Notes on Etale cohomology: 4

Chunye Yang

March 30, 2026

This is the fourth chapter of the notes on etale cohomology. This part of the notes will mainly focus on group cohomology and Galois cohomology. For people who have not studied these topics, this chapter could serve as a good introduction. We will also talk about profinite groups and the cohomology of profinite groups. These are all going to play an important role in our later study.

Before you read the second section, you probably want to go and take a look the section in the FOAG note about derived functors and spectral sequences.

1 Group Cohomology

Let G be a group, we know that an abelian group with a left G action is equivalent to a left $\mathbb{Z}[G]$-module where $\mathbb{Z}[G]$ is a ring with the underlying set being the free abelian group generated by elements in G. Multiplication in this ring is defined by the group multiplication and linearly extended to $\mathbb{Z}[G]$. In this chapter, we will call left $\mathbb{Z}[G]$-modules G-**modules**. A morphism of G-modules is just a left $\mathbb{Z}[G]$-module homomorphism, i.e. a map of abelian groups that is compatible with the left group action.

Definition 1.1. Let A be a G-module, we define:

$$A^G = \{a \in A : ga = a, \text{ for all } g \in G\}$$

$$A_G = A/\{\text{the subgroup generated by } ga - a \text{ for all } g \in G \text{ and all } a \in A\}$$

We shall call A^G the group of A-**invariants** and A_G the group of A-**coinvariants**.

They are called the invariants and coinvariant because A^G is the maximal subgroup of A where G acts trivially and the maximal quotient group of A where G acts trivially.

Clearly we know the category of G-modules is an abelian category and notice that taking the G-invariants is a functor from the category of G-modules to the category of abelian groups, denoted by Γ^G. If $f : A \to B$ is a morphism of G-modules, we know that if $a \in A$ is invariant under G, then $gf(a) = f(ga) = f(a)$ for all $g \in G$. Therefore we know that the G-invariants of A maps to the G-invariants of B, thus the functor is well-defined and it's clear that it's **left exact**.

Definition 1.2. The i-th derived functor of Γ^G is denoted by $H^i(G, -)$ or $R^i\Gamma^G$, which is called the i-th cohomology with respect to G.

Obviously, if we let G act trivially on $\mathbb{Z}$, then we have a canonical isomorphism:

$$A^G \simeq \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

To see what is this isomorphism, we know that a morphism in $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ is completely determined by an element in A^G. if we are given such a map, we only need to see where $1 \in \mathbb{Z}$ goes and clearly this is in A^G. Conversely given an element in A^G, we get a morphism and these are inverses.

Therefore we have a canonical isomorphism:

$$H^i(G, A) \simeq \mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

Recall that since $\mathbb{Z}[G]$ is a ring, and it's from the general theory that for any ring R, the category of R-modules has enough injective or projective objects, therefore if I (resp. P) is an injective (resp. projective) resolution of A (resp. of $\mathbb{Z}$), then we can compute:

$$H^i(G, A) \simeq H^i(I^G) \simeq H^i(\mathrm{Hom}_G(P, A))$$

Let's first try to compute a few easy cohomologies:

Proposition 1.3. If we let $G = \mathbb{Z}$, then we have:

$$H^i(G, A) = \begin{cases} A^G & \text{if } i = 0, \\ A_G & \text{if } i = 1, \\ 0 & \text{if } i \geqslant 2. \end{cases}$$

Proof. First, let $G = \mathbb{Z}$, notice that one common mistake people think of an $\mathbb{Z}$ action on A is that they think this is just the same as the abelian group structure of A. However, this is not the case. Notice that for any $g \in G$, the action is an automorphism of A, for example $2 \in \mathbb{Z}$, if you define $2 \cdot a = a + a$, this is in general not an automorphism of A. The right way to think about the morphism is to notice that an $\mathbb{Z}$-action is the same as a group homomorphism:

$$\mathbb{Z} \to \mathrm{Aut}(A)$$

Notice that this group homomorphism is completely determined by where 1 goes and let's assume that 1 goes to T. Then we know that we can think of a $\mathbb{Z}[\mathbb{Z}]$-module as a $\mathbb{Z}[T, T^{-1}]$-module and T represents the automorphism of A we choose.

Notice that we have a free resolution of $\mathbb{Z}$:

$$0 \to \mathbb{Z}[T, T^{-1}] \xrightarrow{T-1} \mathbb{Z}[T, T^{-1}] \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

We define ϵ to be the map $\sum_i a_i T^i \mapsto \sum_i a_i$, i.e. the summation of all coefficients. Notice that multiplication by $T - 1$ is obviously an $\mathbb{Z}[T, T^{-1}]$-map. Notice that term $\mathbb{Z}$ in the sequence is with trivial action, i.e. T is the identity on $\mathbb{Z}$, then it's easy to check ϵ is indeed a $\mathbb{Z}[T, T^{-1}]$-module. Notice that $\mathbb{Z}[T, T^{-1}]$ is a domain, thus multiplication by $T - 1$ is indeed injective, and clearly ϵ is surjective. I will let you check that the composition is indeed 0, and the kernel of ϵ is a polynomial such that the sum of the coefficients is 0. If $f(x) = \sum_i a_i T^i$ is such a polynomial, let's first assume that not all a_i are 0 otherwise there is not anything interesting. For example we have:

$$-T^{-1} - 1 + 2T$$

Then we know that we can consider $T^{-1} + 2$, we know that it's mapped to $1 + 2T - 2 - T^{-1}$, which is the polynomial we want.

Then for a general polynomial:

$$a_{-n}T^{-n} + \cdots + a_0 + \cdot + a_n T^n$$

then we can consider:

$$b_{-n}T^{-n} + \cdots + b_0 + \cdots + b_{n-1}T^{n-1}$$

it's mapped to $-(b_{-n}T^{-n} + \cdots + b_0 + \cdots + b_{n-1}T^{n-1}) + (b_{-n}T^{-n+1} + \cdots + b_0 T + \cdots + b_{n-1}T^n)$, then we need $b_{n-1} = a_n$, $b_{n-2} - b_{n-1} = a_{n-1}$, all the way to $b_{-n} - b_{-n+1} = a_{-n+1}$ and $-b_{-n} = a_{-n}$. We only need to show such an equation has a solution. We can solve $b_{n-1} = a_n$ first, then inductively $b_{n-2} = a_{n-1} + a_n$, then $b_{n-3} = a_{n-2} + a_{n-1} + a_n$ all the way to $b_{-n+1} = a_{-n+2} + \cdots + a_n$ and $b_{-n} = a_{-n+1} + a_{-n+2} + \cdots + a_n$. Therefore we only need to show that if $-a_{-n} = a_{-n+1} + a_{-n+2} + \cdots + a_n$, this is true since we know all the coefficients sums to 1.

Then we know that to compute the cohomology, we apply $\mathrm{Hom}(-, A)$ and get the complex:

$$0 \to \mathrm{Hom}(\mathbb{Z}[T, T^{-1}], A) \xrightarrow{T-1} \mathrm{Hom}(\mathbb{Z}[T, T^{-1}], A) \to 0$$

We know that this can be identified with:

$$0 \to A \xrightarrow{T-1} A \to 0$$

where $T-1$ is the morphism defined by T minus the identity. Then we know that H^0 is the kernel of the first arrow, this is those fixed by T, thus fixed by G. Then H^1 is the quotient by $ga-a$, therefore is the coinvariant. Notice that all other cohomology are 0, therefore we are done. □

Proposition 1.4. Let $G=\mathbb{Z}/n$ for some n, then for any G-module A, let $T:A\to A$ be the homomorphism defined by the action of the canonical generator $1\in\mathbb{Z}/n$. We have:

$$H^i(G,A)=\begin{cases}A^G & \text{if } i=0,\\ \mathrm{Ker}(T^{n-1}+\cdots+T+1)/\mathrm{Im}(T-1) & \text{if } i=1,3,5,\cdots\\ \mathrm{Ker}(T-1)/\mathrm{Im}(T^{n-1}+\cdots+T+1) & \text{if } i=2,4,,6,\cdots.\end{cases}$$

Proof. Notice that after we choose the automorphism T, we can identity $\mathbb{Z}[G]$ with $\mathbb{Z}[T]/(T^n-1)$.

I claim that we have a free resolution of $\mathbb{Z}$ given by:

$$\cdots \overset{T^{n-1}+\cdots+T+1}{\to} \mathbb{Z}[G] \overset{T-1}{\to} \mathbb{Z}[G] \overset{T^{n-1}+\cdots+T+1}{\to} \mathbb{Z}[G] \overset{T-1}{\to} \mathbb{Z}[G] \overset{\epsilon}{\to} \mathbb{Z}\to 0$$

We need to check exactness. The exactness on the right is the same as the computation we did above. Then what is the kernel of $T-1$, we know that if the polynomial: $f(T)=a_0+a_1T+\cdots+a_{n-1}T^{n-1}$ is mapped to 0, we get:

$$a_{n-1}-a_0+(a_0-a_1)T+\cdots+(a_{n-2}-a_{n-1})T^{n-1}=0$$

Therefore we know that $a_0=a_1=a_2=\cdots=a_{n-1}$, therefore is indeed in the image. Similarly, if $f(T)$ is mapped to 0 by $T^{n-1}+\cdots+T+1$, I will let you show that this implies that the sum of the coefficients is 0, therefore is in the image as we already know the sequence is exact at ϵ.

Then after we apply $\mathrm{Hom}(-,A)$, we know this is identified with:

$$0\to A \overset{T-1}{\to} A \overset{T^{n-1}+\cdots+T+1}{\to} A \overset{T-1}{\to} A\to\cdots$$

□

The above two computations are concrete enough because we are working with G equal to some version of $\mathbb{Z}$. For an arbitrary group G, we also have a way to compute the group cohomology, at least in theory:

Let L_i be the free abelian group generated by elements in G^{i+1} for $i\geqslant 0$. Then we have a left G-action on L by defining:

$$g\cdot(g_0,\cdots,g_i)=(gg_0,\cdots,gg_i)$$

We then extend this action linearly. Then I claim that L_i is a free $\mathbb{Z}[G]$-module with basis of the form

$$(1,g_1,g_1g_2,\cdots,g_1\cdots g_i)$$

where g_i are all in G. This is because clearly for any $(g_0',\cdots,g_i')$, we can consider:

$$(1,(g_0')^{-1}g_1',\cdots,(g_0')^{-1}g_i')$$

Then we can pick $g_1=(g_0')^{-1}g_1'$, $g_2=((g_0')^{-1}g_1')^{-1}\cdot(g_0')^{-1}g_2'$. Then we know that all elements in L_i can be written as a linear combination of such elements. Actually it doesn't have to be this complicated, we know that we can just take them to be:

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

where again $g_1,\cdots,g_i\in G$, intuitively speaking we know that since you are allowing to use G-actions, you can drop one freedom on this free abelian groups, which is the reason why we only need 1 in the first slot. We also need to show these elements are linearly independent, suppose that we have elements $x_1,\cdots,x_r$ in $\mathbb{Z}[G]$ such that

$$x_1(1,g_1^1\cdots,g_i^1)+\cdots+x_r(1,g_1^r\cdots,g_i^r)=0$$

where the superscript is just a index not a power. I claim all x_i must be 0. To see why, we actually only need to see the first component, suppose that x_1 consists of linear combinations of some $y_1,\cdots,y_m$, then we

know that after the product the 1-slot should be $y_1, \cdots, y_m$, therefore if we want the result to be 0, some other x_j must contain, for example y_1, but if you make the first slot y_1, since the later slots differ, we know that multiply by y_1 can not make them equal, therefore we are forced that all x_i are 0.

For each $i \geqslant 1$, let's define a G-module map:

$$\partial_i : L_i \to L_{i-1}, \qquad (g_0, \cdots, g_i) \mapsto \sum_{j=0}^{i} (-1)^j (g_0, \cdots, \hat{g_j}, \cdots, g_i)$$

and a G-module homomorphism:

$$\epsilon : L_0 \to \mathbb{Z}, \qquad g_0 \mapsto 1$$

We linearly extend this morphisms, and you can check these are compatible with G-actions. Then consider the sequence:

$$\cdots \to L_i \xrightarrow{\partial_i} L_{i-1} \to \cdots L_1 \xrightarrow{\partial_1} L_0 \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

I will let you check this is a complex of G-modules. It's also easy to check that for any fixed $g \in G$:

$$h_i : L_i \to L_{i+1}, \qquad h_i(g_0, \cdots, g_i) = (g, g_0, \cdots, g_i)$$
$$h_{-1} : \mathbb{Z} \to L_0, \qquad h_{-1}(1) = (g)$$

are all maps of abelian groups, and is a homotopy between the identity and 0, therefore the sequence is exact. So we have obtained a free resolution of $\mathbb{Z}$ for any group G, and we know that to compute the cohomology, we only need to apply $\mathrm{Hom}(-, A)$ to this complex and take chomology. Notice that since each L_i is free, we know that if we let $C^i(G, A)$ be the set of all maps from G^i to A (notice that since the target is in A, therefore $C^i(G, A)$ has a left G action even though the maps in $C^i(G, A)$ don't have any G-module structure), we have isomorphisms:

$$F_i : \mathrm{Hom}(L_i, A) \to C^i(G, A)$$

where $F_i(\phi)(g_1, \cdots, g_n) = \phi(1, g_1, g_1g_2, \cdots, g_1g_2 \cdots g_i)$. This is indeed an isomorphism as we know that we have a basis of L_i consists of elements of the form $(1, g_1, g_1g_2, \cdots, g_1g_2 \cdots g_i)$. When $i = 0$, we notice that $\mathrm{Hom}(L_0, A)$ is just determined by where the identity goes, therefore can be identified with $C^0(G, A)$, i.e. all maps from the trivial to A, therefore is identified with A.

Under this identification, the sequence:

$$0 \to \mathrm{Hom}(L_0, A) \to \mathrm{Hom}(L_1, A) \to \cdots$$

becomes:

$$0 \to C^0(G, A) \xrightarrow{d_0} C^1(G, A) \to \cdots$$

here the differentials is determined by:

$$(d_i f)(g_1, \cdots, g_{i+1}) = g_1 f(g_2, \cdots, g_n) + \sum_{j=1}^{i} f(g_1, \cdots, g_{j-1}, g_j g_{j+1}, g_{j+2}, \cdots, g_{i+1}) + (-1)^{i+1} f(g_1, \cdots, g_i)$$

for all $f \in C^i(G, A)$. When $i = 0$, consider the following diagram:

$$\begin{array}{ccc} \mathrm{Hom}(L_0, A) & \longrightarrow & \mathrm{Hom}(L_1, A) \\ \downarrow & & \downarrow \\ A & \longrightarrow & C^1(G, A) \end{array}$$

Let $f \in \mathrm{Hom}(L_0, A)$, it's image in $\mathrm{Hom}(L_1, A)$ is $f \circ \partial_1$, therefore we know that it maps (g_0, g_1) to $f(g_1 - g_0)$. Assume that e is mapped to a, we know that the image is $g_1 a - g_0 a$. This is mapped to the map $G \to A$ defined by $g \mapsto f \circ \partial_1(1, g) = ga - a$.

In this definition, we notice that a 1-cocycle is an element in the kernel of d_1. Say $f : G \to A$ is in the kernel, we know that $f(g_1g_2) = g_1f(g_2) + f(g_1)$. We know that a 1-coboundary is a map $f : G \to A$ such that $f(g) = ga - a$ for a fixed $a \in A$.

Then we know that if G acts trivially on A, then $H^1(G, A) = \mathrm{Hom}_{\mathrm{gp}}(G, A)$, where $\mathrm{Hom}_{\mathrm{gp}}(G, A)$ is the set of group homomorphisms.

Remark 1.5. Even though the above discuss gives you a way to describe the group cohomology of any group G, it will not be typically how we compute a group cohomology. The reason we discuss it here is that in later sections, when we compute the cohomology of a profinite group, we will meet similar descriptions and you can compare how they appear to be different but actually are the same.

Then we discuss two important constructions in group cohomology, which are **restriction** and **inflation** maps: Let $f : G' \to G$ be a map of groups, A a G-module and A' a G' module. Let $\phi : A \to A'$ be an additive map compatible with the group actions in the sense:

$$\phi(f(g')a) = g'\phi(a)$$

This implies that ϕ induces a homomorphism from A^G to $A'^{G'}$. You may find it a bit strange when the map f is from G' to G while ϕ is from A to A'. But this is what we need to require if we want the map induces maps between invariants. For example if we use $f : G \to G'$ and the natural definition of ϕ being compatible with the action is $\phi(g \cdot a) = f(g)\phi(a)$. Then just by knowing a is fixed by all $g \in G$ doesn't imply it's fixed by G'.

Recall that the derived functors of Γ^G is a cohomological δ-functor with the property that for any other cohomological δ-functor T_i with $\Gamma^G \to T_0$, then there is a unique extension $R^i\Gamma^G \to T_i$. Then we take another cohomological delta functor to be the derived functor of $\Gamma^{G'}$. Then the fact that ϕ induces a map A^G to $A'^{G'}$ implies that there is a natural transformation $\Gamma^G \to \Gamma^{G'}$ induced by ϕ, therefore we have canonical extensions:

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

Remark 1.6. Recall that when we use universal properties of derived functors, we will need to work with a fixed source category. Here in the above discussion it seems like the two functor Γ^G and $\Gamma^{G'}$ are from the category of G-modules and G'-modules respectively. Notice that we have $f : G' \to G$, which gives ring map $\mathbb{Z}[G'] \to \mathbb{Z}[G]$ which tells us that any G-module is also a G'-module via restriction. So we can effectively view Γ^G and $\Gamma^{G'}$ are from the category of G'-modules.

In particular, if $H \hookrightarrow G$ is a subgroup of G and we take $\phi : A \to A$ to be the identity, we get canonical morphisms:

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

and we will call them the **restriction homomorphisms**. If we consider the quotient map $G \to G/H$ when H is a normal subgroup, and we take $\phi : A \to A'$ by the inclusion $A^H \hookrightarrow A$, we get canonical morphisms:

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

which are called the **inflation homomorphisms**. Recall that A^H has a natural left G/H action where we just define $\overline{g} \cdot x = gx$, we know that if $\overline{g_1} = \overline{g_2}$, then $g_1^{-1}g_2 \in H$, therefore $x = g_1^{-1}g_2x$ which is $g_1x = g_2x$.

Let H be a subgroup of G and let B be an H-module, we will define:

$$\mathrm{Ind}_H^G B = \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], B)$$

Notice that a $\mathbb{Z}[H]$-module map from $\mathbb{Z}[G] \to B$ is actually determined by a map $\phi : G \to B$ such that $\phi(hg) = h\phi(g)$. Notice that given such a morphism $\Phi : \mathbb{Z}[G] \to B$, we get φ by defining $\varphi(g) = \Phi(g)$. Clearly since this is $\mathbb{Z}[H]$-linear, then $\varphi(hg) = h\varphi(g)$. Conversely, recall that we $\mathbb{Z}[H]$-linear map $\mathbb{Z}[G] \to B$ is first an abelian group maps, therefore it comes from $\varphi : G \to B$. Then if $\varphi(hg) = h\varphi(g)$, the you can check the map defined by φ is indeed $\mathbb{Z}[H]$-linear. We define a left G-action on $\mathrm{Ind}_H^G B$ by:

$$(g\phi)(g') = \phi(g'g)$$

Clearly this is indeed a left G action. Then let $\phi \in \mathrm{Ind}_H^G B$, we will define:

$$\theta : \mathrm{Ind}_H^G B \to B, \qquad \theta(\phi) = \phi(1)$$

I claim that this is compatible with H-actions because we have $\theta(h\phi) = h\varphi(1) = h \cdot \theta(\varphi)$.

Remark 1.7. By using the notation $\mathrm{Ind}_H^G B$, you may be reminded of the induced representation when we have a complex representation of H and we want to induce a G representation, what we do is $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} -$ and the result is also denoted by Ind_H^G. So in the case of group cohomology, you may think that this induction should also be some sort of tensor $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} -$, instead of it's Hom definition.

This question is totally reasonable, and the main reason is that if we define it to be the tensor, then we will have functorial isomorphisms:

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} B, A) \simeq \mathrm{Hom}_{\mathbb{G}[H]}(B, A)$$

Therefore it's the left adjoint of the forgetful functor from the category of $\mathbb{Z}[G]$-modules to the category of $\mathbb{Z}[H]$-modules. However, later you will see that instead of being the left adjoint of the forgetful functor, we want it to be the right adjoint. Indeed we have functorial isomorphisms:

$$\mathrm{Hom}_{\mathbb{Z}[H]}(A, B) \simeq \mathrm{Hom}_{\mathbb{Z}[G]}(A, \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], B)) = \mathrm{Hom}_{\mathbb{Z}[G]}(A, \mathrm{Ind}_H^G B)$$

clearly the morphism is defined to be $f \in \mathrm{Hom}_{\mathbb{Z}[H]}(A, B)$ is mapped to the map that maps $a \in A$ to $\varphi_a(g) = f(ga)$. The inverse is given by a map f in $\mathrm{Hom}_{\mathbb{Z}[G]}(A, \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], B))$ is mapped to $a \mapsto f(a)(e)$. This is indeed a $\mathbb{Z}[H]$-map since we know that:

$$ha \mapsto f(ha)(e) = (h \cdot f(a))(e) = f(a)(h) = h(f(a)(e))$$

Clearly these two are inverses of each other and I will let you check it. Therefore this induction we defines here is the right adjoint of the forgetful functor.

