r] & H^1(K,\, M')^*.
\end{tikzcd}$$

As B and C are finite, the first two vertical maps are isomorphisms by the previous cases, and the third one is injective by diagram chasing.

□

Remark 4.3.3 If we only consider p-torsion-free modules, then the theorem also true for local fields of positive characteristic by Remark 4.2.7.

4.4 Local Class Field Theory

Let K be a p-adic field with absolute Galois group Γ. As an immediate application of the local duality theorem, since for any $n > 0$ the Cartier dual of the Γ-module μ_n is $\mathbb{Z}/n\mathbb{Z}$, the cup product induces an isomorphism

$$H^1(K,\, \mu_n) \xrightarrow{\sim} H^1(K,\, \mathbb{Z}/n\mathbb{Z})^*. \tag{4.8}$$

Recall that the groups $K^{\times n}$ are open in $K^\times$ (Proposition 3.2.4), and note that they are cofinal in the open subgroups of finite index: an index n subgroup contains $K^{\times n}$, and the intersection of any two finite index subgroups has finite index. Thus, we get the following description of the abelianization of the absolute Galois group of a p-adic field:

$$\begin{aligned}
\Gamma^{\mathrm{ab}} &= \mathrm{Hom}(\Gamma, \mathbb{Q}/\mathbb{Z})^* && \text{(by Pontryagin duality)}\\
&= \mathrm{Hom}(\Gamma, \varinjlim_n \mathbb{Z}/n\mathbb{Z})^* && \text{(viewing } \mathbb{Q}/\mathbb{Z} \text{ as a colimit)}\\
&= \varprojlim_n \mathrm{Hom}(\Gamma, \mathbb{Z}/n\mathbb{Z})^* && \text{(by contravariance)}\\
&= \varprojlim_n H^1(K, \mathbb{Z}/n\mathbb{Z})^* && \text{(by 1.2.9)}\\
&= \varprojlim_n H^1(K, \mu_n) && \text{(by Tate Duality)}\\
&= \varprojlim_n K^\times/K^{\times n} && \text{(by 3.5.1)}\\
&= \widehat{K^\times} && \text{(by 3.2.4).}
\end{aligned}$$

Remark 4.4.1 Here by G^{ab} we mean the quotient of G by the *closure* of its derived subgroup. If K^{ab} is the maximal abelian extension of K, then we have an isomorphism

$$\Gamma^{\mathrm{ab}} \simeq \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

In particular, passing through Galois theory we deduce a correspondence

$$\{\text{finite abelian extensions of } K\} \longleftrightarrow \{\text{finite index subgroups of } \widehat{K^\times} = \widehat{\mathbb{Z}} \times U_K\}. \tag{4.9}$$

The main result of local class field theory, the existence theorem, makes this correspondence explicit using the *reciprocity map*, which is usually constructed in an explicit manner (as in [Har20] Ch. 9). However, we can define it using the above isomorphism:

Definition 4.4.2 The reciprocity map

$$\omega : K^\times \to \Gamma^{\mathrm{ab}}$$

is the composition of the inclusion $K^\times \hookrightarrow \widehat{K^\times}$ with the isomorphism $\widehat{K^\times} \xrightarrow{\sim} \Gamma^{\mathrm{ab}}$.

Remark 4.4.3 One can show that this has the same properties as the usual reciprocity map that are developed in loc. cit., Ch. 9, and which we will use in the following. In particular, the reciprocity map is surjective, with dense image (by definition of the profinite completion) and if $n > 0$ it induces a map

$$\omega_n : K^\times/K^{\times n} \to \Gamma^{\mathrm{ab}}/n \simeq H^1(K, \mathbb{Z}/n\mathbb{Z})^*, \tag{4.10}$$

which is given by the isomorphism (4.8) of local duality. Above, we used the fact that

$$H^1(K, \mathbb{Z}/n\mathbb{Z}) = \mathrm{Hom}(\Gamma^{\mathrm{ab}}, \mathbb{Z}/n\mathbb{Z}) \simeq (\Gamma^{\mathrm{ab}}/n)^*.$$

Moreover, for any finite abelian Galois extension L/K there is a diagram

$$\begin{tikzcd}
L^\times \arrow[r, "\omega_L"] \arrow[d, "N_{L/K}"'] & \Gamma_L^{\mathrm{ab}} \arrow[d] \\
K^\times \arrow[r, "\omega_K"] & \Gamma_K^{\mathrm{ab}}
\end{tikzcd} \tag{4.11}$$

whose commutativity we can prove at the level of finite quotients:

$$\begin{tikzcd}
L^\times/L^{\times n} \arrow[r, "\delta"] \arrow[d, "N_{L/K}"'] & H^1(L,\, \mu_n) \arrow[r, "\sim"] \arrow[d, "\mathrm{Cor}"] & H^1(L,\, \mathbb{Z}/n\mathbb{Z})^* \arrow[r, "\sim"] \arrow[d, "\mathrm{Res}^*"] & \Gamma_L^{\mathrm{ab}}/n \arrow[d] \\
K^\times/K^{\times n} \arrow[r, "\delta"] & H^1(K,\, \mu_n) \arrow[r, "\sim"] & H^1(K,\, \mathbb{Z}/n\mathbb{Z})^* \arrow[r, "\sim"] & \Gamma_K^{\mathrm{ab}}/n
\end{tikzcd}$$

