Local Class Field Theory

Damanvir Singh Binner

MP15017

A dissertation submitted for the partial fulfilment of MS degree in Science

Indian Institute of Science Education and Research Mohali

April 2018

Certificate of Examination

This is to certify that the dissertation titled “Local Class Field Theory ” submitted by Mr. Damanvir Singh Binner (Reg. No. MP15017) for the partial fulfilment of MS degree programme of the Institute, has been examined by the thesis committee duly appointed by the Institute. The committee finds the work done by the candidate satisfactory and recommends that the report be accepted.

Dr. Abhik Ganguli (Supervisor)	Dr. Aribam Chandrakant	Dr. Chetan Balwe

Dated: April 19, 2018

Declaration

The work presented in this dissertation has been carried out by me under the guidance of Dr. Abhik Ganguli at the Indian Institute of Science Education and Research Mohali.

This work has not been submitted in part or in full for a degree, a diploma, or a fellowship to any other university or institute. Whenever contributions of others are involved, every effort is made to indicate this clearly, with due acknowledgement of collaborative research and discussions. This thesis is a bonafide record of original work done by me and all sources listed within have been detailed in the bibliography.

Damanvir Singh Binner
(Candidate)
Dated: April 19, 2018

In my capacity as the supervisor of the candidate's project work, I certify that the above statements by the candidate are true to the best of my knowledge.

Dr. Abhik Ganguli
(Supervisor)

Acknowledgement

It gives me an immense pleasure to thank my advisor Dr. Abhik Ganguli for his priceless guidance and for giving me so much of his time.

I would like to thank my research progress committee members Dr. Aribam Chandrakant and Dr. Chetan Balwe for their support and encouragement.

I take this opportunity to thank the Head of the department and faculty members for providing a lively atmosphere for research. I am thankful to the non-academic staff of the department for helping me with administrative formalities.

I want to thank my classmates especially Manpreet Singh and Manoj Upreti for their constant support.

I owe the greatest debt to my parents for their emotional support in some of the tough times.

Contents

Chapter 1

Introduction

The central theme of this thesis is to understand Local Class Field Theory which classifies the finite abelian extensions of a local field. We have taken the cohomological approach closely following the expositions by Milne ([1]) and Neukirch ([2]). By a local field, we mean a field K that is locally compact with respect to a nontrivial valuation (cf. Lemma 36 for details). In what follows, we assume that K is a local field of characteristic 0 which means K is a finite extension of Q_p. We note in passing that the main theorems also hold for local fields with characteristic p.

In the second chapter, we have described the cohomology of groups. Firstly, we focus on finite groups. We begin with the study of standard group cohomology theory like Induced Modules, Shapiro's Lemma, restriction, inflation and corestriction maps, Hilbert's Theorem 90. We move on to study some properies of Homology groups and describe how long exact sequences for Homology and Cohomology can be spliced together to give a very long exact sequence for Tate Cohomology. Then we describe an alternative approach to Tate Cohomology which makes it possible to define the functorial maps and cup products directly on Tate Cohomology groups. After that we focus on the Tate cohomology of finite cyclic groups. Finally, we give two proofs of Tate's Theorem.

Theorem 1. *(Tate's Theorem) Let G be a finite group and let C be a G-module. Suppose that for all subgroups H of G,*
1. $H^1(H, C) = 0$, and
2. $H^2(H, C)$ is a cyclic group of order equal to $(H : 1)$. Then, for all r, there is an isomomorphism

$$H^r(G, \mathbb{Z}) \to H^{r+2}(G, C)$$

depending only on the choice of generator for $H^2(G, C)$.

The first one is the original proof by Tate which involves the construction of the splitting module for the chosen generator γ of $H^2(G, C)$. The second proof shows that the isomorphism is given by cup product with the generator γ. Then we discuss the cohomology of profinite groups which allows us to study the cohomology of infinite galois extensions.