Technically speaking, the right adjoint of the forgetful functor is often called the **coinduction** but in the context of group cohomology, we will usually just say it's the induction.

Remark 1.8. Note that as an $\mathbb{Z}[H]$-module, we know that $\mathbb{Z}[G]$ is free with a basis corresponding to the left cosets in G/H. To see why, we choose a representative from each left coset, then via an H-action, we get all $g \in G$. Moreover, we know that since no matter what H-action and linear sums we use, the orbit of a representative of a single coset still lies in that single coset, therefore these representatives are indeed linearly independent.

Then in particular, we know that the induction functor:

$$B \mapsto \mathrm{Ind}_H^G B$$

is going to be an exact functor.

Remark 1.9. Let's prove that right adjoint functors preserves injective objects. Suppose that F a functor between two abelian categories and is the right adjoint of an adjoint functor G. (Notice that the restriction is obviously an exact functor.) Recall that an object I in an abelian category is injective iff the following contravariant functor is exact:

$$\mathrm{Hom}(-, I)$$

Therefore we want to prove that $\mathrm{Hom}(-, FI)$ is an exact functor, and $0 \to A \to B \to C \to 0$ is a short exact sequence. Functoriality of the adjointness implies we have the following diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}(A, FI) & \longrightarrow & \mathrm{Hom}(B, FI) & \longrightarrow & \mathrm{Hom}(C, FI) & \longrightarrow & 0 \\
 & & \uparrow \simeq & & \uparrow \simeq & & \uparrow \simeq & & \\
0 & \longrightarrow & \mathrm{Hom}(GA, I) & \longrightarrow & \mathrm{Hom}(GB, I) & \longrightarrow & \mathrm{Hom}(GC, I) & \longrightarrow & 0
\end{array}$$

Since G is exact and I is injective, we know that the bottom row is exact, which implies the above row is exact.

Theorem 1.10. (Shapiro) Let H be a subgroup of G, and B an H-module. The $\theta : \mathrm{Ind}_H^G B \to B$ induces an isomorphism:

$$H^i(G, \mathrm{Ind}_H^G B) \simeq H^i(H, B)$$

for all i.

Proof. Notice that this θ is compatible with $H \hookrightarrow G$. Notice that:

$$h \cdot \varphi(1) = \varphi(h) = (h\varphi)(1) = \theta(h \cdot \varphi) = h\theta(\varphi) = h \cdot \varphi(1)$$

Therefore we know that θ gives:

$$(\mathrm{Ind}_H^G B)^G \to B^H$$

I claim that this is an isomorphism. First suppose that $\theta(\phi) = 0$, that is $\phi(1) = 0$ where $\phi : \mathbb{Z}[G] \to B$. We can assume that ϕ is fixed by g, that is $g \cdot \phi = \phi$, therefore we know that:

$$\phi(g) = (g \cdot \phi)(1) = \phi(1) = 0$$

Therefore we know that $\phi = 0$. Suppose that $b \in B$ is fixed by all $h \in H$, then consider the ϕ defined by:

$$\phi(g) = b, \quad \forall\ g \in G$$

Notice that $\phi(hg) = b = h \cdot b = h \cdot \phi(g)$, therefore ϕ is well defined. Moreover we know that $(g \cdot \phi)(g') = \varphi(gg') = b$, therefore $g \cdot \phi = \phi$. This proves θ indeed induces an isomorphism $(\mathrm{Ind}_H^G B)^G \to B^H$.

I claim that this fact plus the remark we made above is enough to show the assertion. First, recall that the induction functor is right adjoint to the restriction functor which is exact, therefore for any injective object I in the category of $\mathbb{Z}[H]$-modules, we know that $\mathrm{Ind}_H^G I$ is an injective object in the category of $\mathbb{Z}[G]$-modules. Then we know that given an injective resolution of B, after we apply the induction, we get an injective resolution of B, then we apply the functor Γ^G, then we have the following diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & (\mathrm{Ind}_H^G B)^G & \longrightarrow & (\mathrm{Ind}_H^G I^0)^G & \longrightarrow & (\mathrm{Ind}_H^G I^1)^G & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle \theta} & & \vdots & & \vdots & & \\
0 & \longrightarrow & B^H & \longrightarrow & (I^0)^H & \longrightarrow & (I^1)^H & \longrightarrow & \cdots
\end{array}$$

where the vertical arrow induced by θ is an isomorphism. Then the universal property of derived functors implies that we have the dotted arrows that induced isomorphism on all cohomologies, thus isomorphisms on all $H^i(G, \mathrm{Ind}_H^G B) \to H^i(H, B)$. □

Consider the special case where $H = \{1\}$, then any abelian group M is an H-module. We then can form $\mathrm{Ind}_{\{1\}}^G M = \mathrm{Hom}(\mathbb{Z}[G], M)$ where the hom set is just map of abelian groups. By the previous theorem, we have:

$$H^i(G, \mathrm{Ind}_{\{1\}}^G M) \simeq H^i(\{1\}, M)$$

Recall that we $H^i(\{1\}, M) = 0$ for all $i = 0$ since we know that the functor $\Gamma^{\{1\}}$ is just the identity functor, then for example we apply it to any projective resolution of M, we get the same resolution, therefore we know that only $H^0(\{1\}, M) = M$, and all the other higher degree vanishes.

Definition 1.11. Let G be a group, then any G-module is said to be **induced** if it's isomorphic to $\mathrm{Ind}_{\{1\}}^G M$ for some abelian group M.

A G-module is said to be **weakly injective** if it's a direct summand of a induced G-module. Since we know that cohomology commutes with direct sums and the cohomology of induced G-modules vanishes for all positive degree, we know that the cohomology of weakly injective G-modules also vanishes in positive degrees.

Notice that any G-module A can be embedded into an induced G-module via:

$$\iota : A \hookrightarrow \mathrm{Hom}(\mathbb{Z}[G], A), \qquad \iota(a)(g) = ga$$

This is indeed a G-module homomorphism as $g'a$ is mapped to the $g \mapsto gg'a$, and we know that this is compatible with the G-module structure on $\mathrm{Hom}(\mathbb{Z}[G], A)$. This map is clearly injective as if $ga = 0$ for all g, we know that $a = 0$. One consequence of this embedding shows that injective objects are also weakly injective, thus justifying the name.

Corollary 1.12. Injective G-modules are weakly injective.

Proof. Lett I be an injective G-module. Notice that it's also an abelian group thus is also a $\{1\}$-module. Then we consider the induction:

$$0 \to I \hookrightarrow \mathrm{Hom}(\mathbb{Z}[G], I) \to \mathrm{coker} \to 0$$

We know that since I is injective, then this sequence splits, therefore we know that I is a direct summand of $\mathrm{Hom}(\mathbb{Z}[G], I)$, thus is weakly induced. □

Recall that derived functors can also be computed using acyclic objects, and weakly injective objects are acyclic by our previous discussion. Moreover we also saw that we can embed any G-module into an induced G-module, thus an weakly injective module, therefore we know that we can use resolutions with weakly injective modules to compute cohomology.

Remark 1.13. Notice that if H is a subgroup of G, then any induced G-module is also an induced H-module. Recall that $\mathbb{Z}[G]$ is a free $\mathbb{Z}[H]$-module with basis given by representatives in the cosets G/H, therefore we can also write:

$$\mathbb{Z}[G] \simeq \oplus_{gH \in G/H} \mathbb{Z}[gH]$$

here $\mathbb{Z}[gH]$ is the free abelian group generated by all gh for $h \in H$. The G-actions by g' is first permuting the factors and mapping the element gh to $g'gh$. The H-actions within each factor. Therefore:

$$\mathrm{Hom}(\mathbb{Z}[G], M) \simeq \mathrm{Hom}(\oplus_{gH \in G/H} \mathbb{Z}[gH], M)$$

$$= \prod_{gH \in G/H} \mathrm{Hom}(\mathbb{Z}[gH], M) \simeq \mathrm{Hom}(\mathbb{Z}[H], \prod_{gH \in G/H} M)$$

Therefore by definition any weakly injective G-module I is also an weakly injective H-module. In particular any injective G-module I is a weakly injective H-module, thus we can compute H-cohomology using G-module injective objects. If

$$0 \to I^0 \to I^1 \to \cdots$$

is an injective resolution of a G-module A, then we know that:

$$H^i(H, A) = H^i((I^\bullet)^H)$$

Remark 1.14. (**Hochschild-Serre spectral sequence**) Now suppose that $H \subset G$ is a normal subgroup, we already saw that for a G-module A, A^H is a G/H-module. Most importantly, we know that:

$$(A^H)^{G/H} = A^G$$

It's obvious that the right hand side is contained in the left one, suppose that an element a is fixed by H and then we know that G/H action by $\overline{g'}$ is just defined by $g'a$. Then we know that the left one is contained in the right hand side. This is saying that:

$$\Gamma^{G/H} \circ \Gamma^H = \Gamma^G$$

Then we can apply the Grothendieck composition of functors spectral sequence to get this so called **Hochschild-Serre spectral sequence**:

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

Notice that for and j, $H^j(H, A)$ is indeed still a G/H-module since we know that when we compute the cohomology we already applied the functor Γ^H. This remark will be useful when we study cohomological dimension later and also in later chapters. **** to be completed*

Going back to the main topic, let $H \subset G$ now be any subgroup, for any G-module A, we have a G-module morphism:

$$\iota : A \to \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], A), \qquad \iota(a)(g) = ga$$

I will let you check that for each a, $\iota(a)$ is indeed well define H-module map.

The right hand side of the morphism is like the induction where we first view A as an H-module via restriction. This ι gives a G-module morphism, therefore it induces a morphism:

$$H^i(G, A) \to H^i(G, \mathrm{Ind}_H^G A)$$

we compose this with the isomorphism we obtain eariler:

$$H^i(G, A) \to H^i(G, \mathrm{Ind}_H^G A) \simeq H^i(H, A)$$

we obtain the morphism $H^i(G, A) \to H^i(H, A)$. Note that this map coincide with the restriction morphism we defined earlier since recall that restriction is defined as the unique extension of $A^G \to A^H$. This is just defined by $a \mapsto a$. We consider the above morphism between $H^i(G, A) \to H^i(H, A)$, they are morphisms extending:

$$A^G \to (\mathrm{Ind}_H^G A)^G \xrightarrow{\theta} A^H$$

where this θ is the θ we have in the previous Theorem of Shapiro. Notice that via this map:

$$a \mapsto \iota(a) \mapsto \iota(a)(1) = a$$

Therefore these $H^i(G, A) \to H^i(H, A)$ also extends $A^G \to A^H$, $\quad a \mapsto a$, thus they are equal.

Now let H be a subgroup of finite index of G and A a G-module, we can construct a G-module morphism:

$$\pi : \mathrm{Ind}_H^G A \to A, \qquad f \mapsto \sum_{gH \in G/H} gf(g^{-1})$$

Notice that if g, g' represent the same coset, then we know that $g^{-1}g' \in H$, moreover we know that for any $f \in \mathrm{Ind}_H^G A$, we know that $f(hg) = hf(g)$, therefore we know that:

$$gf(g^{-1}) = gf(g^{-1}g'g'^{-1}) = g(g^{-1}g'f(g'^{-1})) = g'f(g'^{-1})$$

Therefore this definition is well-defined, independent of the representatives we choose for the cosets. This is again, a G-module homomorphism since we know that $g'f \mapsto \sum_{gH \in G/H} g \cdot f(g'g^{-1})$. Notice that:

$$\sum_{gH \in G/H} g \cdot f(g'g^{-1}) = \sum_{gH \in G/H} g'g'^{-1}gf(g^{-1}g') = g' \sum_{gH \in G/H} g'^{-1}gf(g^{-1}g')$$

Then since as g runs over all representatives we know that $g'^{-1}g$ also runs over all representative, the two sides are exactly the same, we are done.

This induces a homomorphism:

$$H^i(G, \mathrm{Ind}_H^G A) \to H^i(G, A)$$

Compose it with the isomorphism $H^i(G, \mathrm{Ind}_H^G A) \simeq H^i(H, A)$ we get:

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

which are called **corestriction homomorphisms**.

Proposition 1.15. Let H be a subgroup of G with finite index n, then we have:

$$\mathrm{Cor} \circ \mathrm{Res} = n$$

Proof. Notice that the composition is:

$$H^i(G,A) \to H^i(G, \mathrm{Ind}_H^G A) \simeq H^i(H,A) \simeq H^i(G, \mathrm{Ind}_H^G A) \to H^i(G,A)$$

The two isomorphism in the sequence are inverses of each other, therefore we know that the composition is induced by:

$$\pi \circ \iota : A \to A, \qquad a \mapsto \iota(a) \mapsto \sum_{gH \in G/H} g \cdot \iota(a)(g^{-1}) = \sum_{gH \in G/H} g \cdot g^{-1} a = na$$

Therefore we know that the corresponding morphism on the derived functors is also multiply by n. □

Proposition 1.16. If G is a finite group of order n, then for any G-module A and any $i \geqslant 1$, $H^i(G,A)$ is annihilated by $|G|$.

Proof. Apply the above proposition to the subgroup $H = \{1\}$. □

Corollary 1.17. Let G be a finite group and p a prime number. If G_p is a Sylow p-subgroup of G and A is a G-module. Recall that the p-primary part of A is the subgroup that is killed by a power of p. Then the restriction map:

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

is injective on the p-primary part of A for any i. In particular if $H^i(G_p, A) = 0$ for all prime number p, $H^i(G,A) = 0$.

Proof. Let $x \in H^i(G,A)$ be an element in the kernel $H^i(G,A) \to H^i(G_p,A)$, we know from the previous proposition that:

$$[G : G_p]x = \mathrm{Cor} \circ \mathrm{Res}(x) = 0$$

If x lies in the p-primary part, then $p^k x = 0$ for some $k \geqslant 0$, then since $[G : G_p]$ is relatively prime to p, then $x = 0$.

Notice that when $i = 0$, the restriction map is just the inclusion $A^G \hookrightarrow A^{G_p}$ and we know that if an element is fixed by all G_p, we know that it's also fixed by G, therefore we know that the assertion on $A^G = 0$ is trivial if $A^{G_p} = 0$. Then if $i \geqslant 1$, we know that since $H^i(G,A)$ is annihilated by $|G|$, then we know that $H^i(G,A)$ decomposes into direct sums of p-primary parts where p is a prime that divides $|G|$, therefore the assertion is also done. □

Remark 1.18. It can be proved quite easily that if an abelian group A is annihilated by some integer $n \geqslant 1$, then:

$$A = \oplus_{p|n} A_p$$

It's clear to show that $A_p \cap A_q = 0$ for different p, q, let $x \in A$, we know that it's order is $p_1^{k_1} \cdots p_r^{k_r}$, then we know that there is integer m, n such that:

$$m p_1^{k_1} \cdots p_{r-1}^{k_{r-1}} + n p_r^{k_r} = 1$$

Then consider:

$$x = (m p_1^{k_1} \cdots p_{r-1}^{k_{r-1}} + n p_r^{k_r}) x$$

We know that now $m p_1^{k_1} \cdots p_{r-1}^{k_{r-1}} x$ is in the p_r-primary part A_{p_r} and the order of $y = n p_r^{k_r} x$ now only is a product of $p_1, \cdots, p_{r-1}$, then we do the same procedure to y until we obtain x as a sum pf p-primary parts.

Corollary 1.19. Let G be a finite group and let A be a G-module finitely generated as an abelian group, then $H^i(G,A)$ is finite for all $i \geqslant 1$.

Proof. Recall that we previously computed the cohomology of G-modules using complexes $C^\bullet(G,A)$. Notice that when A is finitely generated as an abelian group, then we know that the set of all maps from G to A, as G is finite, it just $A^{\oplus |G|}$, therefore is also finitely generated. Then so is the map from G^i to A. Therefore we know that each term in the complex is finitely generated as abelian groups, then so is the cohomology $H^i(G,A)$.

Then we know that for $i \geqslant 1$, $H^i(G,A)$ is annihilated by a finite number, therefore by the structure theorem of finitely generated abelian groups, the group must be finite. □

2 Profinite Groups

In this section we briefly introduce profinite groups before we proceed to the group cohomology of profinite groups.

Definition 2.1. A topological group π is called a profinite group if it's isomorphic to a topological group of the form:

$$\varprojlim_i G_i$$

where I is a direct set and $\{G_i\}$ is an inverse system of finite groups with discrete topology.

Remark 2.2. Let's make a side remark here about why some system is called an inverse (projective) system and some system is called an direct (injective) system. After you see this remark, you will never be confused about the direction of arrows.

Let's explain this through an example. Recall that in the chapter introducing fundamental groups we introduced a weird notation: we define the category I to be the category whose objects are symbols i for each pointed connected etale covering (X_i, α_i) of (S, γ). But we defined the arrows to be $j \to i$ iff there is a pointed S-morphism $(X_i, \alpha_i) \to (X_j, \alpha_j)$. Then we say that $\{(X_i, \alpha_i)\}$ forms an inverse system. In this definition we are think that that if there is an arrow $j \to i$, then the index i is larger than j, and we know that the corresponding morphism $(X_i, \alpha_i) \to (X_j, \alpha_j)$ is a morphism from the space (X_i) to (X_j), which is surjective by the covering space properties. Therefore we regard X_i as containing more refined information than X_j and the morphism is sort of a projection where we forget some information. This is why we call this a projective system (inverse system since the flowing is from the place where there is more information to where there are less information, so regarded as "inverse").

An easier example is the p-adic integers, which is also an inverse system. For example 2-adic integers, the system is given by:

$$\cdots \longrightarrow \mathbb{Z}/2^n \longrightarrow \mathbb{Z}/2^{n-1} \longrightarrow \cdots \longrightarrow \mathbb{Z}/2^2 \longrightarrow \mathbb{Z}/2^1$$

Here the system is index by integers $n \geqslant 1$, therefore has a natural sense of which is larger than another, i.e. there is an arrow $m \to n$ iff $n \geqslant m$. Indeed, we see that in this system there is an arrow $\mathbb{Z}/2^n \to \mathbb{Z}/2^m$ iff there is an arrow $m \to n$. Indeed with the index growing larger, the object contains more information and morphisms between then going in the inverse direction as opposed to the direction of the index or is a projection going from an object with more information to object with less information.

A direct system is the opposite where the arrows between objects is in the same direction as that of index, or from objects with less information to objects with more information. This is like an injective morphism, thus is called an injective system or directed system.

Before we begin any serious study on profinite groups, we need to do some topological preparation.

Lemma 2.3. Let X be a compact Hausdorff topological space and let $x \in X$, then the connected component of X containing x is $\cap_\lambda U_\lambda$ where U_λ is the family of compact open neighborhoods x.

Proof. Recall that in a Hausdorff space a compact subset is closed (which is not true if without Hausdorffness). Then we know that each U_λ is both open and closed, then we know that the connected components containing x must be contained in U_λ. (This also proves that an open and closed subset in any space is a union of connected components.) Therefore we know that:

$$C \subset \cap_\lambda U_\lambda$$

To show that the converse inclusion, it suffice to show that the intersection is connected.

Let $A \subset \cap_\lambda U_\lambda$ is open and closed, we need to show that A is either the entire $\cap_\lambda U_\lambda$ or the empty set. Notice that A and $\cap_\lambda U_\lambda - A$ are both closed in X. Then notice that since $A, \cap_\lambda U_\lambda - A$ are both compact, I will let you see why Hausdorffness implies there are U, V disjoint open neighborhoods of A and $\cap_\lambda U_\lambda - A$.

Then we know that:

$$\cap_\lambda U_\lambda \subset U \cup V$$

Therefore $X-(U\cap V)\subset \cup_\lambda (X-U_\lambda)$. But notice that $X-(U\cap V)$ is closed and X is compact, therefore $X-(U\cap V)$ is compact therefore there will be a finite subcover, i.e.:

$$X-(U\cup V)\subset (X-U_{\lambda 1})\cup\cdots\cup(X-U_{\lambda_n})$$

for finitely many compact open neighborhood of x.

Therefore we know:

$$U_{\lambda 1}\cap\cdots\cap U_{\lambda n}\subset U\cup V$$

Recall that U,V are disjoint, then we know that $U_{\lambda 1}\cap\cdots\cap U_{\lambda n}$ is the union of:

$$U_{\lambda 1}\cap\cdots\cap U_{\lambda n}\cap U,\quad U_{\lambda 1}\cap\cdots\cap U_{\lambda n}\cap V$$

more over since this is a finite intersection, it's both open and closed. Clearly it's open as it's a finite intersection of open subsets, it's closed because we know that they are complement of each other in $U_{\lambda 1}\cap\cdots\cap U_{\lambda n}$ and each of them is clearly open in $U_{\lambda 1}\cap\cdots\cap U_{\lambda n}$.

Notice that only one of them contains x as they are disjoint as the union is $U_{\lambda 1}\cap\cdots\cap U_{\lambda n}$ which contains x. If $x\in U_{\lambda 1}\cap\cdots\cap U_{\lambda n}\cap U$, then we know that $U_{\lambda 1}\cap\cdots\cap U_{\lambda n}\cap U$ is a compact neighborhood of x, thus:

$$\cap_\lambda U_\lambda\subset U_{\lambda 1}\cap\cdots\cap U_{\lambda n}\cap U$$

In particular we know that $\cap_\lambda U_\lambda - A\subset U$, but $\cap_\lambda U_\lambda - A\subset V$, therefore this is the empty set since U,V are disjoint. If $x\in\cap_\lambda U_\lambda\cap V$, we know that:

$$\cap_\lambda U_\lambda\subset U_{\lambda 1}\cap\cdots\cap U_{\lambda n}\cap V$$

in particular, we know that $A\subset V$, but $A\subset U$, therefore $A=\varnothing$. □

Recall that a topological space is said to be **totally disconnected** if any connected subset of X has only a single point. This is equivalent to the fact that every connected component of X is a singleton.