Indeed, the left square commutes by compability of the corestriction with the coboundary map (which induces the Kummer isomorphism from Proposition 2.5.4); the right one commutes because by definition the restriction is compatible with the inclusion $\Gamma_K \hookrightarrow \Gamma_L$. As for the middle square, the horizontal maps are given by local duality, which factors through the cup product:

$$\begin{tikzcd}
H^1(L,\, \mu_n) \arrow[dd, "\mathrm{Cor}"] & \times & H^1(L,\, \mathbb{Z}/n\mathbb{Z}) \arrow[r, "\cup"] & H^2(L,\, \mu_n) \arrow[dd, "\mathrm{Cor}"] \arrow[dr, "\sim"] & \\
 & & & & \mathbb{Z}/n\mathbb{Z} \\
H^1(K,\, \mu_n) & \times & H^1(K,\, \mathbb{Z}/n\mathbb{Z}) \arrow[r, "\cup"] \arrow[uu, "\mathrm{Res}"] & H^2(K,\, \mu_n) \arrow[ur, "\sim"] &
\end{tikzcd}$$

As the corestriction induces the identity on $\mathbb{Q}/\mathbb{Z}$ (Proposition 3.3.2), the above diagram commutes by the projection formula (which is proven e.g. in [GS06] Prop. 3.4.10):

$$\mathrm{Cor}(a \cup \mathrm{Res}(b)) = \mathrm{Cor}(a) \cup b$$

for any $a \in H^1(L,\, \mu_n)$ and $b \in H^1(K,\, \mathbb{Z}/n\mathbb{Z})$.

Finally, the reciprocity map ω_K induces a surjection

$$\omega_{L/K} : K^\times \to \mathrm{Gal}(L/K),$$

which translates to an isomorphism

$$K^\times/N_{L/K}(L^\times) \simeq \mathrm{Gal}(L/K)$$

by density of the image of ω_K and diagram chasing through (4.11). This recovers the reciprocity isomorphism associated with the extension L/K from loc. cit., Th. 9.2.

Therefore, the correspondence (4.9) in one direction is given by $L \mapsto N_{L/K}(L^\times)$. To conclude our exploration of local class field theory, we use the above properties to prove the existence theorem, which gives the correspondence in the other direction:

Theorem 4.4.4 (Existence Theorem) *Let K be a p-adic field and fix an algebraic closure $\overline{K}$. Then, for any finite index subgroup $U \subset \widehat{K^\times}$ there exists a unique finite abelian extension L/K such that $L \subset \overline{K}$ and $U = N_{L/K}(L^\times)$.*

Proof. Recall that any finite index subgroup U contains a subgroup of the form $K^{\times n}$. Then, it's enough to prove the claim for $U = K^{\times n}$ because then we can complete the diagram

$$\begin{tikzcd}
K^\times/N_{L/K}(L^\times) \arrow[r, "\omega_{L/K}"] \arrow[d, two heads] & \mathrm{Gal}\,(L/K) \arrow[d, two heads, dashed] & \\
K^\times/U \arrow[r, "\omega_K"] & \mathrm{Gal}\,(M/K) \arrow[r, phantom, "\simeq"] & K^\times/N_{M/K}(M^\times)
\end{tikzcd}$$

for some finite abelian extension M/K by Galois theory, and this implies that $U = N_{L/K}(L^\times)$.

Now, since $n\Gamma^{\mathrm{ab}}$ is compact in Γ^{ab}, the reciprocity isomorphism (4.10) implies that Γ^{ab}/n is a finite group, and so $n\Gamma^{\mathrm{ab}}$ is closed of finite index in Γ^{ab}. By Galois theory, we can find a finite abelian extension L/K such that $\mathrm{Gal}\,(L/K) = \Gamma^{\mathrm{ab}}/n$, and thus $K^{\times n} = N_{L/K}(L^\times)$ because it is the kernel of the surjection $\omega_{L/K}$.

As for uniqueness, given L, M are finite abelian extensions of K with $N_{L/K}(L^\times) = N_{M/K}(M^\times)$ the preimages of the open subgroups $\mathrm{Gal}\,(K^{\mathrm{ab}}/L)$ and $\mathrm{Gal}\,(K^{\mathrm{ab}}/M)$ by ω_K are the same. By density of the image of ω_K, we get $\mathrm{Gal}\,(K^{\mathrm{ab}}/L) = \mathrm{Gal}\,(K^{\mathrm{ab}}/M)$ and thus $L = M$ again by Galois theory. □

Bibliography

[Gro57] A. Grothendieck. *Sur quelques points d'algèbre homologique.* 1957.

[Gro61] A. Grothendieck. *Technique de descente et théorèmes d'existence en géométrie algébrique. II. Le théorème d'existence en théorie formelle des modules.* Séminaire Bourbaki, Vol. 6, Exp. No. 190, 1961.

[GS06] P. Gille and T. Szamuely. *Central Simple Algebras and Galois Cohomology.* Cambridge University Press, 2006.

[Har20] D. Harari. *Galois Cohomology and Class Field Theory.* Springer-Verlag, 2020.

[NSW00] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields.* Springer-Verlag, 2000.

[RZ10] L. Ribes and P. Zalesskii. *Profinite Groups.* Springer-Verlag, 2010.

[Ser79] J.-P. Serre. *Local Fields.* Springer-Verlag, 1979.

[Ser97] J.-P. Serre. *Galois Cohomology.* Springer-Verlag, 1997.

[Wei94] C. Weibel. *An Introduction to Homological Algebra.* Cambridge University Press, 1994.