Lemma 2.4. Let G be a compact topological group, then G is totally disconnected if and only if $\cap_\lambda U_\lambda=1$ where U_λ is the family of compact open neighborhood of 1.

Proof. Let's first assume that G is totally disconnected, then we know that $\overline{\{1\}}$ is connected, therefore $\overline{\{1\}}=\{1\}$, thus $\{1\}$ is closed. Recall that the diagonal is the inverse image of $\{1\}$ under:

$$G\times G\to(x,y)\mapsto xy^{-1}$$

therefore the diagonal is closed therefore the space is Hausdorff. Therefore we can apply the above proposition, we must have $\cap_\lambda U_\lambda=\{1\}$.

Conversely, suppose that $\cap_\lambda U_\lambda=\{1\}$, let $g\in\overline{\{1\}}$, we know that gU_λ^{-1} is an open neighborhood of g we know that $1\in gU_\lambda^{-1}$, therefore $g\in U_\lambda$, therefore $g\in\cap_\lambda U_\lambda$, thus $g=1$, therefore $\{1\}$ is closed. Then this implies the space is Hausdorff, therefore we again apply the above lemma to conclude that since the compact open neighborhood at g is just the translation of those at 1 by g, therefore the intersection is still a singleton, thus is $\{g\}$, thus the connected component containing g is $\{g\}$, therefore the space is totally disconnected. □

Lemma 2.5. Let G be a Hausdorff topological group and let U be a compact open neighborhood of $\{1\}$. Then U contains a compact open subgroup of G.

Proof. First notice that any open subgroup must also be closed in any topological group. To see why, we notice that the complement of that subgroup is the union of it's cosets, which are all open, therefore the union is open, which means the subgroup is closed.

Consider $F=(G-U)\cap U^2$. Notice that U^2 is the image of:

$$m:U\times U\to U,\qquad (x,y)\mapsto xy$$

Since the source is compact we know that the image is compact in U, thus compact in X, therefore closed. This implies F is also closed. Notice that:

$$U \cdot 1 \subset G - F = U \cup (G - U^2)$$

Now since U is compact, we can find an open neighborhood V of 1 contained U such that $UV \subset G - F$. To see why, notice hat $U \cdot 1 \subset G - F$ is equivalent to the fact that:

$$U \times \{1\} \subset m^{-1}(G - F)$$

where m is the multiplication map. Then we know that for each $u \in U$, there will be an open neighborhood W_u of u and an open neighborhood V_u of 1 such that $W_u \times V_u \subset m^{-1}(G - F)$, then since U is compact, we only need finitely many then we consider W to be the union of these finitely many W_u and V to be the intersection of these finitely many V_u, we are done.

Recall that V^{-1} is also an open neighborhood of 1, then we can replace V by $V \cap V^{-1}$, we can assume that $V = V^{-1}$. Then we know that:

$$UV \subset (G - F) \cap U^2 \subset U$$

Therefore $UV^n \subset U$ for all $n \geqslant 1$. Then consider:

$$H = \bigcup_{n=1}^{\infty} V^n$$

Notice that since $V = V^{-1}$ this is indeed an open subgroup and the fact $UV^n \subset U$ implies this subgroup is contained in U and is open, therefore is closed, therefore is compact since U is compact. □

Lemma 2.6. Let G be a totally disconnected group and U is a compact subset of G containing some open neighborhood of 1 then U contains a compact open subgroup of G.

Proof. Recall that if G is totally disconnected, then it's Hausdorff since $\{1\}$ is closed, which implies the diagonal is closed, thus Hausdorff.

Let V be the open neighborhood of 1 contained in U. Since U is compact Hausdorff as a subspace of G, we know that $\{1\} = \cap_\lambda U_\lambda$, where U_λ is the family of compact open neighborhoods of 1 in U. We have $\cap_\lambda U_\lambda = \{1\} \subset V$, hence $U - V \subset \cup_\lambda (U - U_\lambda)$. But $U - V$ is compact, then we can find finitely many, say $U_{\lambda 1}, \cdots, U_{\lambda n}$ such that $U - V \subset (U - U_{\lambda 1}) \cup \cdots \cup (U - U_{\lambda n})$ for finitely many compact open neighborhoods U_{λ_i} of 1 in U. Therefore we know that that $U_{\lambda 1} \cap \cdots \cap U_{\lambda n}$ is contained in V. Therefore since $U_{\lambda 1} \cap \cdots \cap U_{\lambda n}$ is open in V then in G, and we know that they are compact, therefore is an open compact neighborhood of 1, therefore contains compact open subgroup of G. □

Remark 2.7. The difference between this lemma and the one before it is that this one we requires G to be totally disconnected, which is stronger than just being Hausdorff, then in this case we don't need a compact open neighborhood of 1 to contain a compact open subgroup. We only need a compact subset of 1 which contains an open neighborhood of 1.

Lemma 2.8. Let G be a topological group and K a compact subset of G. Let U be a neighborhood of 1, then there is another neighborhood V of 1 such that:

$$xVx^{-1} \subset U$$

for all $x \in K$.

Proof. Consider the continuous map:

$$G \times G \to G, \qquad (x, y) \mapsto xyx^{-1}$$

Notice that $(x, 1) \mapsto 1$ for any $x \in G$. Therefore for any $x \in K$, we can find a neighborhood W'_x of 1 and a neighborhood W_x of x such that:

$$x' y x'^{-1} \in U$$

for all $x' \in W_x$ and $y \in W'_x$. Since K is compact, we can find finitely many W_x, say $W_{x_1}, \cdots, W_{x_n}$ so that they cover K, then we define $V = W'_{x_1} \cap \cdots \cap W'_{x_n}$. □

All these lemmas above is for the following result:

Proposition 2.9. Let G be a compact totally disconnected topological group and let U be a subset of G that contains a open neighborhood of 1, then U contains a normal open subgroup of G.

Proof. G is compact and Hausdorff. Since we know that U contains an open neighborhood of 1, say it's W. Then consider $F = G - W$, we know that since G is compact F is compact. Since G is Hausdorff, we know that for each $x \in F$, there is an open neighborhood W_x of 1 and W'_x of x such that $W_x \cap W'_x = \varnothing$. Notice that F is compact, we can choose finitely many W'_x that covers F. Then we find an open neighborhood O of 1 such that it doesn't intersect F, which means that it's contained in W. Moreover we know that $\overline{O} \subset W$ since we know that O is the intersection of finitely many W_x, and O doesn't intersect an open neighborhood of F, then if the closure of O intersects F, we know that it O must intersection with every open neighborhood of F a contradiction, we are done.

This implies that U contains a compact subset of G which again contains an open neighborhood of 1. Therefore by the previous lemma, U contains a compact open subgroup of G, let's call it V. Then we know there is another open neighborhood V' of 1 such that $xV'x^{-1}V$ for any $x \in G$ since G is itself compact. Therefore:

$$V' \subset \cap_{x \in G} x^{-1} V x$$

is a subgroup contained in U.

Now notice that in a topological group, any subgroup containing an open neighborhood of 1 is open. I will let you prove why, therefore $\cap_{x \in G} x^{-1} V x$ is open and normal. □

Corollary 2.10. Let G be a compact totally disconnected topological group, then open normal subgroups of G forms a basis of 1.

Proof. Notice that any open neighborhood of 1 contains such an open normal subgroup of G. In particular, we know that an open normal subgroup also contains a normal open subgroup of G, we are done. □

Remark 2.11. Let's summarize some of the topological properties we used to prove the above several lemmas and the proposition.

1. First we know that in a topological group the identity being closed implies Hausdorff and it's clear that Hausdorff implies the identity is closed.
2. Then in a compact Hausdorff space, for any closed subset F and a point not in F, there is an open neighborhood of x and an open neighborhood of F such that these two neighborhoods are disjoint.
3. Then in a topological group, any open subgroup is closed.
4. Any subgroup containing an open neighborhood of 1 is open.

Using the above proposition, we can prove several properties of profinite groups:

Corollary 2.12.
1. A topological group is a profinite group iff it's compact and totally disconnected.
2. Direct products of profinite groups are profinite.
3. The inverse limit of any inverse system of profinite groups is profinite.
4. If H is a closed subgroup of a profinite group, then the spaces of cosets with the quotient topology is totally disconnected and if H is normal, G/H is profinite.

Proof. Let's first deal with 1. Let $G = \varprojlim G_i$ where $\{G_i\}$ is an inverse system of finite discrete groups. Notice that by Tychnoff's theorem, $\prod_i G_i$ is compact. Then I claim that with the subspace topology $\varprojlim G_i$ is closed. This is very similar to the preliminary section where we proved that the Galois group of an infinite Galois extension is closed in the product space. Notice that if we write:

$$C_{i,,j} = \{(x_k) : \pi_{ij}(x_i) = x_j\}$$

if there is no π_{ij} from G_i to G_j, then $C_{i,j}$ is just the whole space. Then $\varprojlim G_i$ is the intersection of all $C_{i,j}$ when i, j ranges through all pairs of index. Notice that each $C_{i,j}$ is the inverse image of the identity under the map:

$$\varprojlim G_i \to G_j, \qquad (x_k) \mapsto x_j/\pi(x_i)$$

I will let you check this is continuous since each G_i is discrete. Then the inverse limit is also closed. Therefore $\varprojlim G_i$ is compact. Let C be a connected subset of $\varprojlim G_i$, then we know that the projection of C to each G_i is connected, therefore is only one point since each G_i is discrete. This implies C only contains one point, we are done.

Conversely, suppose that G is a compact totally disconnected group. Recall that open normal subgroups of G is a basis of 1. Notice that if N is an open normal subgroup of G, we consider G/N, this is again compact since G is compact. Then since N is normal, we know that G/N is a discrete group as we know that the inverse image of a coset in G/N is just a translation of N, which is open, then since G/N is with the quotient topology, that singleton is open. Therefore G/N is finite and discrete. Then consider:

$$\varprojlim_N G/N$$

where N is the system of open normal subgroup of G. We know that it's a direct set via inclusion, and G/N forms an inverse system with respect to this order.

Noticed that we have a canonical morphsim induced by the quotient maps: $G \to G/N$:

$$G \to \varprojlim_N G/N$$

This is continuous since it's induced by the universal property. I claim that the image is the morphism is dense. To see why, we know that the basic opens in $\varprojlim_N G/N$ is the intersection of $\varprojlim_N G/N$ with the basic opens in $\prod_N G/N$, which is $\prod_N U_N$ where U_N are open in G/N and only finitely many of them is not the whole space G/N. Recall that since we work with a direct set, there is a N' such that G/N' maps to all these finitely many G/N. Then we know that if an element is in the intersection of $\varprojlim_N G/N$ with this basic open. The G/N component all comes from some gN' in G/N'. Then consider (gN) in the product, we know that this is indeed in the inverse limit and is in the intersection. Since (gN) is the image of $G \to \varprojlim_N G/N$, the image is indeed dense.

Recall that since $\varprojlim_N G/N$ is Hausdorff and G is compact, this map is closed, therefore is surjective. To prove it's injective, we know that if g in G is mapped to 0, then it's in all the normal open subgroup in G. Recall that G is totally disconnected, therefore $\{1\} = \cap_\lambda U_\lambda$ where U_λ are all the compact open neighborhoods of 1. Note that any compact open neighborhood of 1 contains such an open normal subgroup, therefore we know that $g \in U_\lambda$ for all λ, therefore $g = 1$. This implies $G \to \varprojlim_N G/N$ is a bijective and closed homomorphism, therefore is an isomorphism of topological groups.

Then let's prove 2: Notice that a closed subgroup of a compact group is compact. It's also totally disconnected as a subspace.

Notice that direct product of compact spaces is compact. Moreover let G_i be compact and totally disconnected topological groups, consider the projection:

$$\prod_i G_i \to G_i$$

If C in the product space is connected, we know that the image in G_i is connected, therefore is a single point, therefore C is also a single point.

4 is also easy, let G_i be an inverse system of profinite groups, we know that their product is also profinite, then the inverse limit of these system is a closed subgroup of the direct product, we are done. What need to be noticed here is that by an inverse system of profinite groups, we automatically assume that the transition maps between G_i and G_j are continuous, without this condition the inverse limit may not be a closed subgroup.

Finally to prove 5: let's first show that G/H is totally disconnected. To prove this, first notice that G/H with the quotient topology is also a compact topological group. Then by our previous lemma, a compact

topological group is totally disconnected iff $\cap_\lambda U_\lambda = \{1\}$ where U_λ is the family of compact open neighborhoods of 1. Then suppose that $xH \notin \{H\}$, we want to show that there is a compact open neighborhood of H such that xH is not in that compact open neighborhood. $xH \notin \{H\}$ means that $1 \notin xH$, since xH is a closed subset of G, then we know that there will be an open subgroup U that is disjoint from xH. Notice that the quotient map $\pi : G \to G/H$ is open, then since U is open in G, it's closed and compact, then the image of U in G/H is a compact open neighborhood of 1, therefore we know that $xH \notin \pi(U)$, therefore we are done. Finally H is normal, then G/H is a group that is compact and totally disconnected therefore is profinite. □

Definition 2.13. A **surnatural** number (sometimes also called **supernatural** number) is a formal product $\prod_p p^{n_p}$ where p ranges over all prime numbers and n_p is a nonnegative number that is probably ∞.

It's clear that the product of two surnatural numbers is defined component-wise. We can also define the greatest common divisor of two surnatural number using their exponent power in an obvious way. Similarly, we can define the least common multiple. Similar definition can also be applied to any family of surnatural numbers, where the exponent power is defined to be the supremum or infimum.

Definition 2.14. let G be a profinite group and let H be a closed subgroup of G, we define the **index** of H in G by the least common multiple of:

$$[G/U : H/(H \cap U)]$$

where U is goes over the family of normal open subgroups of G.

Recall that for any open normal subgroup U, G/U is a finite discrete group, and $H/(H \cap U)$ is a subgroup of G/U, therefore has a finite index. Notice that the least common multiple of these finite index is a surnatural number.

We only define the index for closed subgroups because we know that the index for open subgroups is always finite (can you see why?). We will later see that a closed group is open iff it's index defined in the above way is finite.

Remark 2.15. There is another way to think about the index of the closed subgroup H in G. Let V be an open subgroup of G that contains G. We know that G/V is a finite discrete space, therefore we know that $[G : V]$ is a finite number, then we define the index of H in G to be the least common multiple of:

$$[G : V]$$

where V goes over all open subgroup of G that contains H.

To see why, if U is an open normal subgroup of G, then consider HU, which is the union of of hU for all $h \in H$. Therefore HU is still an open subgroup containing H. Moreover notice that we have an isomorphism:

$$H/H \cap U \simeq HU/U$$

Then we know that:

$$[G/U : H/(H \cap U)] = [G/U : HU/U]$$

since we have a bijection coming from:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H/H \cap U & \longrightarrow & G/U & \longrightarrow & (G/U)/(H/H \cap U) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \vdots & & \\ 0 & \longrightarrow & HU/U & \longrightarrow & G/U & \longrightarrow & (G/U)/(HU/U) & \longrightarrow & 0 \end{array}$$

Chasing the diagram tell you that the dotted arrow is a bijection.

Conversely, if V is an open subgroup containing $H = H \cdot 1$, then since H is closed, then it's compact, then there will be U and open neighborhood of 1 such that $HU \subset V$, we can assume that U is a normal open subgroup by the previous proposition. Then we know that V as a subgroup sitting in between HU and G, we know that the index $[G : V]$ must divide that of $[G : HU] = [G/U : H/H \cap U]$ (a finite number), i.e.:

$$[G : V] | [G : HU] = [G/U : H/H \cap U]$$

The first equation shows that the least common multiple of $[G : V]$ is at least as large as that of $[G/U : H/H \cap U]$. The second equation shows that it's at most as large as that of $[G/U : H/H \cap U]$, therefore they are equal.

The fact that $[G : V]$ must divide $[G : HU]$ comes from the surjection:

$$G/HU \to G/V$$

The "kernel" (the preimage of the identity coset in G/V) looks like HU/V, then using the fact that G/HU only has finitely many element, we get that the assertion. Or you can use the fact that $[G : HU]$ is finite to do counting.

Remark 2.16. Recall that if H is a closed subgroup such that indeed G/H is a finite set, then we know that we can define the index traditionally, by the number of elements in G/H. Or we can still define it according to the above definition. It can be checked that these two definitions agree, first, we know that for any open subgroup V containing H, the number of elements in G/V is at most that of G/H. Moreover we know that:

$$[G : V] \cdot [V : H] = [G : H]$$

Therefore we know that each $[G : V]$ will divide $[G : H]$, therefore we know that the least common multiple will divide $[G : H]$ and in particular is finite. We will prove later that a finite index implies the closed subgroup is open, therefore the two definition agrees.

One caveat here is that before we prove that finite index imply open subgroup, we can't conclude that the two ways of definition are the same. So when you prove finite index implies open, you can not say that G/H is a finite set and H is the complement of a finite union of closed subsets, thus open. Be careful!

Proposition 2.17. Let G be a profinite group:

1. For all closed subgroups K and H of G such that $K \subset H$, we have:

$$[G : K] = [G : H] \cdot [H : K]$$

2. For all closed subgroups K and H of G such that $K \subset H$ and K is normal in G, we have:

$$[G/K : H/K] = [G : H]$$

3. A closed subgroup H in G is open iff $[G : H]$ is finite.

4. Let $\{H_i\}$ be a decreasing filtered family of closed subgroups in G and $H = \cap_i H_i$, then $[G : H]$ is the least common multiple of $[G : H_i]$.

Proof. Let's deal with 1 first: we will show that $[G : K] | [G : H] \cdot [H : K]$. Notice that for any normal open subgroup U in G, we have:

$$[G/U : K/K \cap U] = [G/U : H/H \cap U] \cdot [H/H \cap U : K/K \cap U]$$

By definition we know that:

$$[G/U : H/H \cap U] \cdot [H/H \cap U : K/K \cap U] | [G : H] \cdot [H : K]$$

as we know that $U \cap H$ is also an open normal subgroup in H.

Then since each $[G/U : K/K \cap U]$ divide $[G : H] \cdot [H : K]$, the least common multiple divides it, we are done.

Conversely, let U be an open normal subgroup of G and V an open subgroup of H. We know that there is an open normal subgroup U' of G such that $H \cap U' \subset V$. This is because we know that $V \subset H$ is $V' \cap H$ where V' is an open neighborhood of 1, therefore it contains a normal open subgroup U' and $U' \cap H \subset V' \cap H = V$. Let $U' = U \cap U''$ which is still an open normal subgroup of G. Then we have:

$$[G : HU] \cdot [H : KV] | [G : HU''] \cdot [H : K(H \cap U'')]$$

This holds because we know that $HU'' \subset HU$ and the index $[G : HU'']$ is finite. Then again we know that $K(H \cap U'') \subset KV$, and the index $[H : K(H \cap U'')]$ is finite.

Note that:

$$[G : HU] = [G/U : H/H \cap U], \quad [H : KV] = [H/V : K/K \cap V]$$

$$[G : HU''] \cdot [H : K(H \cap U'')] = [G/U'' : H/H \cap U''] \cdot [H/H \cap U'' : K/K \cap U''] = [G/U'' : K/K \cap U'']$$

Therefore we know that:

$$[G/U : H/H \cap U] \cdot [H/V : K/K \cap V] | [G/U'' : K/K \cap U'']$$

Hence we know that we proved:

$$[G : H] \cdot [H : K] | [G : K]$$

Therefore they are equal.

Then we deal with 2: recall that if we have an open subgroup in G/K containing H/K, we know that it's preimage in G is an open subgroup containing H, conversely any open subgroup containing H in G is mapped to an open subgroup of G/K containing H/K. They are bijection of each other.

Moreover we know that:

$$[G/K : U/K] = [G : U]$$

Then we use the description of the index using open subgroup containing that group, we are done.

For 3: we already know that if H is open, then G/H is finite since gH forms an open cover of G, then we can use the fact that G is compact. Then $[G : H]$ is indeed finite. Conversely, if $[G : H]$ is finite, we can find an open subgroup V containing H such that $[G : H] = [G : V]$. To see why, let's assume that $[G : H] = p_1^{n_1} \cdots p_r^{n_r}$ where p_i's are distinct primes. Then since $[G : H]$ is defined to be the least common multiple of $[G : V]$ where V is an open subgroup containing H. Then we know that there will be finitely many open subgroups V such that $[G : V]$ actually has factor $p_i^{n_i}$. Then we take intersection, it will suffice. Then I claim that $V = H$. Suppose that V is not H, then there is an $x \in V - H$, since x is not in H, we know that $1 \notin xH$. Notice xH is closed, then we know that there is an open normal subgroup U of G such that $U \cap xH$ is empty. Therefore we know that $x \notin UH$, hence $V \cap UH$ is strictly contained in V. But $V \cap UH$ is an open subgroup containing H so we have:

$$[G : H] \geqslant [G : V \cap UH] > [G : V]$$

which is a contradiction, we are done.

Finally to prove 4: notice that if V is an open subgroup of G, we know that $G - V$ is compact, then we know that $\cap_i H_i \subset V$ iff $H_i \subset V$ for some i. Indeed consider $G - H_i$, which are all open. Then if $\cap_i H_i \subset V$, we know that $G - H_i$ covers $G - V$, we know that by compactness, we only need finitely many $G - H_i$, therefore $H_{i_1} \cap \cdots \cap H_{i_n}$ is contained in G, then there is some H_i contained in the intersection. Conversely if there is such a $H_k \subset G$, then since the system is filtered, we know that for any H_i not contained in H_k, there will be some H_j contained in $H_i \cap H_k$, then:

$$\cap_i H_i = \cap_{i \leqslant k} H_i$$

therefore we are done. Then we know that if V is an open subgroup containing H_i, then V contains H, therefore

$$[G : H_i] | [G : H]$$

therefore the least common multiple of $[G : H_i]$ divides $[G : H]$. Conversely, we know that if V is an open subgroup containing H, it must contain some H_i, therefore:

$$[G : V] | [G : H_i]$$

therefore we know that $[G : H]$ as the least common multiple of $[G : V]$, divides the least common multiple of $[G : H_i]$, we are done. □

Definition 2.18. Fix a prime number p, we will say a profinite gourp is a **pro-p-group** if $[G : 1]$ is a power of p as a surnatural number.

Given a profinite group G, a closed subgroup H is called a **Sylow-p-subgroup** if H is a pro-p-group and $[G : H]$ is prime to p as a surnatural number.

One thing to notice here is that a profinite group is a pro-p-group iff it's an inverse limit of finite p-groups, i.e. finite groups whose order is a power of p. To see why, suppose that G is a pro-p-group, then we know that $[G:1]$, which is the least common multiple of $[G/N : 1/1 \cap N]$ where N is a normal open subgroup of G. This implies that for each normal open subgroup N, the order of G/N is a power of p. We have seen that G is isomorphic to $\varprojlim_N G/N$ where N ranges over all normal open subgroups of G. Conversely, suppose that $G = \varprojlim_i G_i$ where each G_i is a finite p-group. Then consider the projection to the i-th component:

$$\varprojlim_i G_i \to G_i$$

we know that the kernel is a normal open subgroup of $\varprojlim_j G_i$ and suppose that N is a normal open subgroup of G, then I claim that N must contain one of these kernels. To see why, we know that the basic opens of the identity in $\varprojlim_i G_i$ are finite intersections of the kernels. Therefore we know that the normal open subgroup N contains some intersection of K_i. But recall that this is an inverse system, therefore we know that that there will be some G_k that maps to G_i for these finitely many i. Then we know that the kernel with respect to G_k is contained in the intersection, we are done.

Therefore we know from the previous proposition that:

$$[G/N : 1]||G_k| = p^{n_k}$$

therefore the least multiple of $[G/N : 1]$ is also a power of p.

Proposition 2.19. 1. Let G be a profinite group, then any pro-p-group H is contained in a Sylow-p-subgroup. In particular, Sylow-p-subgroup exists and any two Sylow-p-subgroup are conjugate in G.

2. Let $G \to G'$ be an epimorphism of profinite groups, then the image of of a Sylow-p-subgroup of G in G' is again a Sylow-p-subgroup.

Proof. Let's deal with 1: notice that for any normal open subgroup U of G, G/U is a finite discrete group with $H/H \cap U$ a subgroup of G/U. Notice that since H is a pro-p-subgroup, we know that the index of order of $H/H \cap U$ is a power of p as $H \cap U$ is an open normal subgroup of H. Then we know that there will be a Sylow-subgroup in G/U containing $H/H \cap U$, then let $\mathcal{I}_U$ be the set of Sylow-p-subgroups of G/U containing $H/H \cap U$.

Then suppose that we have two normal subgroups $V \subset U$, we know that we have a surjective group homomorphism between finite groups:

$$G/V \to G/U$$

Recall that for a surjective homomorphism between finite groups, Sylow-p-subgroups is mapped to Sylow-p-subgroups. Therefore this map induces a map $\mathcal{I}_V \to \mathcal{I}_U$. This gives you an inverse system and we can consider:

$$\varprojlim_U \mathcal{I}_U$$

I claim that this inverse limit is not empty.

This is an important fact, which also explains why for example the profinite group is nonempty and the fundamental group is nonempty. To see this, notice that we can give eachh $\mathcal{I}_U$ the discrete topology. Since each of them is finite we know that it's compact, therefore the product space is compacy by Tychnoff's theorem. We also know that we can represent the inverse limit as intersections of closed subsets. We know that given any finitely many such closed subsets, the intersection is nonempty, then since the space is compact, the intersection of all the closed subsets must also be nonempty since this is what characterize a compact space.

Then we can assume that (P_U) is an element in this inverse limit and we know that we can consider the inverse limit of P_U, i.e. $\varprojlim_U P_U$. We know that each P_U is a finite p group, then we know that the inverse limit is a pro-p-group by our remark above. Moreover we know that we have the following diagram:

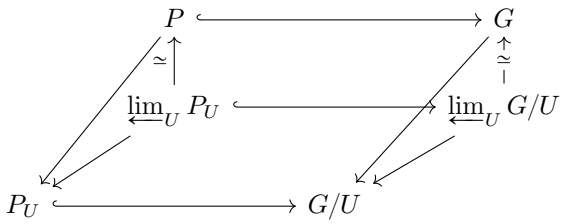
$$0 \longrightarrow \varprojlim_U P_U \hookrightarrow \varprojlim_U G/U \xrightarrow{\simeq} G$$

The first morphism is injective since we know that inverse limit of an inverse system is left exact. Then we know that $\varprojlim_U P_U$ defines a pro-p-subgroup P that contains H.

Now we know that the index $[G : P]$ is going to be the least common multiple of:

$$[G/U : P/P \cap U]$$

where U is an open normal subgroup of G. Notice that we have a diagram:



Then I will let you check that:

$$[G/U : P/P \cap U] = [G/U : P_U]$$

where $[G/U : P_U]$ is a number that is prime to p, then $[G : P]$ is the least common multiple of these numbers therefore is a number prime to p, therefore P is indeed a Sylow-p-group.

Then let P, P' be two Sylow-p-subgroups of G, we need to show that they are conjugate. Again, let U be a normal open subgroup of G, we know that $PU/U \simeq P/P \cap U$ and $P'U/U \simeq P'/P' \cap U$ are two subgroups of G/U. I claim that $P'U/U$ and PU/U are both Sylow-p-subgroups of G/U. To see why, we know that:

$$[G/U : PU/U] = [G : PU]|[G : P]$$

Since P is a Sylow-p-subgroup, we know that $[G : P]$ is prime to p, therefore $[G/U : PU/U]$ is prime to p, therefore PU/U is a Sylow-p-subgroup. Similar proof can be applied to $P'U/U$. Then consider the set of elements $x \in G/U$ such that $x^{-1}(PU/U)x = P'U/U$. Let's call it A_U, since we know that $PU/U, P'U/U$ are Sylow-p-subgroups of G/U, we know that A_U is nonempty and finite. Moreover if $V \subset U$, we know that we have a morphism $A_V \to A_U$ defined by $G/V \to G/U$. Since we know that if $x^{-1}(P/V \cap P)x = P'/V \cap P'$. Then I will let you show that $x^{-1}(P/U \cap P)x = P'/U \cap P'$. Then we know that this $A_V \to A_U$ is actually well defined. Then we can consider the inverse limit $\varprojlim_U A_U$ and we know it's not empty, pick (x_U) in the inverse limit and let x be it's image in G, we consider:

$$x^{-1}Px$$

Recall that this is the same as $\varprojlim_U x_U^{-1}(PU/U)x_U = \varprojlim_U P'U/U = P'$ we are done.

Then let's prove 2: let N be the kernel of $G \to G'$, then $G' \simeq G/N$. Let P be a Sylow-p-subgroup of G, we know that it's image in G' is identified with PN/N, then we know that:

$$[G/N : PN/N] = [G : PN]|[G : P]$$

since $[G : P]$ is prime to p, then so is $[G : PN]$. Recall that for it to be a Sylow-p-subgroup we need to show PN/N is a pro-p-subgroup, which is to show that: $[PN/N : 1]$ is a power of p. Notice that P is a pro-p-subgroup, then we know that:

$$[PN/N : 1] = [P/P \cap N : 1] = [P : P \cap N]$$

The last equation holds trivially. But by definition of $[P : 1]$ we know that $[P : P \cap N]$ divides $[P : 1]$, therefore $[P : P \cap N]$ is a power of p. □

Remark 2.20. One last remark we make here is that notice that any Sylow-p-subgroup of a profinite group is closed. We prove that any two Sylow-p-subgroups are conjugate, therefore we only need to prove one of them is closed.

Consider how we constructed one Sylow-p-subgroup, we picked a Sylow-p-subgroup in G/U for each normal open subgroup U of G and take the inverse limit. I will let you check that the inverse limit is equal

to the intersection of all the inverse images of P_U under the map $G \to G/U$. Since P_U is closed in G/U, then the inverse image in G is closed, therefore the intersection is closed. We mention this because that in the preliminary section on Galois theory, we prove that if we deal with an infinite Galois extension, for example the separable closure of a field, K_s/K. Then if we pick a closed subgroup H of $\mathrm{Gal}(K_s/K)$ and let $L = K_s^H$, we can conclude that $\mathrm{Gal}(K_s/L) = H$. But this only holds for closed subgroups, therefore since any Sylow-p-subgroup is closed, we can apply this to any Sylow-p-subgroup.

3 Cohomology of Profinite Groups

Let G be a profinite group and let A be an abelian group on which G acts on the left. We will put discrete topology on A, we will in this section study continuous actions of G on A and the cohomology of this group action.

Remark 3.1. Let's first make a few useful observations. First of all recall that we say G acts continuously on A if the following map is continuous:

$$G \times A \to A$$

We have three equivalent conditions to guarantee a continuous action. Consider the stabilizer of $x \in A$, i.e.:

$$G_x = \{g \in G : gx = x\}$$

It's easy to see that if the action is continuous then G_x is open. Consider the restriction of this map to the subspace $G \times \{x\} \to A$, then we know that in this subspace an open subset is $U \times \{1\}$ where U is open in G. Then we know that G_x is the inverse image of $\{x\}$ in A, which is open, therefore G_x is open.

Consider the condition that:

$$A = \bigcup_U A^U$$

where U run over all the open subgroups of G. If G_x is open, then we know that obviously:

$$A = \bigcup_{x \in A} A^{G_x} = \bigcup_{x \in A} \{x\} = A$$

Then finally suppose that A is the union of all A^U. We know that to prove $G \times A \to A$ is continuous, we only need to show that the inverse image of each $x \in A$ is open. Notice that any $x \in A$ is in A^U for some U, then if $gy = x$, i.e. (g, y) is mapped to x, we know that $gU \times \{y\}$ is mapped to x, therefore we know that the inverse image of x is going to be open, therefore $G \times A \to A$ is continuous.

Remark 3.2. Here is a side remark which gives you an example of an action of a profinite group on the left of a discrete abelian groups which is not continuous. By seeing this example, you will have the feeling that in general the action we see will be continuous, as to provide the following example, we have to use abstract cardinality argument.

First of all, consider the $\mathbb{F}_2$-vector space $\prod_{n \geqslant 1} \mathbb{F}_2$, where $\mathbb{F}_2$ is given the discrete topology and the product is the product topology. Consider a group homomorphism from:

$$\prod_{n \geqslant 1} \mathbb{F}_2 \to \mathbb{F}_2$$

which is just a linear functional of $\mathbb{F}_2$-vector space on $\prod_{n \geqslant 1} \mathbb{F}_2$. It's it's a continuous linear functional, we know that the kernel should be open in the product. Then using the basic opens in $\prod_{n \geqslant 1} \mathbb{F}_2$, we know that the continuous linear functions are those that are determined by finitely many components in the product. That is saying if $\chi : \prod_{n \geqslant 1} \mathbb{F}_2 \to \mathbb{F}_2$ is continuous, then $\chi(x) = \sum_{x_n \in F} a_n x_n$ where F is a finite subset of the positive integers. Therefore we know that continuous linear functionals only has cardinality that is countable, i.e. of cardinality $\aleph_0$.

However, we know that since the dimension of $\prod_{n \geqslant 1} \mathbb{F}_2$ is $2^{\aleph_0}$, we know that the linear functionals on $\prod_{n \geqslant 1} \mathbb{F}_2$ will be $2^{2^{\aleph_0}}$, which is strictly larger than $\aleph_0$, therefore we know that there will be a linear functional that is not continuous. You can also try to give a description of such a noncontinuous functional, but it will

also use something called an ultrafilter on the natural numbers, which again uses axiom of choice. So in this way, you will see that it's not easy to encounter in real life such a noncontinuous linear functional.

Then think about the action of $\prod_{n\geqslant 1}\mathbb{F}_2$ on $\mathbb{Z}$, which is a group homomorphism:

$$\prod_{n\geqslant 1}\mathbb{F}_2 \to \mathbb{Z}/2\mathbb{Z}$$

We know that if this is a continuous action, then the stabilizer of 1 is open, which is the kernel of 1 in $\prod_{n\geqslant 1}\mathbb{F}_2 \to \mathbb{Z}/2\mathbb{Z}$, where $\mathbb{Z}/2\mathbb{Z}$ is given the discrete topology. This is equivalent to the group homomorphism $\prod_{n\geqslant 1}\mathbb{F}_2 \to \mathbb{Z}/2\mathbb{Z}$ is continuous, but we have seen that there are noncontinuous such homomorphisms.

For the sake of the above remark, since we will not typically see a noncontinuous action, we simply call a discrete abelian group on which G acts left continuous a G-module and it will be our convention in this section unless otherwise stated.

Therefore we are effectively considering a full-subcategory of the category of all $\mathbb{Z}[G]$-modules where we require the action to be continuous, i.e. we are putting constraints on what sort of $\mathbb{Z}[G]$-module structures are allowed. This category obvious still have enough projectives, as we can always use free $\mathbb{Z}[G]$-modules and the fact that G is a topological group implies that the free objects with the usually actions is indeed continuous. Then you can prove that this category is still abelian by checking that the usual kernel cokernel satisfies the condition. Then we can prove that this category is with enough injectives. We will later define a induction functor Ind_H^G for a closed subgroup H in this new category and will show that it's right adjoint to the forgetful functor and is exact, therefore we know that this functor preserves injectives, then if B is an injective abelian group, we know that:

$$\mathrm{Ind}_{\{1\}}^G B$$

is an injective G-module, then if A is a G-module, we can first embed it into an injective abelian group $A \hookrightarrow A$, then we apply:

$$\mathrm{Ind}_{\{1\}}^G A \hookrightarrow \mathrm{Ind}_{\{1\}}^G B$$

Therefore we can define the group cohomology in this new category similarly as what we did in the general group cohomology setting, i.e. as the right derived functor of the left exact functor Γ^G.

We can do this, but when we insist on continuous actions, there will be another way of defining the derived functor that is easier to work with. This is what we will discuss below, and later we will show that this new definition agrees with the usual definition of the derived function.

Now for a G-module A and a nonnegative integer n, let $C^n(G,A)$ be the set of continuous maps from G^n to A. Recall that if you play out the argument we gave in the general group cohomololy, this notation is used to denote all the maps from G^n to A, but here we use it to denote only the continuous maps.

Notice that $C^n(G,-)$ is an exact functor from the category of G-modules to the category of abelian groups. (Notice that for each G-module A, $C^n(G,A)$ is an abelian group.) Then we define:

$$d_n; C^n(G,A) \to C^{n+1}(G,A)$$

by:

$$(d_n f)(g_1,\cdots,g_n) = g_1 f(g_2,\cdots,g_{n+1}) + \sum_{j=1}^{n}(-1)^j f(g_1,\cdots,g_{j-1},g_j g_{j+1},g_{j+2},\cdots,g_{n+1}) + (-1)^{n+1} f(g_1,\cdots,g_n)$$

You may recall that this is exactly the same definition we give in the section introducing the abstract group cohomology, except here $C^i(G,A)$ are only continuous maps rather than all maps. Therefore this is a complex. Note that $d_n f$ is also a continuous map.

Definition 3.3. Let G be a profinite group and A be a discrete abelian group which has a continuous left G-action, then we define the n-**th cohomology group** of A with respect to this action by $H^n(G,A)$ being the n-th cohomology of this complex $C^\bullet(G,A)$. We will also denote it by $R^n\Gamma^G(A)$.

Remark 3.4. By this notation $R^n\Gamma^G$, we are implying that this definition of cohomology is going to be the same as the old group cohomology we defined before when discussing the general group cohomology stuff. We will prove this later.

Theorem 3.5. Let I be a direct set. Let $\{G_i\}_{i\in I}$ be an inverse system of profinite groups and let $\{A_i\}_{i\in I}$ be a direct limit of abelian groups such that each A_i is a G_i-module. For $i \leqslant j$ in I, suppose that $A_i \to A_j$ is compatible with the homomorphism $G_j \to G_i$ in the obvious sense. Set $G = \varprojlim_i G_i$ and $A = \varinjlim_i A_i$, then there is a canonical isomorphism of complexes:

$$\varinjlim_i C^\bullet(G_i, A_i) \to C^\bullet(G, A)$$

Recall that the direct limit is an exact functor, thus commutes with the cohomology functor, thus we have an isomorphism:

$$\varinjlim_i H^\bullet(G_i, A_i) \to H^\bullet(G, A)$$

Like the assumption we made in the previous sections, by an inverse limit of topological groups, we mean that the transition maps between them should be continuous as well. The proof of the theorem is not interesting, but a lot of details, just make sure you understand it and don't have to be too serious:

Proof. First, note that $C^\bullet(G_i, A_i)$ is indeed a direct system of complexes since we have the diagram:

$$\begin{array}{ccccc} A_k & \longleftarrow & A_j & \longleftarrow & A_i \\ & & & & \uparrow \\ G_k^n & \longrightarrow & G_j^n & \longrightarrow & G_i^n \end{array}$$

where $k \geqslant j \geqslant i$. Then we know that given a morphism $G_i^n \to A_i$, we can use the above diagram to give a morphism $G_j^n \to A_j$ and so on. You can check this is indeed a direct system. Then the map $\varinjlim_i C^\bullet(G_i, A_i) \to C^\bullet(G, A)$ is just defined by the universal property of the direct limit.

Another thing to notice here is that A the direct limit is still equipped with the discrete topology as it's just the quotient of a discrete space, thus is still discrete. Then we know that the action of G on A is defined by $((g_i), \overline{a_j}) \mapsto \overline{g_k a_k}$ where k is some index dominating i, j. This is well defined since if we consider another representative $a_{j'}$, then we know that we can now take k' to dominate k, j' and we know that we need to prove that $\overline{g_{k'} a_{k'}} = \overline{g_k a_k}$, since we know that the image of a_k is $a_{k'}$, then we use the fact that the group action is compatible with the map to conclude the assertion. Then we know that this is also a continuous action. We only need to check the stabilizer, for example of $\overline{a_k}$. We know that if $(g_k)\overline{a_k} = \overline{g_k a_k}$ is equal to $\overline{a_k}$, then we know after passing to some larger j, $a_j = g_j a_j$, therefore we know that g_j is in the stabilizer of a_j. We notice that the stabilizer of $\overline{a_k}$ in this case is just union of the intersection of $\varprojlim_i G_i$ with one of the open of the product of G_i where we have the stabilizer of a_j at the j-th component and all other components are all G_i. Therefore is open, therefore we know that this action is indeed a continuous action.

Then let's first prove this map $\varinjlim_i C^\bullet(G_i, A_i) \to C^\bullet(G, A)$ is injective. I will let you check that it suffices to prove that for $f_1, f_2 : G_i^n \to A_i$, if they are are mapped to the same map $G^n \to A$, then after passing to something larger say $G_j^n \to A_j$, $f_1 = f_2$. Let's denote $f_1', f_2' : G_i^n \to A_i \to A$, the map induced by f_1, f_2. Let:

$$X = \{x \in G_i^n : f_1'(x) = f_2'(x)\}$$

Notice that f_1', f_2' is the composition of $G_i^n \to A_i$ with $A_i \to \varinjlim_i A_j$, which are both continuous, therefore the composition is also continuous. Therefore X will be open in G_i^n. Let

$$\pi_i : G^n = \varprojlim_i G_i^n \to G_i^n$$

be the projection to the i-th component and $\pi_{ji} : G_j^n \to G_i^n$ be the transition map where $j \geqslant i$.

Notice that the image of π_i is the intersection of all images of π_{ji} for $j \geqslant i$. It's clear the image of π is contained in the intersection. Suppose that something is in the intersection, then we need to find something in the inverse limit such that it's mapped to the intersection. We know that for any other index i', we can find some j dominating i, i', then we pick the i' component to be the image of that in the j component, I will let you show that this indeed defines an element in the inverse limit which satisfies our need. Or you can prove this by defining for $x \in \cap_{j\geqslant i} \mathrm{Im}\pi_{ji}$ and each $j_1 \geqslant j_2 \geqslant i$:

$$A_{j_1, j_2} = \{(x_j) \in \prod_i G_j^n : \pi_{j_1 j_2}(x_{j_1}) = x_{j_2}), \pi_{j_2 i}(x_{j_2}) = x\}$$

Notice that each such set is closed since it's the inverse image of the identity element of the continuous map:

$$\prod_i G_i^n \to G_{j_2}^n \times G_i^n, \qquad (x_j) \mapsto (\frac{x_{j_2}}{\pi_{j_1 j_2}(x_{j_1})}, \frac{x}{\pi_{j_2 i}(x_{j_2})})$$

We know that any finitely many such intersection is nonempty, then since the product space is compact, the intersection for all pairs (j_1, j_2) will also be nonempty. Take one element y in in such a intersection, I will let you check it can be extended to an element in the inverse limit, say (x_i) such that $\pi_i(x_i) = x$.

Notice that since we assume that after precomposing $\pi_i : G^n \to G_i^n$, $f_1' = f_2'$, then we know that $\mathrm{Im}\pi_i \subset X$, therefore $\cap_{j \geqslant i} \mathrm{Im}\pi_{ji} \subset X$. Since X is open, we know that $G_i^n - X$ is closed thus compact, and $G_i^n - \mathrm{Im}\pi_{ji}, j \geqslant i$ forms an open covering of $G_i^n - X$. (Here we know that the image of π_{ij} is open since we know that the topology is the discrete topology.) Therefore we know that we can pick finitely many to do the covering, then we find a common upper bound and conclude that $\mathrm{Im}(\pi_{ji}) \subset X$ for a single j. Therefore:

$$f_1' \circ \pi_{ji} = f - 2' \circ \pi_{ji}$$

Notice that A is discrete and G_j^n is compact, therefore the image of $f_1' \circ \pi_{ji} = f - 2' \circ \pi_{ji}$ is finite in A, then by further enlarging j, we can assume that f_1, f_2 induces the same map from G_j^n to A_j, therefore we are done with injectivity.

Then let's show surjectivity. Let $f : G^n \to A$ be a continuous map, we know that G^n is compact and A is discrete, therefore we know that the image is finite, so let's say the image is $\mathrm{Im}f = \{a_1, \cdots, a_k\}$. For each a_λ, $f^{-1}a_\lambda$ is both open and closed in G^n, so we know that each $f^{-1}a_\lambda$ is a finite union of sets of the form:

$$(\prod_i U_i) \cap (\varprojlim_i G_i^m)$$

where U_i is open in G_i^m and $U_i = G_i^m$ for all but finitely many i. (Finite because we know that the inverse limit is also compact, then we know that we can use only finitely many basic opens to cover it.)

Let j be large enough such that for any $i \geqslant j$, U_i in the above product is G_i^m, then for any $x, x' \in G^n$ such that $\pi_j(x) = \pi_j(x')$, we have $f(x) = f(x')$. Notice that x, x' will be mapped to one of the a_λ, but we know that to determine where x, x' lie in which inverse image, we only need to see where $\pi_j(x), \pi_j(x')$ is. Therefore if $\pi_j(x) = \pi_j(x')$, we know that $f(x') = f(x)$. So we know that we can factor f by:

$$G^n \xrightarrow{\pi_j} \pi_j(G^n) \xrightarrow{f'} A$$

for some continuous map f'. This is because we can think of $\pi_j(G^n)$ with the subspace topology as the quotient space of G^n with the kernel of π_j, therefore we know that by the universal property of the quotient space we get such continuous f', which can be checked to be a group homomorphism.

Notice that the space $\pi_j(G^n)$ in G_j^n is again compact, then we know that for each a_λ, the inverse image of a_λ under f' is closed in a compact subset, therefore is again compact, therefore I will let you check why we can find disjoint opens in G_j^n, say V_λ such that $f'^{-1}(a_\lambda) \subset V_\lambda$. Then since we only have finitely many a_λ, by again enlarging j if needed, we can assume that these a_λ are images of $a_{\lambda j} \in A_j$.

Then we define:

$$f_j : G_j^n \to A_j$$

by $f_(V_\lambda) = \{a_{\lambda j}\}$ and those that are not in any V_λ is mapped to 0. We know that this in by definition continuous and clearly it induces f. □

Remark 3.6. Before we go to further discussion, let's make a useful observation here. If we deal with a finite group G with discrete topology, then we know that continuous maps from G^n to A where A is a discrete abelian group is the same as all the maps from G^n to A as both are with discrete topology. similarly, all left actions of G on A will be discrete. Therefore the conventions we make for profinite groups all degenerates to the normal group cohomology conventions.

Corollary 3.7. Let G be a profinite group and A is a G-module, then we have:

$$H^i(G, A) \simeq \varinjlim_U H^i(G/U, A^U)$$

where U goes over the set of open normal subgroups of G. In particular, for all $i \geqslant 1$, $H^i(G, A)$ are torsion groups.

Proof. Since G acts continuously on A, we know that A is the union of A^U where U is an open subgroup of G. Recall that in a profinite group, any open subgroup contains an open normal subgroup, we know that A is also A^U where U runs over all the normal open subgroups of G. Therefore we know that we have a direct set of open normal subgroups ordered by inclusion. We also know that we have a direct system A^U whose direct limit is A. Similarly we have an inverse system G/U, whose inverse limit is G. G/U's are all finite groups, therefore every act is continuous and I will let you show that the action will be compatible with the transition maps.

Then by the above theorem, we have:

$$H^i(G, A) \simeq \varinjlim_U H^i(G/U, A^U)$$

since G/U is a finite group, then we know that for $i \geqslant 1$, every $H^i(G/U, A^U)$ is annihilated by the order of G/U, therefore the direct limit is also torsion. □

Corollary 3.8. For each $i \geqslant 0$, $H^i(G, -)$ define above is the i-th derived functor of the functor $A \to A^G$ on the abelian category of G-modules where G acts continuous.

Proof. Let's first check that $H^0(G, A)$ is A^G. Recall that the complex is the following:

$$0 \to C^0(G, A) \to C^1(G, A) \to C^2(G, A) \to \cdots$$

Then we know that $H^0(G, A)$ is the 0-th cohomology of this complex, i.e. the kernel of $C^0(G, A) \to C^1(G, A)$.

Notice that $C^0(G, A)$ is just A, then we know that the map is defined by:

$$a \mapsto f(g) = ga - a$$

Then we know that the kernel is given by those in A that is invariant under G actions, therefore is A^G.

Then we know that taking cohomology of the complex $C^\bullet(G, A)$ is a δ-functor. Moreover, we know that if I is an injective G-module, we know that I^U is an injective G/U-module for any open normal subgroup of G. To prove this, consider the functor from the category of G/U-modules to the category of G-modules where G acts continuously:

$$A \mapsto A$$

where the action of U is trivial. Then I claim that this action is indeed continuous as if we compute the stabilizer of $a \in A$, we know that if it's stabilizer in G/U is the subgroup H/U, then the stabilizer in G is just H. Since H/U is open in G/U we know that H is the inverse image of H/U under the quotient map $G \to G/U$, thus is still open. Let's call this functor the inflation functor, denoted by Inf. Then notice that we have an adjoint relation:

$$\mathrm{Hom}_G(\mathrm{Inf} A, I) \to \mathrm{Hom}_{G/U}(A, I^U)$$

Clearly if we have a map $f : \mathrm{Inf} A \to I$, then we know that since U acts on $\mathrm{Inf} A$ trivially, then we know that the image of f lies in I^U. Conversely, if we have any $f : A \to I^U$ that is G/U-linear, then clearly that if we compose it with $I^U \hookrightarrow I$, we get a G-map. Clearly these are inverses of each other. I will let you check this is functorial in both slots. But this implies that the functor $I \mapsto I^U$ preserves injective objects.

This implies that

$$H^i(G, I) \simeq \varinjlim_U H^i(G/U, I^U) = 0$$

The fact that this δ functor vanishes for injective modules implies that it's also a universal δ-functor such that on the 0-th degree, it's Γ^G, therefore it's uniquely isomorphic to the derived functor of Γ^G. □

Let $f : G' \to G$ be a continuous homomorphism of profinite groups. Let A be a G-module and A' be a G'-module, both with discrete topology. Let $\phi : A \to A'$ be an additive map that is compatible with the group actions, i.e.

$$\phi(f(g')a) = g'\phi(a)$$

Then we know that ϕ induces an morphism $A^G \to A'^{G'}$, then again the universal property of derived functors gives a canonical extension:

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

This map is induced by the chain map $C^\bullet(G,A) \to C^\bullet(G',A')$ induced by f and ϕ. The definition of the chain map is obvious and let's check it's indeed a chain map. On the one hand, a map $h: G^n \to A$ is mapped to:

$$h'(g'_1,\cdots,g'_{n+1}) = \phi(f(g'_1)h(f(g'_2),\cdots,f(g'_{n+1}))) + \sum_{j=1^n}(-1)^j\phi(h(f(g'_1),\cdots,f(g'_jg'_{j+1}),\cdots,f(g'_{n+1})))$$

$$+(-1)^{n+1}\phi(h(f(g'_1),\cdots,f(g'_n)))$$

I will let you check another way of mapping h gives you the same result.

In particular, let H be a closed subgroup of G and A is a G-module, then we have the restriction homomorphism:

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

Now let H be a closed subgroup of G and let B be an H-module, we denote by $\text{Ind}_H^G B$ the group of continuous maps $\phi: G \to B$, satisfying $\phi(hg) = h\phi(g)$. This is meant to mimic our definition before that $\text{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G],A)$, but here we will want to impose the continuous condition, therefore we will directly say we want continuous maps $\phi: G \to B$ such that $\phi(hg) = h\phi(g)$. Again, we will define a G-action on $\text{Ind}_H^G B$ by:

$$(g\phi)(g') = \phi(g'g)$$

Again this is a functor from the category of H-modules to the category of G-modules which is called the **induction** (no continuous action assumed). This is also a continuous action if we put discrete topology on $\text{Ind}_H^G B$. To prove this it suffice to prove that the stabilizer of ϕ is open in G. It suffices to prove that there is a neighborhood of 1 such that for all g in that neighborhood $g\phi = \phi$.

Recall that since B is discrete, for each $x \in G$, we can consider the inverse image of $\phi(x)$, which is open, therefore there is an open neighborhood of 1, say U_x, such that for all $g \in U_x$ we have $\phi(xg) = \phi(x)$. Then we know that xU_x covers G and G is compact, therefore we can pick finitely many of them, say $U_{x_1},\cdots,U_{x_n}$. Then we know that let U to be the intersection of all these finitely many opens. Then suppose that $g \in U$, then for any $g \in G$, we know that since $x_iU_{x_i}$ covers G, we can write $g = x_iv_i$ for some $v_i \in U_{x_i}$, then we know that:

$$u\phi(g) = \phi(x_iv_iu) = \phi(x_i) = \phi(x_iv_i) = \phi(g)$$

Therefore elements in U fixes ϕ. Then suppose that g also fixes ϕ, then we know that gU fixes ϕ since:

$$(gu)\phi(x) = \phi(xgu) = (u\phi)(xg) = \phi(xg) = g\phi(x) = \phi(x)$$

Therefore the stabilizer is indeed open.

Then let:

$$\theta: \text{Ind}_H^G B \to B, \qquad \theta(\phi) = \phi(1)$$

where B is an H-module and $\text{Ind}_H^G B$ is a G-module. Clearly this is compatible with the group actions, therefore we have the induced maps:

$$H^i(G,\text{Ind}_H^G B) \to H^i(H,B)$$

Again, we have Shapiro's theorem in the context of profinite groups:

Theorem 3.9. (Shapiro) Using the notation from the above discussion, for any H-module B, the map:

$$H^i(G,\text{Ind}_H^G B) \to H^i(H,B)$$

induced by θ is an isomorphism.

Proof. First, we need to prove that this induction functor is the right adjoint of the forgetful functor, i.e. we need to prove the following functorial isomorphism:

$$\mathrm{Hom}_H(A, B) \to \mathrm{Hom}_G(A, \mathrm{Ind}_H^G B)$$

Here again by H-modules A and B, we mean that H acts continuously on A, B. Recall that the proof is no different from the fact that now in the induction we only think about continuous group maps since if you look back to the proof of the adjointness there we know that a map $f : A \to B$ is mapped to the map that maps a to φ_a and $\varphi_a(g) = f(ga)$, then this map is the composition:

$$G \xrightarrow{\cdot a} A \xrightarrow{f} B$$

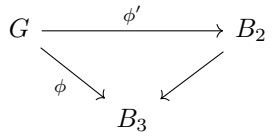
Notice that since G acts continuous on A, then the first map is continuous and f is also continuous since A, B are discrete. Therefore this φ_a is indeed a continuous map from G to B. Clearly, the inverse is given by any map F from A to $\mathrm{Ind}_H^G B$ is mapped to f where $f(a) = F(a)(1)$. The fact that these are inverses doesn't change as we know that the hom sets in this new subcategory is the same as the hom sets in the larger category since the smaller category is full.

We also know that this induction functor is exact. Recall that this functor is clearly left exact. Suppose that we have a SES of H-modules:

$$0 \to B_1 \to B_2 \to B_3 \to 0$$

If we have a continuous map $\phi : G \to B_3$ such that $\phi(hg) = h\phi(g)$ for all $h \in H, g \in G$, I want to show that it factors through B_2. Notice that the value of ϕ is determined by it's value on any representative of the cosets G/H. Say we choose a representative set S.

Then we define $\phi' : G \to B_2$ by $\phi'(s)$ is any lift of $\phi(s)$ in B_3 to B_2. Notice that the extends to a map from G to B_2. Moreover we automatically have the factorization:



Notice that ϕ is continuous and $B_2 \to B_3$ is continuous and is surjective and is a quotient map. Then automatically ϕ' is continuous. By our definition we have $\phi'(hg) = h\phi'(g)$. Therefore Ind_H^G is indeed exact. Then using the same argument as in the general theory for group cohomology, we are done. □

Let H be the trivial subgroup, i.e. $\{H\} = 1$, any abelian group M is an H-module. We can form the G-module $\mathrm{Ind}_{\{1\}}^G M$, which is continuous maps from G to M. A G-module is called **induced** if it's isomorphic to $\mathrm{Ind}_{\{1\}}^G M$ for an abelian group M. A G-module is called **weakly injective** if it's a direct factor of an induced G-module. Notice that for an induced G-module, by the above theorem, the cohomology vanishes for all $i \geqslant 1$. This is because we know that in this case $\Gamma^{\{1\}}$ is the identity functor, which has trivial higher cohomology. Then we know that a weakly injective G-module also has trivial higher cohomology.

Again, we know that any G-module A can be embedded in an induced G-module which is:

$$A \mapsto \mathrm{Ind}_{\{1\}}^G A, \qquad a \mapsto (g \mapsto ga)$$

This is clearly injective. Then if A itself is injective, we know that it's automatically a direct sum of an induced G-module, therefore any injective G-module is again weakly injective. Again, we can use resolutions of weakly injective G-modules to compute $H^i(G, A)$.

Similar to the usual group cohomology, we have the Hochschild-Serre-Spectral sequence. **** to be completed later*

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

Now if H is an open subgroup of G, we know that H has finite index in G, therefore we can also define the corestriction map for any G-module A:

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

Again, this is induced by:

$$\pi : \mathrm{Ind}_H^G A \to A$$

where $f \mapsto \sum_{gH \in G/H} gf(g^{-1})$, again you check that this is compatible with group actions of $H \hookrightarrow G$. We call the morphism it induces on the cohomology the corestriction. By the same argument as in general group cohomology theory, we have:

Proposition 3.10. Suppose that H is a closed subgroup of G which has finite index n, then we have $\mathrm{Cor} \circ \mathrm{Res} = n$.

Proof. Notice that a closed subgroup with finite index is open. Then we notice:

$$A \xrightarrow{\iota} \mathrm{Ind}_H^G A \to A$$

is just multiply by n. □

Proposition 3.11. Let H be a closed subgroup of a profinite group G such that $[G : H]$ is prime to a prime number p, then for any G-module A and any i, the restriction map:

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

is injective on the p-primary part.

Proof. First, if $[G : H] < \infty$, then we know H is actually open and from the previous proposition that if x is a nonzero element annihilated by a power of p, we know that it's not annihilated by n as n is prime to p, therefore annihilated by n and a power of p implies that $1x = 0$, that is $x = 0$. But this implies that the image of x in $H^i(H, A)$ is not 0, otherwise the image $\mathrm{Cor} \circ \mathrm{Res}(x) = nx = 0$, a contradiction, therefore we know that the those annihilated by a power of p is only mapped to 0 by Res if it's 0.

Then assume that $[G : H]$ is a infinite surnatural number. First, notice that H is the intersection of all open subgroups containing H. To see why, notice that if g is not in H, we know that we can find an open neighborhood of g and an open neighborhood of H such that they are disjoint. Notice that since U contains H, we know that U^{-1} contains H, then by using $U \cap U^{-1}$, we can assume that the open neighborhood of H is an open subgroup, therefore we are done. Then in particular, we know that:

$$H = \varprojlim_U U$$

where U are open subgroups of G containing H. Then we know that the cohomology of H is the direct limit of the cohomology of U, i.e.:

$$H^i(H, G) \simeq \varinjlim_U H^i(U, G)$$

Now for each of these U, we know that G/U is finite, and we know that since $[G : U]$ divides $[G : H]$ then it's also prime to p, then we know that the restriction:

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

is injective on the p-primary parts. Notice that if $U' \supset U$, we have the following diagram:

$$\begin{array}{ccc} H^i(G, A) & \longrightarrow & H^i(U', A) \\ & \searrow \quad \swarrow & \\ & H^i(U, A) & \end{array}$$

Therefore we get a morphism $H^i(G, A)$ to the direct limit $\varinjlim_U H^i(U, A)$ that is independent of how we choose $H^i(G, A) \to H^i(U, A)$.

Then I will let you show that this is compatible with $H^i(G,A) \to H^i(H,A)$ and therefore we know that we have a morphism:

$$\begin{array}{ccc} H^i(G,A) & \xrightarrow{\quad\text{Res}\quad} & H^i(H,G) \\ & \searrow^{\text{Res}} \quad \nearrow_{\simeq} & \\ & \varinjlim_U H^i(U,A) & \end{array}$$

Then we know that if x is in the p-primary part of $H^i(G,A)$ then only 0 is mapped to 0 in the direct limit, therefore the same happens for the top map as well. □

Then let's compute some concrete examples of cohomologies of profinite groups. The first example if to consider the following abelian group, which is called **profinite completion** of $\mathbb{Z}$:

$$\hat{\mathbb{Z}} = \varprojlim_{n \geqslant 1} \mathbb{Z}/n$$

Here the index is given by $n \leqslant m$ iff $n|m$ and the transition map between $\mathbb{Z}/m \to \mathbb{Z}/n$ is just the usual map. Before we study it's group cohomology, we make the following observation: recall that we have the p-adic integers $\mathbb{Z}_p$ for each prime number p, which is the inverse limit of $\mathbb{Z}/p^n$. I claim that we have the following isomorphosm of topological rings:

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

To see what is this isomorphism, we first notice that for each n, we have it's prime factorization:

$$n = \prod_p p^{n_p}$$

Then we know that by the Chinese Remainder Theorem, we have an isomorphism:

$$\mathbb{Z}/n \simeq \prod_p \mathbb{Z}/p^{n_p}$$

We know that if $n|m$, we can also write:

$$\mathbb{Z}/m \simeq \prod_p \mathbb{Z}/p^{m_p}$$

where we know that for each p, m_p is at least as large as n_p. We also have the following diagram:

$$\begin{array}{ccc} \mathbb{Z}/m & \longrightarrow & \mathbb{Z}/n \\ \downarrow^{\simeq} & & \downarrow^{\simeq} \\ \prod_{p|m} \mathbb{Z}/p^{m_p} & \longrightarrow & \prod_{p|n} \mathbb{Z}/p^{n_p} \end{array}$$

where the map between the two product is defined by if p is present in both product, then we define it by the usual map $\mathbb{Z}/p^{m_p} \to \mathbb{Z}/p^{n_p}$. If p is present in the first product but not the second one, we define it to be projected all to 0. Then clearly this diagram commutes. Therefore we know that the former inverse limit of $\varprojlim_n \mathbb{Z}/n$ can be now written as:

$$\varprojlim_n \prod_{p|n} \mathbb{Z}/p^{n_p}$$

Then notice that we have a morphism:

$$\prod_p \mathbb{Z}_p \to \varprojlim_n \prod_{p|n} \mathbb{Z}/p^{n_p}$$

where (x_p) is mapped to each $\prod_{p|n} \mathbb{Z}/p^{n_p}$ by:

$$\prod_p \mathbb{Z}_p \to \prod_{p|n} \mathbb{Z}_p \to \prod_{p|n} \mathbb{Z}/p^{n_p}$$

Then I will let you check that by the universal property of inverse limit, this gives you a map $\prod_p \mathbb{Z}_p \to \varprojlim_n \prod_{p|n} \mathbb{Z}/p^{n_p}$. Conversely, we define a morphism from $\varprojlim_n \prod_{p|n} \mathbb{Z}/p^{n_p}$ to $\prod_p \mathbb{Z}_p$ by first defining $\varprojlim_n \prod_{p|n} \mathbb{Z}/p^{n_p} \to \mathbb{Z}_p$ by:

$$\varprojlim_n \prod_{p|n} \mathbb{Z}/p^{n_p} \to \prod_n \prod_{p|n} \mathbb{Z}/p^{n_p} = \prod_p \prod_n \mathbb{Z}/p^n \to \mathbb{Z}/p'^{n'}$$

Then you check that this is compatible with the inverse limit structure in $\mathbb{Z}_p$, thus indeed gives a morphism to $\mathbb{Z}_p$. Then you check these two are inverses of each other. This isomorphism is an isomorphism of rings and since everything is defined by universal property (including universal property in topological spaces, this is also an isomorphism of topological rings).

Definition 3.12. If G is a topological group, we say that a subset $S \subset G$ is a set of **topological generators of** G if the subgroup generated by S is dense in G.

One observation is that in the profinite completion of $\mathbb{Z}$, the element $(\overline{1})$ is a topological generator of $\hat{\mathbb{Z}}$. To see why, we notice that it generates $\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}}$. This is because we have a canonical map $\mathbb{Z} \to \hat{\mathbb{Z}}$, then this is injective since if n is mapped to 0, then it's 0 in every $\mathbb{Z}/m$, therefore $n = 0$. Therefore we need to show $\mathbb{Z}$ is dense. We only need to show that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ as we know that the profinite completion is just a product of $\mathbb{Z}_p$, and the any open in the product contains a fundamental open. To show $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, suppose that we have a p-adic integer $\sum_{n \geqslant 0} a_n p^n$ where each a_n is $0 \leqslant a_n < p$, then we know that any open neighborhood of this number will contain a fundamental open, which means that we only need to consider finitely many $\mathbb{Z}/p^n$, say the largest n we need to think about in N, then we know that we know that the number:

$$\sum_{n \geqslant 0}^{N-1} a_n p^n \in \mathbb{Z}$$

is in the open neighborhood.

Proposition 3.13. Let $\hat{\mathbb{Z}}$ be the profinite completion of $\mathbb{Z}$ as in the above discussion, then for any torsion abelian group A with a continuous $\hat{\mathbb{Z}}$ action, we have:

$$H^i(\hat{\mathbb{Z}}, A) = \begin{cases} A^{\hat{\mathbb{Z}}} & \text{if } i = 0, \\ A_{\hat{\mathbb{Z}}} & \text{if } i = 1, \\ 0 & \text{if } i \geqslant 2. \end{cases}$$

Proof. The full computation of this result is going to be a bit complicated.

Let $T = (\overline{1}) \in \hat{\mathbb{Z}}$ be the canonical topological generator of the profinite completion, then for any $n \in \mathbb{N}$, let:

$$A^{T^n} = \{a \in A : T^n(a) = a\}$$

Notice that this is the invariant part of A under T^n where we use T and T^n to denote the automorphism induced by T and T^n(you should check that the restriction of T to A^{T^n} indeed maps A^{T^n} to itself). Notice that since T is the topological generator, I claim that the union of A^{T^n} for all $n \in \mathbb{N}$ is the whole abelian group A. Let $a \in A$, we consider it's stabilizer, which is open $\hat{\mathbb{Z}}$ by our assumption that $\hat{\mathbb{Z}}$ acts continuous on A. Then it contains some T^n where n is an integer, but we know that we can assume that n is nonnegative since if it's negative, we know that T^{-n} is the inverse of T^n and since $T^n(a) = a$, then we know that $T^{-n}a = T^{-n}T^n(a) = a$.

Then we conclude that $A = \cup_{n \geqslant 0} A^{T^n}$. Notice that $\mathbb{Z}/n$ acts on A^{T^n} continuously by letting 1 to act like T. Then the induced action on the inverse limit of $\mathbb{Z}/n$, i.e. on the profinite completion will still be the same action as we started with. To see this, if we have a continuous maps:

$$f, g : G \to A$$

where A is with the discrete topology and f, g agrees on a dense subgroup of G, then f, g agrees on all of G. To see why, say f, g differs on x, then we know that $f(x) \neq g(x)$, which is open in A. Consider the inverse image of x under f, g, which are open and contains x, then consider the intersection, which is again open and contains x. But we know that this open intersects with the dense subgroup, which is a contradiction.

Therefore:

$$H^i(\hat{\mathbb{Z}}, A) \simeq \varinjlim_n H^i(\mathbb{Z}/n, A^{T^n})$$

Here the transition maps in $H^i(\mathbb{Z}/n, A^{T^n})$ are determined by the complex maps for $m, n \in \mathbb{Z}$:

$$C^\bullet(\mathbb{Z}/n, A^{T^n}) \to C^\bullet(\mathbb{Z}/mn, A^{T^{mn}})$$

or more specifically determined by the following diagram:

$$\begin{array}{ccc} (\mathbb{Z}/n)^k & \longrightarrow & A^{T^n} \\ \uparrow & & \downarrow \\ (\mathbb{Z}/mn)^k & \dashrightarrow & A^{T^{mn}} \end{array}$$

Now for each n, m, we have the following diagram:

$$\begin{array}{ccccccccccccc} 0 & \longrightarrow & A^{T^n} & \xrightarrow{T-1} & A^{T^n} & \xrightarrow{T^{n-1}+\cdots+T+1} & A^{T^n} & \xrightarrow{T-1} & A^{T^n} & \xrightarrow{T^{n-1}+\cdots+T+1} & A^{T^n} & \xrightarrow{T-1} & A^{T^n} & \xrightarrow{T^{n-1}+\cdots+T+1} & A^{T^n} & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle m^2} & & \downarrow{\scriptstyle m^2} & & \downarrow{\scriptstyle m^3} & & \\ 0 & \longrightarrow & A^{T^{mn}} & \xrightarrow{T-1} & A^{T^{mn}} & \xrightarrow[T^{mn-1}+\cdots+T+1]{} & A^{T^{mn}} & \xrightarrow{T-1} & A^{T^{mn}} & \xrightarrow[T^{mn-1}+\cdots+T+1]{} & A^{T^{mn}} & \xrightarrow{T-1} & A^{T^{mn}} & \xrightarrow[T^{mn-1}+\cdots+T+1]{} & A^{T^{mn}} & \longrightarrow & \cdots \end{array}$$

Notice that the horizontal row on top is obtained by apply the functor $\mathrm{Hom}_{\mathbb{Z}[G]}(-, A^{T^n})$ (where G here is $\mathbb{Z}/n$) to the free free resolution of $\mathbb{Z}$ we obtained in the general theory of group cohomology. Then we know that the cohomology $H^i(\mathbb{Z}/n, A^{T^n})$ is just the cohomology of this complex. Similar situation happens for the horizontal row at the bottom. The vertical maps are multiplications by $1, m, m^2$ and etc. I claim that this gives a chain map. Notice that A^{T^n} is a subgroup of $A^{T^{mn}}$ therefore the multiplication makes sense. Those squares with the same multiplication obviously commute, therefore we only need to consider the squares with multiplication of m^i and m^{i+1}.

Let $x \in A^{T^n}$, then it's first mapped to $m^i x$ in $A^{T^{mn}}$, then we have:

$$m^i(T^{mn-1}(x) + \cdots + T(x) + x)$$

Notice that $T^n x = x$, then we know that $T^{mn-1}(x) + \cdots + T(x) + x$ is just $m(T^{n-1}(x) + \cdots + T(x) + x)$, therefore it's easy to see that the square still commutes. Notice that the induced map on cohomology, for example on the 0-th cohomology is just:

$$\mathrm{Ker}(T-1|_{A^{T^n}}) \hookrightarrow \mathrm{Ker}(T-1|_{A^{T^{mn}}})$$

That is $(A^{T^n})^{\mathbb{Z}/n} \hookrightarrow (A^{T^{mn}})^{\mathbb{Z}/mn}$. Notice that in the map induced using $C^\bullet(\mathbb{Z}/n, A^{T^n}) \to C^\bullet(\mathbb{Z}/mn, A^{T^{mn}})$ on the 0-th cohomology is also $(A^{T^n})^{\mathbb{Z}/n} \hookrightarrow (A^{T^{mn}})^{\mathbb{Z}/mn}$, then we know that the uniqueness of the extension of derived funcotrs to another δ-functor implies that the transition maps we obtained using $C^\bullet$ or the above computation are the same, therefore we know that:

$$H^0(\hat{\mathbb{Z}}, A) \simeq \varinjlim_n (A^{T^n})^{\mathbb{Z}/n} = A^{\hat{\mathbb{Z}}}$$

I will let you check the this direct limit is indeed the $\hat{\mathbb{Z}}$-invariant part. This computation agrees with our definition that the 0-th derived functor should be the functor itself, which is not a surprise.

To compute $H^1(\hat{\mathbb{Z}}, A)$, let:

$$A' = \{a \in A : T^n(a) = a, \quad (T^{n-1} + \cdots + T + 1)(x) = 0, \text{ for some } n \in N\}$$

Again, we have the direct limit description of the cohomology:

$$H^1(\hat{\mathbb{Z}}, A) = \varinjlim_n H^1(\mathbb{Z}/n, A^{T^n})$$

We know from the description of the group cohomology of $\mathbb{Z}/n$ that:

$$H^1(\mathbb{Z}/n, A^{T^n}) = \mathrm{Ker}(T^{n-1} + \cdots + T + 1|_{A^{T^n}})/\mathrm{Im}(T - 1|_{A^{T^n}})$$

Recall that the direct limit is exact, therefore we have:

$$\varinjlim_n H^1(\mathbb{Z}/n, A^{T^n}) = (\varinjlim_n \mathrm{Ker}(T^{n-1} + \cdots + T + 1|_{A^{T^n}}))/(\varinjlim_n \mathrm{Im}(T - 1|_{A^{T^n}}))$$

Notice that the inverse limit of the kernel is A' and the inverse limit of the image is $(T-1)(A) \subset A$.

Therefore we know that:

$$H^1(\hat{\mathbb{Z}}, A) = A'/(T-1)(A)$$

Notice that since A is torsion, then for any $a \in A$, there are $m, n \in \mathbb{N}$ such that $mx = 0$ and $x \in A^{T^n}$, therefore we know that:

$$(T^{mn-1} + \cdots + T + 1)(x) = m(T^{n-1} + \cdots + T + 1)(x) = 0$$

Therefore $A = A'$, therefore we know that the cohomology is just:

$$A/(T-1)A$$

Recall that the definition of the coinvariant is A mod the subgroup generated by $ga - a$. Since T is the topological generator and A is discrete, consider the continuous map:

$$\hat{\mathbb{Z}} \to A, \qquad g \mapsto gx$$

Then we consider the inverse image of gx, then using the fact that A is discrete and $\mathbb{Z}$ is dense, we know that there is T^n such that $T^n x = gx$, we know that:

$$gx - x = T^n x - x$$

Notice that $T^n x - x = (T-1)(x + Tx + \cdots + T^{n-1}x)$. Therefore we know that the subgroup generated by $gx - x$ is the image $(T-1)A$, therefore:

$$H^1(\hat{\mathbb{Z}}, A) = A_{\hat{\mathbb{Z}}}$$

Finally for higher cohomology, since every $x \in A$ is torsion, which means that $mx = 0$ for some $m \in \mathbb{N}$, then if $x \in A^{T^n}$, consider:

$$H^i(\mathbb{Z}/n, A^{T^n}) \to H^i(\mathbb{Z}/mn, A^{T^{mn}})$$

where the class of x is mapped to $m^j x$ for some $j \geqslant 1$, therefore we know that it's mapped to 0. In other words, every element in $H^i(\mathbb{Z}/n, A^{T^n})$ will eventually be mapped to 0, therefore the direct limit is 0. □

Besides this profinite completion of $\mathbb{Z}$, we have another kind of completion. Notice that if we fix a prime number p, then the subgroups $n\mathbb{Z}$ of $\mathbb{Z}$ where n is prime to p can be used to define a basis for the point $0 \in \mathbb{Z}$, then the completion of $\mathbb{Z}$ with respect to this topology is often called the **prime to p completion** of $\mathbb{Z}$. This is usually denoted by:

$$\hat{\mathbb{Z}}^{(p)} = \varprojlim_{(n,p)=1} \mathbb{Z}/n$$

Again the index is given by $m \geqslant n$ iff $n|m$ and the transition map $\mathbb{Z}/m \to \mathbb{Z}/n$ is the usual map. Using similar arguments as of how to prove $\hat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p$, here we can show there is an isomorphism of topological rings:

$$\hat{\mathbb{Z}}^{(p)} \simeq \prod_{q \neq p} \mathbb{Z}_q$$

Notice that if q is a power of p, then multiplication by q induces a continuous isomorphism of groups:

$$q : \hat{\mathbb{Z}}^{(p)} \to \hat{\mathbb{Z}}^{(p)}$$

Notice that to prove this is an isomorphism, we only need to show that q is invertible in $\hat{\mathbb{Z}}^{(p)}$. Notice that since q is a power of p, we know that if we consider the map $\mathbb{Z} \to \hat{\mathbb{Z}}^{(p)}$, we know that the image of q in each component is invertible (this is similar to how to prove $\mathbb{F}_p$ is indeed a field), therefore the image in $\hat{\mathbb{Z}}^{(p)}$ is also invertible. This is also continuous since we know that both of the two groups are actually topological rings, therefore multiplication is going to be continuous.

Proposition 3.14. Let A be a $\hat{\mathbb{Z}}^{(p)}$-module and suppose that every element of A is annihilated by some elements relatively prime to p. Then we have:

$$H^i(\hat{\mathbb{Z}}^{(p)}, A) = \begin{cases} A^{\hat{\mathbb{Z}}^{(p)}} & \text{if } i = 0, \\ A_{\hat{\mathbb{Z}}^{(p)}} & \text{if } i = 1, \\ 0 & \text{if } i \geqslant 2. \end{cases}$$

Moreover, let $\phi : A \to A$ be a homomorphism compatible with a homomorphism of groups $q : \hat{\mathbb{Z}}^{(p)} \to \hat{\mathbb{Z}}^{(p)}$, i.e.:

$$\phi((qg)x) = g\phi(x)$$

Then q, ϕ induces morphisms on $H^0(\hat{\mathbb{Z}}^{(p)}, A)$ and $H^1(\hat{\mathbb{Z}}^{(p)})$ by:

$$\phi : A^{\hat{\mathbb{Z}}^{(p)}} \to A^{\hat{\mathbb{Z}}^{(p)}}$$

$$q\phi : A_{\hat{\mathbb{Z}}^{(p)}} \to A_{\hat{\mathbb{Z}}^{(p)}}$$

where $q\phi(\overline{x}) = q\overline{\phi(x)}$.

Proof. The assertion about the cohomology is basically proved the same way as the cohomology for $\hat{\mathbb{Z}}$, so we omit it here.

Recall that ϕ induces a map:

$$\phi : A^{\hat{\mathbb{Z}}^{(p)}} \to A^{\hat{\mathbb{Z}}^{(p)}}$$

Then we know that by the universal property of derived functors, it gives maps $H^i(\hat{\mathbb{Z}}^{(p)}, A) \to H^i(\hat{\mathbb{Z}}^{(p)}, A)$. Obviously on degree 0, it's just ϕ and for degree $i \geqslant 0$, since everything is 0, the induced map is 0. Therefore we only have to look at degree 1.

Let's first compute the degree 1 cohomology using the definition in the start of this section, i.e. using the complex $C^\bullet(\hat{\mathbb{Z}}^{(p)}, A)$. Notice that by this definition, a 1 co-cycle is the kernel of d_1, that is a continuous map:

$$f : \hat{\mathbb{Z}}^{(p)} \to A, \quad \text{such that } f(g_1 + g_2) = g_1 f(g_2) + f(g_1)$$

Similar to the profinite completion, we know that in $\hat{\mathbb{Z}}^{(p)}$, the element $T = (\overline{1}) \in \hat{\mathbb{Z}}^{(p)}$ is a topological generator of $\hat{\mathbb{Z}}^{(p)}$. Then recall that we proved before a continuous map $\hat{\mathbb{Z}}^{(p)} \to A$ is completely determined by it values on T^n. However, if f is such a map, then we know that $f(T+T) = Tf(T) + f(T)$, therefore we know that the map f is completely determined by it's value $f(T) \in A$.

Conversely, let $a \in A$, we define $f : \mathbb{Z} \to A$ by $f(0) = 0$, $f(1) = a$, $f(n) = T^{n-1}f(1) + f(n-1)$ and $f(-n) = -T^{-n}f(n)$. This implies that for all $g_1, g_2 \in \mathbb{Z}$, we have $f(g_1 + g_2) = g_1 f(g_2) + f(g_1)$. This is indeed continuous, since recall that a is again in A^{T^n} for some n relatively prime to p (if m is not relatively prime to p, say it has a factor of p^k, recall that p_k is invertible in $\hat{\mathbb{Z}}^{(p)}$ with inverse q, then we can take T^{nq}, which is equal to $T^{n'}$ where n' is prime to p), and since we assume that every element in A is annihilated by some m which is prime to p, we then have:

$$(T^{mn-1} + \cdots + T + 1)(a) = m(T^{n-1} + \cdots + T + 1)(a) = 0$$

Then if you expand $f(mn)$ using our inductive definition of f, we find $f(mn) = 0$. Then if $\delta \in mn\mathbb{Z}$, then $f(\delta) = 0$. Moreover, we have:

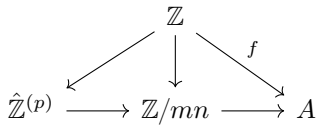
$$f(g + \delta) = gf(\delta) + f(g) = f(g)$$

Therefore we know that the inverse image of any thing in A under f is open, therefore f is continuous.

Then we note that f can be extended to a continuous map $f : \hat{\mathbb{Z}}^{(p)} \to A$. To see why, recall that we know f factors though $\mathbb{Z}/mn$ since we know that f vanishes on all $mn\mathbb{Z}$, then we define the map $f : \hat{\mathbb{Z}}^{(p)} \to A$ by:

$$\hat{\mathbb{Z}}^{(p)} \to \mathbb{Z}/mn \to A$$

The projection is continuous therefore the composition is continuous and clearly we have a commutative diagram:



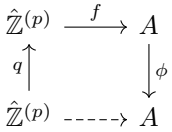
therefore the definition indeed extends $\mathbb{Z} \to A$. You can check that these two constructions are inverses of each other, therefore the 1-cocycle is identified with A.

Under this identification, you can check that the group of 1-coboundary is identified with those $f : \hat{\mathbb{Z}}^{(p)} \to \mathbb{Z}$ such that $f(g) = ga - a$ for a fixed $a \in A$ and all $g \in \hat{\mathbb{Z}}^{(p)}$. But notice that if f is in the coboundary, it's in the cocycle, therefore f is determined by $f(T)$, then f need to satisfy $Ta - a = f(T)$, therefore we know that the degree 1 cohomology is:

$$H^1(\hat{\mathbb{Z}}^{(p)}, A) \simeq A/(T-1)A$$

Again, you can prove $(T-1)A$ is the subgroup generated by $ga - a$, therefore the quotient is $A_{\hat{\mathbb{Z}}^{(p)}}$.

Let's figure out what is the map induced by ϕ in this identification. Notice that we have the following diagram:



We know that in this case f is mapped to $\phi \circ f \circ q$, therefore T is mapped to qT and mapped to $f(qT) = T^{q-1}f(T) + T^{q-1}f(T) + \cdots + f(T)$, then to $\phi(T^{q-1}f(T) + T^{q-1}f(T) + \cdots + f(T))$. Let $f(T) = a$, then the image is $\phi(T^{q-1}a + T^{q-2}a + \cdots + Ta + a)$, but we notice that:

$$\phi(T^{q-1}a + T^{q-2}a + \cdots + Ta + a) = q\phi(a) + \phi(\sum_{i=0}^{q-1}(T^i(a) - a))$$

Recall that ϕ induces a morphism of degree 1 cohomology implies that the image of the subgroup $(T-1)A$ under ϕ is invariant, therefore we know that $\phi(\sum_{i=0}^{q-1}(T^i(a) - a))$ is still in $(T-1)A$, therefore the class in the quotient is the same as that of $q\phi(a)$, therefore the map induced is $q\phi$. □

Let's compute one more example before moving forward. Recall that if k is a separably closed field, say of characteristic p. This p has to be a positive prime number since we know that if the characteristic is 0, then every algebraic extension is separable. Then if n is a positive integer that is prime to p, then we consider the following set:

$$\boldsymbol{\mu}_n(k) = \{x \in k : x^n = 1\}$$

which is the set of all n-th root of unity. Since k is separably closed, we know that since 1 is a root of $x^n - 1$, then this splits in k, which means that every root of $x^n - 1$ is in k. Notice that the derivative of $x^n - 1 = nx^{n-1}$ and the only root of this is 0, which is not a root of $x^n - 1$. Therefore we know that $x^n - 1$ has n distinct roots in k, and $\boldsymbol{\mu}_n(k)$ has exactly n elements. Notice that this is a finite abelian group, moreover we know that for each $d|n$, there are most d-elements $x \in \boldsymbol{\mu}_n(k)$ such that $x^d = 1$, therefore $\boldsymbol{\mu}_n(k)$

is cyclic, therefore we can pick one generator, denoted by ζ_n, which is called the primitive n-th root of unity. Via this primitive root, we have an isomorphism of groups:

$$\mathbb{Z}/n \to \boldsymbol{\mu}_n(k), \qquad 1 \mapsto \zeta_n$$

Now suppose that m is another positive integer prime to p such that $m|n$, then we know that we can also consider $\boldsymbol{\mu}_m(k) \subset \boldsymbol{\mu}_n(k)$. Consider the following map:

$$\boldsymbol{\mu}_n(k) \to \boldsymbol{\mu}_m(k) \qquad x \mapsto x^{n/m}$$

Notice that this map is surjective since each we know that if we pick an n-th root of unity ζ_n in $\boldsymbol{\mu}_n(k)$, then the order of $\zeta_n^{n/m}$ is now m, therefore we know that it's now a primitive m-th root of unity. Conversely, suppose that ζ_m is a primitive m-th root of unity. We need to show that it's the image of x, which means that $x^{n/m} = \zeta_m$ and x is a primitive n-th root of unity. Notice that if $n/m = r$, which is also prime to p, then consider:

$$x^r - \zeta_m = 0$$

Notice that $x \mapsto x^r$ is surjective, therefore there is such a x, then we only need to show that we can pick an x such that the order of x is n.

Suppose that we have a surjective group homomorphism φ from cyclic group A to cyclic group B, then I claim that the preimage of each generator in B contains a generator of A. Notice that if b is a generator, we know that we can assume that $b = \varphi(x)^u$ while the order of $\varphi(x)$ is m. Then we know that $\gcd(u, m) = 1$. Then we want to find $a = x^t$ a generator of A such that:

$$\varphi(x)^t = \varphi(x)^u$$

This implies that $t = u \bmod m$. Notice that since a is a generator of A, $\gcd(t, n) = 1$. Suppose that $t = u + rm$ we want to find a suitable r such that $\gcd(t, n) = 1$ while $\gcd(u, m) = 1$. Notice that for each prime $p|m$, we know that since t divide tm but not u, we know that p doesn't divide t. Then for any $p|n$ but not divide m, then we know that m is going to be invertible mod p. Then we have r such that:

$$u + rm \neq 0, \mod p$$

We can do this for all $p_1, \cdots, p_r$ which are distinct primes those divide n but not m, then we know that if we consider:

$$\mathbb{Z}/(p_1 \cdots p_r) \simeq \mathbb{Z}/(p_1) \times \cdots \times \mathbb{Z}/p_r$$

There will be an r in $\mathbb{Z}$ such that $u + rm \neq 0 \bmod p_i$ for all p_i. Then we know that $u + rm$ is not divisible by all prime factors that divide n but not m and it's not divisible by m, therefore it's not divisible by n, therefore we have found such an r and we let $t = u + rm$, which the desired object.

Clearly we know that this roots of unity form an inverse system and we can consider the inverse limit:

$$\varprojlim_n \boldsymbol{\mu}_n(k)$$

I claim that there is an element in this inverse limit (ζ_n) such that each ζ_n is an n-th root of unity. To see why, consider the following procedure. Let the characteristic of the field be p, then we have a sequence:

$$1|2!|\cdots|(p-1)!|(p-1)!(p+1)|\cdots$$

Then for each number in this field, we can consider the following sequence:

$$\boldsymbol{\mu}_1(k) \leftarrow \boldsymbol{\mu}_{2!}(k) \leftarrow \cdots \leftarrow \boldsymbol{\mu}_{(p-1)!}(k) \leftarrow \boldsymbol{\mu}_{(p-1)!(p+1)}(k) \leftarrow \cdots$$

Notice that by the above discussion, we can choose a compatible sequence of primitive roots of unity. Then for each integer n not divisible by p, we know that there is one number N in the above sequence such

that n divides that, then we know that we can pick the primitive in $\boldsymbol{\mu}_n(k)$ by the map $\boldsymbol{\mu}_N(k) \to \boldsymbol{\mu}_n(k)$. Then we only need to check this is indeed a compatible sequence which is omitted.

Then notice that once we choose ζ_n, ζ_m in $\boldsymbol{\mu}_n(k), \boldsymbol{\mu}_m(k)$, then the map:

$$\boldsymbol{\mu}_n(k) \to \boldsymbol{\mu}_m(k)$$

is identified with the map:

$$\mathbb{Z}/n \to \mathbb{Z}/m$$

Then we know that the inverse limit is identified with $\hat{\mathbb{Z}}^{(p)}$ as an abstract topological group. But notice that this identification depends on the choice of the compatible sequence (ζ_n), therefore is not canonical. Notice that if we consider a number q, which is a power of p, then we have an isomorphism of groups:

$$q : \varprojlim_{(n,p)=1} \boldsymbol{\mu}_n(k) \to \varprojlim_{(n,p)=1} \boldsymbol{\mu}_n(k), \qquad x \mapsto x^q$$

That is raising every element to the q-th power. This is indeed an isomorphism since you can identify this with multiplication by q in $\hat{\mathbb{Z}}^{(p)} \to \hat{\mathbb{Z}}^{(p)}$.

Proposition 3.15. Let k be a separably closed field of characteristic p, then using the above notation, we let:

$$G = \varprojlim_{(n,p)=1} \boldsymbol{\mu}_n(k)$$

Let A be an abelian group such that every element of A is annihilated by some integer relatively prime to p, then we have:

$$H^i(G, A) \cong \begin{cases} A^G & \text{if } i = 0, \\ \mathrm{Hom}\Big(\varprojlim_{(n,p)=1} \mu_n,\ A_G\Big) & \text{if } i = 1, \\ 0 & \text{if } i \geqslant 2. \end{cases}$$

Let q be the isomorphism $q : G \to G$ we talked about above and let $\phi : A \to A$ be an additive map that is compatible with q, i.e.:

$$\phi((qg)x) = g\phi(x)$$

for all $g \in G$ and $x \in A$, then ϕ induces an map:

$$\phi : A^G \to A^G$$

which induces a map on H^1:

$$\mathrm{Hom}(\varprojlim_{(n,p)} \boldsymbol{\mu}_n(k), A_G) \to$$

by map any $\psi \in \mathrm{Hom}(\varprojlim_{(n,p)} \boldsymbol{\mu}_n(k), A_G)$ to $\phi \circ \psi \circ q$

Proof. By our discussion above, after we choose such $\zeta = (\zeta_n)$, we have an isomorphism of topological groups:

$$G \to \varprojlim_{(n,p)=1} \mathbb{Z}/n$$

where $\zeta = (\zeta_n)$ is mapped to $(\overline{1})$, a topological generator.

Then by the above theorem we have:

$$H^i(G, A) \simeq \begin{cases} A^G & \text{if } i = 0, \\ A_G & \text{if } i = 1, \\ 0 & \text{if } i \geqslant 2. \end{cases}$$

Recall that the 1-th cohomology being isomorphic to A_G is given by the map:

$$(G \to A) \to A : f \mapsto f(\zeta)$$

But this isomorphism will depend on the choice of ζ, so we want to make it canonical. Consider the following map:

$$H^1(G,A)\otimes_{\hat{\mathbb{Z}}^{(p)}}(\varprojlim_{(n,p)}\boldsymbol{\mu}_n(k))\to A_G$$

defined by:

$$[f]\otimes g\mapsto\overline{f(g)}$$

Recall that $\hat{\mathbb{Z}}^{(p)}$ is not only just a topological group, it's a topological ring and we have a ring map:

$$\hat{\mathbb{Z}}^{(p)}\to\mathbb{Z}[\hat{\mathbb{Z}}^{(p)}]$$

which means that $H^1(G,A)$ is also a $\hat{\mathbb{Z}}^{(p)}$-module in the sense of $\hat{\mathbb{Z}}^{(p)}$ as a ring, not as an abelian group. Similarly, after choosing ζ, we get a ring isomorphism:

$$\hat{\mathbb{Z}}^{(p)}\to G$$

Then the above tensor is understood that over objects are $\hat{\mathbb{Z}}^{(p)}$-module.

Then notice that we know that g_1g_2 is the addition in G and g_1^n is the multiplication by n in G. Then we need to check the tensor map is well-defined. That is to check that it's independent the representative of $[f]$ and is $\hat{\mathbb{Z}}^{(p)}$-balanced. However one thing to notice is that when checking balanced is to show that:

$$f(xg)=\Phi(f,xg)=\phi(xf,g)=xf(g)\in A_G$$

For all $x\in\hat{\mathbb{Z}}^{(p)}$. I claim that you don't have to worry about all elements in $\hat{\mathbb{Z}}^{(p)}$, but only $\mathbb{Z}\subset\hat{\mathbb{Z}}^{(p)}$. To see why, recall that $\hat{\mathbb{Z}}^{(p)}$ and G are Hausdorff, which means that limit is unique. Then $\mathbb{Z}$ is dense in $\hat{\mathbb{Z}}^{(p)}$, then we know that for each $x\in\hat{\mathbb{Z}}^{(p)}$, we can find $x_i\in\mathbb{Z}$ converging to x, then notice that multiplication and f are continuous, therefore we know that:

$$f(x_ig)\to f(xg)$$

Then if $f(x_ig)=x_if(g)$, we know that $x_if(g)\to xf(g)$, therefore by uniqueness of limit we know $f(xg)=xf(g)$.

Then, notice that via the isomorphism $\hat{\mathbb{Z}}^{(p)}\to G$ $1\mapsto\zeta$ we know that we have the following diagram:

$$\begin{array}{ccc} H^1(G,A)\otimes_{\hat{\mathbb{Z}}^{(p)}}(\varprojlim_{(n,p)}\boldsymbol{\mu}_n(k)) & \longrightarrow & A_G \\ {\scriptstyle\zeta\mapsto 1}\big\downarrow & \nearrow_{f\mapsto f(\zeta)} & \\ H^1(G,A) & & \end{array}$$

Therefore we know that the horizontal map is an isomorphism, therefore if we cal this map $\Phi: H^1(G,A)\otimes_{\hat{\mathbb{Z}}^{(p)}}(\varprojlim_{(n,p)}\boldsymbol{\mu}_n(k))\to A_G$, it's an isomorphism, then it induces an isomorphism:

$$H^1(G,A)\simeq\mathrm{Hom}_{\hat{\mathbb{Z}}^{(p)}}((\varprojlim_{(n,p)}\boldsymbol{\mu}_n(k)),A_G)$$

where $f:G\to A$ is mapped to the map f, which is canonical! Using this, we obtained a canonical description from something depending on choices.

Notice that this identification is made by:

$$H^1(G,A)\simeq H^1(G,A)\otimes_{\hat{\mathbb{Z}}^{(p)}}(\varprojlim_{(n,p)}\boldsymbol{\mu}_n(k))\simeq A_G\simeq\mathrm{Hom}_{\hat{\mathbb{Z}}^{(p)}}(\hat{\mathbb{Z}}^{(p)},A_G)\simeq\mathrm{Hom}_{\hat{\mathbb{Z}}^{(p)}}((\varprojlim_{(n,p)}\boldsymbol{\mu}_n(k)),A_G)$$

where $f\mapsto f\otimes\zeta\mapsto(1\mapsto f(\zeta))\mapsto(\zeta\mapsto 1\mapsto f(\zeta))=f$.

Then other assertions of how (q,ϕ) works can be proved similar to the above proposition. □

4 Cohomological Dimensions

Before we discuss Galois cohomology, let's introduce a quite useful tool, the cohomological dimensions. We won't explain everything in general but instead we will focus on how this notion applies to the study of profinite groups. We begin with the definition:

Definition 4.1. Let G be a profinite group, for each prime number p, we define the **p-cohomological dimension** $\mathrm{cd}_p(G)$ (resp. the **strict-p-cohomological dimension** $\mathrm{scd}_p(G)$) to be the smallest integer n such that for any torsion G-module (resp. any G-module) A and any $i > n$, the p-primary part of $H^i(G, A)$ vanishes.

We define the **cohomological dimension** $\mathrm{cd}(G)$ (resp. the **strict cohomological dimension** $\mathrm{scd}(G)$) to be the $\sup_p \mathrm{cd}_p(G)$ (resp. $\sup_p \mathrm{scp}_p(G)$).

Proposition 4.2. Let G be a profinite group, then the following conditions are equivalent:

1. $\mathrm{cd}_p(G) \leqslant n$.
2. $H^i(G, A) = 0$ for all $i > 0$ and any p-torsion G-module A.
3. $H^{n+1}(G, A) = 0$ for all simple p-torsion G-module A.

Proof. Recall that for any torsion G-module A. We know that we have the following decomposition:

$$A = \oplus_p A(p)$$

where p is the p-primary part of A. This is not just as a direct sum of abelian groups, it' also a direct sum of $\mathbb{Z}[G]$-modules.

Then we know that recall that cohomology commutes with direct sums, therefore:

$$H^i(A, G) \simeq \oplus_p H^i(G, A(p))$$

Notice that using our description of the cohomology using $C^\bullet(G, A)$, we know that every element in $H^i(G, A(p))$ is annihilated by some power of p. Therefore we know that $H^i(G, A(p))$ lies in the p-primary part of $H^i(G, A)$. Now notice that multiplication by any power of p will be an automorphism on $A(q)$ if $p \neq q$. I will let you show this, but this is essentially the fact that $\gcd(p^k, q) = 1$ then you can show multiplication is both surjective and injective. This map is also compatible with the group action, therefore we know that multiplication by p on $H^i(G, A(q))$ also induces an isomorphism on $H^i(G, A(q))$, therefore we know that if a nonzero element in $H^i(G, A)$ is mapped to 0 by multiplication of p^k, then this element is necessarily in $H^i(G, A(p))$.

Then if we assume 1: by definition we know that the p-primary part of $H^i(G, A)$ will vanish, that is $H^i(G, A(p))$ will vanish. Then if A itself is p-torsion, $A = A(p)$, we are done with $1 \Rightarrow 2$. Conversely, $A(p)$ is a p-torsion module for any torsion A-module, therefore $2 \Rightarrow 1$.

Clearly if 1 holds, then 3 holds since a simple p-torsion module is also a p-torsion module. So let's assume 3 holds. Recall that any finite R-module have a finite filtration whose successive quotients are simple. To see why, we know that the set of submodules of a finite R-module is finite, therefore we can pick one with minimal size, then it has no submodule. Then it's simple, then we consider the quotient, and do induction on the size of the quotient, we are done. Then notice that each submodule in the finite filtration here is still a p-torsion G-module.

Another observation is that any torsion G-module is a direct limit of it's finite G-submodules. To see why this is true, we first know that this module is the direct limit of it's finitely generated submodule. For each finitely generated torsion G-module, I claim that it finite. Recall that G is compact and A is discrete, we know that the orbit of each element in A is going to be compact in A, therefore finite, then you can use this to show that the finitely generated submodule is finite. Now if further that A is a p-torsion G-module, then each finite submodule in the direct limit is also p-torsion, then since cohomology commutes with direct limit, we know that:

$$H^{n+1}(G, A) \simeq \varinjlim H^{n+1}(G, A')$$

where A' is a finite p-torsion G-module. Recall that G has a filtration of simple p-torsion G-modules. Then you can use the associated LES to show that $H^{n+1}(G, A') = 0$, therefore $H^{n+1}(G, A) = 0$ for any torsion G-module A.

Then to prove for other $i > n$, let's notice that we have an embedding:

$$0 \to A \to \mathrm{Ind}_{\{1\}}^{G} A \to \mathrm{coker} \to 0$$

Then consider the induced LES of the cohomology we notice that $H^i(G, \mathrm{Ind}_{\{1\}}^{G} A) = 0$ for $i \geqslant 1$. Then we know that:

$$\cdots \to H^{n+1}(G, A) \to H^{n+1}(G, \mathrm{Ind}_{\{1\}}^{G} A) \to H^{n+1}(G, \mathrm{coker}) \to H^{n+2}(G, A) \to H^{n+2}(G, \mathrm{Ind}_{\{1\}}^{G} A) = 0 \to H^{n+2}(G, \mathrm{coker})$$

Notice that if A is p-torsion, then so is the induced module, therefore so is the cokernel. Then $H^{n+1}(G, \mathrm{coker}) = 0$, then we know that that $H^{n+2}(G, A) \simeq H^{n+1}(G, \mathrm{coker}) = 0$. Then we can use induction to keep going to conclude condition 2. □

Proposition 4.3. For any profinite group G, we have:

$$\mathrm{cd}_p(G) \leqslant \mathrm{scd}_p(G) \leqslant \mathrm{cd}_p(G) + 1$$

Proof. The first inequality is easy since we know that $\mathrm{cd}_p(G)$ is defined for all torsion G-modules but $\mathrm{scd}_p(G)$ is defined for all G-modules. Therefore we know that if n is a number such that all the p-primary part of $H^i(G, A)$ vanishes for all $i > n$ and all G-modules A, then this holds for all torsion G-modules as well.

To prove the second equation, let A be a G-module, consider the following 2 SES:

$$0 \to A_p \to A \to pA \to 0$$

$$0 \to pA \to A \to A/pA \to 0$$

where A_p is the kernel of the map $p : A \to A, \quad a \mapsto pa$. Notice that $A_p, A/pA$ are both p-torsion G-modules. We know that $H^i(G, A_p)$ and $H^{i-1}(G, A/pA)$ vanishes for all $i > \mathrm{cd}_p(G)$. Hence if we consider the associated LES of the two SES, we get:

$$H^i(G, A) \to H^i(G, pA), \quad H^i(G, pA) \to H^i(G, A)$$

are both injective for any $i > \mathrm{cd}_p(G) + 1$. Notice that the composition is $\times p$, therefore we know that:

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

is injective for all $i > \mathrm{cd}_p(G) + 1$. This implies the p-primary part vanishes, therefore we are done. □

Proposition 4.4. Let H be a closed subgroup of a profinite group G, then:

$$\mathrm{cd}_p H \leqslant \mathrm{cd}_p G, \quad \mathrm{scd}_p H \leqslant \mathrm{scd}_p G$$

If $[G : H]$ is relatively prime to p, then we get equality in the above equation.

Proof. Recall that from Shapiro's theorem we have an isomorphism:

$$H^i(G, \mathrm{Ind}_{H}^{G} B) \to H^i(H, B)$$

Moreover we notice that if B is p-torsion then so is the induced module $\mathrm{Ind}_{H}^{G} B$. Then this isomorphism tells us that if the p-primary part of $H^i(G, \mathrm{Ind}_{H}^{G} B)$ vanishes, then so is $H^i(H, B)$. This gives us the two inequalities.

To show the equality recall that when $[G : H]$ is prime to p, the restriction map:

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

will be injective on the p-primary part, therefore we know that when the p-primary part of $H^i(H, A)$ vanishes, so is that of $H^i(G, A)$. Therefore we know that we get the inverse inequality, we are done. □

Corollary 4.5. Let G_p be a Sylow-p-subgroup of a profinite group G, then:

$$\mathrm{cd}_p G = \mathrm{cd}_p G_p = \mathrm{cd} G_p$$

$$\mathrm{scd}_p G = \mathrm{scd}_p G_p = \mathrm{scd} G_p$$

Proof. By definition of a Sylow-p-subgroup, we know that the index is prime to p. Then the first equality in the two rows is clear. To show that $\mathrm{cd}_p G_p$ is equal to $\mathrm{cd} G_p$, notice that if ℓ is a prime number prime to p, we know that the number $[G_p : 1]$ will be prime to ℓ, therefore:

$$\mathrm{cd}_\ell(G_p) = \mathrm{cd}_\ell\{1\} = 0$$

$$\mathrm{scd}_\ell(G_p) = \mathrm{scd}_\ell\{1\} = 0$$

□

Proposition 4.6. Let H be a closed normal subgroup of G, we have:

$$\mathrm{cd}_p G \leqslant \mathrm{cd}_p H + \mathrm{cd}_p(G/H)$$

Proof. Recall that for a closed normal subgroup H, we have the Hochschild-Serre-Spectral sequence:

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

Now let $m = \mathrm{cd}_p H$ and $n = \mathrm{cd}_p(G/H)$. We know that if A is a torsion A-module, then it's a torsion H-module and $H^i(H, A)$ will be a torsion G/H-module. Similar statement holds for p-primary G-module A.

Recall that by previous theorem we only need to prove that for $i > m+n$, $H^i(G, A)$ vanishes for p-torsion G-modules A. Notice that by assumption that when A is p-torsion, $H^i(G/H, H^j(H, A))$ vanishes for $i > n$ and $H^j(H, A)$ vanishes for $j > m$. This implies that the E_2-page vanishes out side the rectangle $0 \leqslant i \leqslant n$ and $0 \leqslant j \leqslant m$. Therefore if $r > m + n$, we know that nothing converging to $H^r(G, A)$ can be nonzero, therefore the limit is 0. □

Lemma 4.7. Let G be a finite p-group and A a nonzero p-torsion G-module, then $A^G \neq 0$.

Proof. Let let's replace A by subgroup generated by the orbit of a single element, then since A is torsion, we can assume that this subgroup is finite as well. Then let's assume A is finite as well.

Notice that A is p-torsion and is finite, then we know that by the structure theorem of finitely generated abelian group, we know that $|A| = p^n$ for some positive integer n. We can assume that there are $x_1, \cdots, x_k$ such that A is disjoint union of the orbits Gx_i.

Notice that if we denote by G_{x_i} the stabilizer of x_i, then we know that we have bijections:

$$G/G_{x_i} \to Gx_i, \qquad gG_{x_i} \mapsto gx_i$$

Then $|Gx_i| = |G/G_{x_i}|$. Since G is finite p-group, we know that $|G/G_{x_i}| = p^{n_i}$ with $n_i = 0$ iff $x \in A^G$.

Then:

$$p^n = |A| = \sum_{i=1}^{k} |Gx_i| = \sum_{n_i \geqslant 1} p^{n_i} + |A^G|$$

Then we know that $p||A^G|$ with $|A^G| \geqslant 1$, then we know that $|A^G|$ is at least p. □

Lemma 4.8. Let G be a pro-p-group, any nonzero simple p-torsion G-module is isomorphic to $\mathbb{Z}/p$ with the trivial G action.

Proof. Let A be a nonzero simple G-module, we know that if we consider the submodule generated by a nonzero element in A, it's the whole module due to simplicity, then A is finite. Consider the stabilizer of each $a \in A$, which is an open subgroup, then we consider the intersection, which is still an open subgroup. Notice that if g is in the intersection, then clearly xgx^{-1} is also in the group as it also fixed every element in A, therefore we know that this subgroup is normal. Then we know that the group action factors through a finite quotient group, therefore $A^G \neq 0$. Since A is simple $A = A^G$, so G acts trivially on A, therefore being simple simply means that A has no sub abelian group, therefore we know that $A = \mathbb{Z}/p$ by the structure theorem of finitely generated abelian groups. □

Proposition 4.9. Let G be a pro-p-group, then $\mathrm{cd}(G) \leqslant n$ iff $H^{n+1}(G, \mathbb{Z}/p) = 0$.

Proof. Recall that by the previous proposition $\mathrm{cd}(G) \leqslant n$ is equivalent to the fact that $H^{n+1}(G, A)$ vanishes for all simple p-torsion G-module A.

But we saw that they are all $\mathbb{Z}/p$ with trivial action. □

5 Galois Cohomology

In this section, let K be a field and we fix a separable closure K_s of K, which is by definition an algebraic closure of K such that K_s has no nontrivial separable extension. Recall that we proved in the preliminary section on Galois theory that we have an isomorphism:

$$\mathrm{Gal}(K_s/K) \simeq \varprojlim_{L} \mathrm{Gal}(L/K)$$

where L/K is a finite Galois extension in K_s and the isomorphism is given by restriction of automorphisms. Recall that if we give the discrete topology on each $\mathrm{Gal}(L/K)$, then the absolute Galois group $\mathrm{Gal}(K_s/K)$ is a profinite group, and we can talk about $\mathrm{Gal}(K_s/K)$-module A. Then we know that we have an isomorphism:

$$H^i(\mathrm{Gal}(K_s/K), A) \simeq \varinjlim_{L} H^i(\mathrm{Gal}(L/K), A^{\mathrm{Gal}(K_s/L)})$$

Here what we are using is that if L/K is a finite Galois extension of K then the group $\mathrm{Gal}(K_s/L)$ is a normal subgroup of $\mathrm{Gal}(K_s/K)$ such that the quotient is $\mathrm{Gal}(L/K)$. Moreover, we know that if U is a normal subgroup of any group G, then for any G-module A, we know that A^U will be a G/U-module. In the case of the Galois group, we know that if we consider the projection:

$$\mathrm{Gal}(K_s/K) \to \mathrm{Gal}(L/K)$$

defined by restriction, we know that the kernel is just $\mathrm{Gal}(K_s/L)$. Moreover we know that any automorphism L/K extends to an automorphism of K_s/K, thus the restriction is surjective. Then we know that any element of of $\mathrm{Gal}(L/K)$ comes from a restriction of $\mathrm{Gal}(K_s/K)$, then it's action on $A^{\mathrm{Gal}(K_s/L)}$ is just defined to be the action of the lift restricted to $A^{\mathrm{Gal}(K_s/L)}$. Notice that this is independent of choice of the lift since the difference of the two lifts is in $\mathrm{Gal}(K_s/L)$, thus is the trivial action. Moreover suppose that $x \in A^{\mathrm{Gal}(K_s/L)}$, then we want to check that gx is still in $A^{\mathrm{Gal}(K_s/L)}$, let $g' \in \mathrm{Gal}(K_s/L)$, then we know that $g'gx = gg^{-1}g'gx = gx$ since $\mathrm{Gal}(K_s/L)$ is a normal subgroup. Finally, you can easily see that for $x \in A$, it's stabilizer is open in $\mathrm{Gal}(K_s/K)$ thus contains an open normal group corresponding to such a L/K. Therefore every $x \in A$ is fixed by some $\mathrm{Gal}(K_s/L)$. Therefore the union (direct limit) of $A^{\mathrm{Gal}(K_s/L)}$ will be A.

Therefore everything we know about the Galois group action agrees with the general theory of profinite group action.

Let's further review some Galios theory as they are quite useful in this section. The first one we will need is the **normal basis theorem**:

Lemma 5.1. Let L/K be a field extension and let $\sigma_1, \cdots, \sigma_n$ be a finite family of distinct K-automorphisms of L, i.e. distinct family in $\mathrm{Gal}(L/K)$, then they are linearly independent over L, that is if:

$$\sum_{i=1}^{n} a_i \sigma_i = 0$$

Then $a_i = 0$ for all i.

Proof. Let's assume that they are not linearly independent over L, therefore we can pick a minimal set $\{a_1, \cdots, a_m\} \in L - \{0\}\}$ such that:

$$a_1\sigma_{i_1} + \cdots + a_m\sigma_{i_m} = 0$$

Since $\simeq_i$ are all automorphisms, we must have $m \geqslant 2$. For any $x, y \in L$, we have:

$$a_1\sigma_{i_1}(xy) + \cdots + a_m\sigma_{i_m}(xy) = 0$$

that is;

$$a_1\sigma_{i_1}(x)\sigma_{i_1} + \cdots + a_m\sigma_{i_m}(x)\sigma_{i_m} = 0$$

We also have:

$$a_1\sigma_{i_1}(x)\sigma_{i_1} + \cdots + a_m\sigma_{i_1}(x)\sigma_{i_m} = 0$$

Therefore:

$$a_2(\sigma_{i_1}(x) - \sigma_{i_2}(x))\sigma_{i_2} + \cdots + a_m(\sigma_{i_1}(x) - \sigma_{i_m}(x))\sigma_{i_m}$$

Notice that $\sigma_{i_1} \neq \sigma_{i_2}$, therefore there is a x such that $\sigma_{i_1}(x) - \sigma_{i_2}(x) \neq 0$, but the above equation is a contradiction to the minimality. □

Lemma 5.2. Let L/K be a finite Galois extension and let $\mathrm{Gal}(L/K) = \{\sigma_1, \cdots, \sigma_n\}$, then there exists $x \in L$ such that $\sigma_1(x), \cdots, \sigma_n(x)$ is a basis of L over K.

A basis of L over K of the above form is usually called a **normal basis** of L over K.

Proof. We will divide the proof of this result to two cases: the first case is when K is infinite and the second case is when the Galois group $\mathrm{Gal}(L/K)$ is cyclic. Recall that when K is a finite field, then any finite extension of K will be Galois and that it's Galois group will be cyclic generated by a power of the Frobenius map. This justifies our strategy.

Now we make the following observation: $\{\sigma_1(x), \cdots, \sigma_n(x)\}$ is a basis iff the determinant of the matrix $(\sigma_i\sigma_j(x))$ is 0. First if:

$$\det(\sigma_i\sigma_j(x)) \neq 0$$

and $\sum_j a_j\sigma_j(x) = 0$ for some $a_j \in K$. Then firstly by apply σ_i to $\sum_j a_j\sigma_j(x) = 0$, we conclude that $\sum_j a_j\sigma_i\sigma_j(x) = 0$ for all i. Since the determinant is none zero, we conclude that the column vectors are independent, then we know that:

$$\sum_j a_j\sigma_i\sigma_j(x) = 0$$

implies that the a_j-linear combinations of the column vectors vanish, therefore $a_j = 0$ for all j. Therefore $\sigma_j(x)$ will be independent, thus a basis.

Conversely, suppose that the determinant is 0. Then there will be $b_1, \cdots, b_n \in L$ not all 0 such that:

$$\sum_j b_j \simeq_i \sigma_j(x) = 0$$

for all i. Let's assume $b_1 \neq 0$, then recall that we proved in the etale covering space chapter that L/k is finite separable iff the following bilinear form is nondegenerate:

$$L \times L \to k, \qquad (x, y) \mapsto \mathrm{Tr}_{L/k}(xy)$$

Therefore take $x = 1$ which is not 0, then there will be a $b \in L$ such that $\mathrm{Tr}_{L/K}(b) \neq 0$. Now replace b_j by $bb_1^{-1}b_j$ we can assume that $\mathrm{Tr}_{L/K}(b_1) \neq 0$. Then recall that another definition of the trace of b_1 will be the summation of all the Galois conjugates of b_i, i.e.:

$$\mathrm{Tr}_{L/K}(b_1) = \sum_j \sigma_j(b_1)$$

Then we know that by apply σ_i^{-1} to $\sum_j b_j\sigma_i\sigma_j(x) = 0$, we get:

$$\sum_j \sigma_i^{-1}(b_j)\sigma_j(x) = 0$$

Summing over i we get:

$$\sum_j \mathrm{Tr}_{L/K}(b_j)\sigma_j(x) = 0$$

Therefore $\sigma_j(x)$ will not be linearly independent.

Then let's assume that K is infinite and prove the existence of a normal basis. Recall that for all σ_i, σ_j, we know that $\sigma_i\sigma_j$ will be another $\sigma_{p(i,j)}$. Then we define the function $p(i,j)$ by the above relation. Consider the polynomial:

$$f(X_1, \cdots, X_n) = \det(X_{p(i,j)})$$

I claim that f is not 0. To prove this, since K is infinite, we only need to prove that there is one element x in K^n such that $f(x) \neq 0$. Notice that if $p(i,j) = p(i',j)$, then $i = i'$ and if $p(i,j) = p(i,j')$ we conclude that $j = j'$. Then we know that $f(1, 0, \cdots, 0)$ is the determinant of a matrix whose entries are either 1 or 0. Moreover we know that 1 only appear once on each column and each row, therefore this matrix has determinant ± 1, thus f is not 0.

We have:

$$f(\sigma_1(x), \cdots, \sigma_n(x)) = \det(\sigma_i\sigma_j(x))$$

Let $\{x_1, \cdots, x_n\}$ be a basis of L over K, any $x \in L$ is $x = \sum_j a_j x_j$ where $a_j \in K$. Then $\sigma_i(x) = \sum_j a_j \sigma_i(x_j)$. let:

$$g(Y_1, \cdots, Y_n) = f(\sum_j \sigma_1(x_j)Y_j, \cdots, \sum_j \sigma_n(x_j)Y_j)$$

Now notice that the matrix $(\sigma_i(x_j))$ is an invertible matrix. Indeed, is $\sum_j b_j \simeq_i (x_j) = 0$ for some $b_1, \ldots, b_n \in L$ and for all j, we find that $\sum_i b_i\sigma_i$ vanishes on all basis, therefore $\sum_i b_i\sigma_i = 0$ therefore $b_i = 0$. Let (b_{ij}) be the inverse matrix of $(\sigma_i(x_j))$. Then we have:

$$g(\sum_j b_{1j}X_j, \cdots, \sum_j b_{nj}X_j) = f(X_1, \cdots, X_n)$$

Then since $f(X_1, \cdots, X_n)$ is not 0, we get $g(Y_1, \cdots, Y_n) \neq 0$. Since K is infinite, there will be $(a_1, \cdots, a_n) \in K^n$ such that:

$$g(\sigma_1(a_1), \cdots, \sigma_n(a_n)) \neq 0$$

That is:

$$f(\sigma_1(\sum_j a_j x_j), \cdots, \sigma_n(\sum_j a_j x_j)) \neq 0$$

Let $x = \sum_j a_j x_j$, we know that $\sigma_j(x)$ will be a basis, thus a normal basis.

Now if K is finite, we can assume that $\mathrm{Gal}(L/K)$ is cyclic, then choose a generator $\sigma \in \mathrm{Gal}(L/K)$, then we know that we have a $K[T]$-module structure on L defined by:

$$(\sum_i a_i T^i)x = \sum_i a_i \sigma^i(x)$$

Notice that σ satisfies $T^n - 1 = 0$. Moreover, if σ any relation of lower degree, then consider the automorphisms:

$$1, \sigma, \sigma^1, \cdots, \sigma^{n-1}$$

which are distinct K-automorphisms of L, will be linearly dependent contradicting the previous result. Therefore the minimal polynomial of σ is $T^n - 1$. We also notice that $[L : K] = n$.

Recall that $K[T]$ is a PID, and L is finitely generated over $K[T]$. Moreover, notice that since every $x \in L$ is annihilated by some polynomial in $K[T]$, then L is a torsion $K[T]$-module therefore by the structure theorem of finitely generated module over $K[T]$:

$$L \simeq \oplus_{i=1}^n K[T]/(f_i)$$

such that $f_1|f_2|\cdots|f_n$. Moreover, we know that the action of T over the direct sum is just multiply by T, therefore it's minimal polynomial is the least common multiple of f_i, therefore is f_n, therefore $f_n = T^n - 1$. Notice that $K[T]/T^n - 1$ is already dimension n over K, therefore $L \simeq K[T]/T^n - 1$.

Then let $x \in L$ be the element corresponding to $1 \in K[T]/(T^n - 1)$. Then we know that $x, \sigma(x), \sigma^{n-1}(x)$ correspond to $1, T, \cdots, T^{n-1}$ in $K[T]/(T^n - 1)$, thus is a basis, we are done. $\square$

Remark 5.3. Let's make a short remark here about why a normal basis is useful. Recall that if L/K is a finite Galois extension, we have a natural $\mathrm{Gal}(L/K)$-module structure on L. Let $\sigma_1(x), \cdots, \sigma_n(x)$ be a normal basis, then I claim that L/K is an induced $\mathrm{Gal}(L/K)$-module.

To see why, let $G = \mathcal{G}\dashv\updownarrow(L/K)$, then we have an $\mathbb{Z}[G]$-module isomorphism:

$$K[G] \to L, \qquad \sigma_i \mapsto \sigma_i(x)$$

This is indeed an isomorphism of K-vector spaces which is compatible with the group action. Then notice that we have an isomorphism of $\mathbb{Z}[G]$-modules:

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], K) \simeq K[G]$$

Therefore we know that $K[G]$ is induced and thus L is also induced.

Proposition 5.4. For any finite Galois extension L/K, we have:

$$H^i(\mathrm{Gal}(L/K), L) = \begin{cases} K & \text{if } i = 0, \\ 0 & \text{if } i > 0, \end{cases}$$

hence:

$$H^i(\mathrm{Gal}(K_s/K) : K_s) = \begin{cases} K & \text{if } i = 0, \\ 0 & \text{if } i > 0, \end{cases}$$

Proof. This first assertion just following from the fact that L is an induced $\mathrm{Gal}(L/K)$-module and therefore $H^0(\mathrm{Gal}(L/K), K) = L^{\mathrm{Gal}(L/K)} = K$. Moreover all the higher cohomology vanishes due to Shapiro's theorem.

Using the direct limit formula we have:

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

Notice that K_s/L is again Galois, therefore in particular normal, then in the section of field theory, we know that $K_s^{\mathrm{Gal}(K_s/L)}$ is purely inseparable over L. Moreover since K_s/L is separable we know that $K_s^{\mathrm{Gal}(K_s/L)} = K_s \cap K_s^{\mathrm{Gal}(K_s/L)} = L$. Therefore:

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

Then we can use the first part the assertion. □

Theorem 5.5. (Hilbert 90) For any finite Galois extension L/K, we have:

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

Proof. Clearly that we have a left action of $\mathrm{Gal}(L/K)$ on L^*. Then let:

$$f : \mathrm{Gal}(L/K) \to L^*$$

be a 1-cocycle, then since $f(\sigma) \neq 0$ for all $\sigma \in \mathrm{Gal}(L/K)$, then from the normal basis theorem, there is a $x \in L$ such that:

$$y = \sum_{\sigma \in \mathrm{Gal}(L/K)} f(\sigma)\sigma(x) \neq 0$$

For any $\tau \in \mathrm{Gal}(L/K)$, since f is in the kernel of the first differential, we have:

$$f(\tau\sigma) = \tau \cdot (f(\sigma)) \cdot f(\tau)$$

Then we know that:

$$\begin{aligned} \tau(y) &= \sum_{\sigma \in \mathrm{Gal}(L/K)} \tau(f(\sigma))\tau\sigma(x) \\ &= \sum_{\sigma \in \mathrm{Gal}(L/K)} f(\tau)^{-1} f(\tau\sigma)\tau\sigma(x) \\ &= f(\tau)^{-1} y \end{aligned}$$

So $f(\tau) = y\tau(y)^{-1}$. Recall that the image of the 0-th differential if there is an $a \in A$ such that:

$$f(g) = ga - a$$

Since the addition in the group L^* is represented using multiplication, then notice that $f(\tau) = y - \tau \cdot y$ using the additive form. Therefore f is in fact in the image of the 0-th differential, therefore $H^1(\mathrm{Gal}(L/K), L^*) = 0$ as well.

Then notice that K_s^* is the union of all L^*, then the direct limit formula tells us:

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

□

We will give another proof of this later using descent theory and etale cohomology in the next chapter.

The above Hilbert 90 tells us that the degree 1 cohomology of K_s^* vanishes. Then a natural question becomes can we say anything about it's higher degree cohomology. For example we can ask when all it's higher cohomology vanishes? The following theorem tells you that the key is lies in whether $H^2(\mathrm{Gal}(K_s/K), K_s^*)$ vanishes or not.

Theorem 5.6. 1. Let K be a field of characteristic p, then $\mathrm{cd}_p(\mathrm{Gal}(K_s/K)) \leqslant 1$.

2. Assume that $H^2(\mathrm{Gal}(K_s/L), K_s^*)$ for any finite extension L of K contained in K_s, then $\mathrm{cd}(\mathrm{Gal}(K_s/K)) \leqslant 1$, that is for any torsion $\mathrm{Gal}(K_s/K)$-module A, we have:

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

for all $i \geqslant 2$. Moreover we have:

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

for all $i \geqslant 1$.

Proof. Let's deal with 1 first. Let G_p be a Sylow-p-subgroup of $\mathrm{Gal}(K_s/K)$ and let $M = K_s^{G_p}$. Recall that we have an SES of $\mathrm{Gal}(K_s/K)$-modules:

$$0 \to \mathbb{Z}/p \to K_s \xrightarrow{\wp} K_s \to 0$$

where $\mathrm{Gal}(K_s/K)$ acts trivially on $\mathbb{Z}/p$. This $\wp$ is the map $\wp(x) = x^p - x$ for all $x \in K_s$. Notice that this indeed is compatible with the group action since $\sigma(x^p - x) = \sigma(x)^p - \sigma(x)$.

Recall that G_p, being a Sylow-p-subgroup, is a closed subgroup in $\mathrm{Gal}(K_s/K)$, therefore we know that the Galois group of K_s/M is again G_p. Then we know from previous result:

$$H^i(G_p, K_s) = H^i(\mathrm{Gal}(K_s/M), K_s) = 0$$

for all $i \geqslant 1$. Then we consider the LES associated to the above SES, therefore we know that $H^i(G_p, \mathbb{Z}/p) = 0$ for $i \geqslant 2$. Since G_p is also a pro-p-group, by the discussion in the previous section, we know that this implies:

$$\mathrm{cd}_p(\mathrm{Gal}(K_s/K)) = \mathrm{cd}_p(G_p) = \mathrm{cd}(G_p) \leqslant 1$$

Then let's prove 2: Let ℓ be a prime number distinct from p and let G_ℓ be a Sylow-ℓ-subgroup of $\mathrm{Gal}(K_s/K)$ and let $M = K_s^{G_\ell}$, we know that $M = \varinjlim_L L$ where L goes over all finite extensions of K contained in M. Then consider the following sequence of $\mathrm{Gal}(K_s/K)$-modules:

$$0 \to \boldsymbol{\mu}_\ell(K_s) \to K_s^* \xrightarrow{x \mapsto x^\ell} K_s \to 0$$

Notice that for any finite extension L contained in M, we have:

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

for $i = 1, 2$ by Hilbert 90 and the assumption. Then the LES associated to the above SES gives:

$$H^2(\mathrm{Gal}(K_s/L), \boldsymbol{\mu}_\ell(K_s)) = 0$$

Then notice that $G_\ell = \mathrm{Gal}(K_s/M)$ is the inverse limit of all $\mathrm{Gal}(K_s/L)$ where L is a finite extension of K contained in M. (Here the inverse image is just an intersection since if we have an automorphism of K_s over K that doesn't preserve M, then there is one element in M that mapped outside M, we can use this to show that it's not in the intersection of all $\mathrm{Gal}(K_s/L)$.) Therefore the direct limit formula gives:

$$H^2(G_\ell, \boldsymbol{\mu}_\ell(K_s)) = \varinjlim_L H^2(\mathrm{Gal}(K_s/L), \boldsymbol{\mu}_\ell(K_s)) = 0$$

Notice that $\boldsymbol{\mu}_\ell(K_s)$ has no trivial subgroup (this is where we need the assumption $\ell \neq p$), therefore is simple and isomorphic to $\mathbb{Z}/\ell$ with trivial G_ℓ action.

Therefore we know that this implies:

$$\mathrm{cd}_\ell(\mathrm{Gal}(K_s/K)) = \mathrm{cd}G_\ell \leqslant 1$$

From one we see that $\mathrm{cd}_p(\mathrm{Gal}(K_s/K)) \leqslant$, thus:

$$\mathrm{cd}(\mathrm{Gal}(K_s/K)) \leqslant 1$$

Then we know that:

$$\mathrm{scd}(\mathrm{Gal}(K_s/K)) \leqslant \mathrm{cd}(\mathrm{Gal}(K_s/K)) + 1 \leqslant 3$$

Then since K_s^* is a nontorsion $\mathrm{Gal}(K_s/K)$-module:

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

for all $i \geqslant 3$. Then the assumption plus Hilbert 90 implies that this actually vanishes for all $i \geqslant 1$. □

References