In the third chapter, we describe the Local Class Field Theory using the techniques developed in the second chapter. Firstly we describe finite unramified extensions. These extensions are cyclic and thus allow us to use the cohomology of finite cyclic groups. This leads us to the invariant map

$$inv_{L/K} : H^2(L/K) \to \mathbb{Q}/\mathbb{Z}$$

which is an isomorphism onto $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$. This shows that the second condition in the hypothesis of Tate's Theorem is satisfied. The first condition is satisfied because of Hilbert's Theorem 90. Thus the Tate's Theorem gives us the isomorphism

$$H^r(G, \mathbb{Z}) \to H^{r+2}(G, L^*)$$

for all $r \in \mathbb{Z}$. In particular for $r = -2$, it gives us the isomorphism

$$Gal(L/K) \to K^*/Nm_{L/K}(L^*)$$

The inverse of this isomorphism is known as the Local Artin Map. Then we show using the first proof of Tate's Theorem that the Local Artin Map for the finite unramified extensions has a very simple description namely it takes the class of uniformizer to the Frobenius element in $Gal(L/K)$. Then the definition of invariant map is extended to infinite unramified extensions to get the following isomorphism

$$inv_K : H^2(K^{un}/K) \to \mathbb{Q}/\mathbb{Z}$$

Furthermore, we show that the inflation map

$$H^2(K^{un}/K) \to H^2(K^{al}/K)$$

is an isomorphism. These isomorphisms help us to prove that for finite ramified extensions also, there is an isomorphism

$$inv_{L/K} : H^2(L/K) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

Thus the hypothesis of Tate's Theorem is satisfied in the general case also and we get the isomorphism

$$Gal(L/K)^{ab} \to K^*/Nm_{L/K}(L^*)$$

The inverse of this isomorphism induces the surjective map

$$\phi_{L/K} : K^* \to Gal(L/K)^{ab}$$

The second proof of Tate's Theorem tells us that this map is given by cup product with a chosen generator of $H^2(L/K)$ (which we call the Local Fundamental Class). The properties of cup products and invariant maps help us to show the following Theorem :

Theorem 2. *Let $L \supset E \supset K$ be local fields with both L and E Galois over K. Then the following diagram commutes :*

$$\begin{array}{ccc} K^* & \xrightarrow{\phi_{L/K}} & Gal(L/K)^{ab} \\ \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \pi} \\ K^* & \xrightarrow{\phi_{E/K}} & Gal(E/K)^{ab} \end{array} \tag{1.1}$$

where the map π is induced by the surjective map $Gal(L/K) \to Gal(E/K)$ given by $\sigma \mapsto \sigma_E$.

Theorem 2 implies that if $L \supset E \supset K$ is a tower of finite abelian extensions of K, then $\forall\ a \in K^*$,

$$\phi_{L/K}(a) \restriction_E = \phi_{E/K}(a)$$

This compatibility helps us to define the Local Artin Map ϕ_K

$$\phi_K : K^* \to Gal(K^{ab}/K)$$

to be the homomorphism such that for every finite abelian extension L/K,

$$\phi_K(a) \restriction_L = \phi_{L/K}(a)$$

This definition leads us to the following Theorem which is known as the Local Reciprocity Law.

Theorem 3. *For every local field K, there exists a homomorphism (Local Artin Map)*

$$\phi_K : K^* \to Gal(K^{ab}/K)$$

with the following properties :
(a) for every prime element π of K, $\phi_K(\pi) \restriction_{K^{un}} = Frob_K$;
(b) for every finite abelian extension L of K, $Nm_{L/K}(L^*)$ is contained in the kernel of $a \mapsto \phi_K(a) \restriction_L$, and ϕ_K induces an isomorphism

$$\phi_{L/K} : K^*/Nm_{L/K}(L^*) \to Gal(L/K)$$

The explicit description of the corestriction map in dimensions 0 and -2 helps us to prove the following Theorem :

Theorem 4. *(Norm Limitation Theorem) Let L be a finite extension of K, and let E be the largest abelian extension of K contained in L; then*

$$Nm_{L/K}(L^*) = Nm_{E/K}(E^*)$$

Using the definition of the local Artin map, we can define a pairing known as the Hilbert Symbol

$$K^*/K^{*n} \times K^*/K^{*n} \to \mu_n$$

The properties of the Hilbert Symbol help us to prove the following Theorem :

Theorem 5. *Let K be a local field containing a primitive n^{th} root of 1. Any element of K^* that is a norm from every cyclic extension of K of degree dividing n is an n^{th} power.*

A subgroup N of K^* is known as a norm group if there is a finite abelian extension L/K such that

$$Nm_{L/K}(L^*) = N$$

Theorem 5 and the properties of norm subgroups of K^* helps us to prove the Existence Theorem :

Theorem 6. *(Existence Theorem) Every open subgroup of finite index in K^* is a norm group.*

Theorem 2 and the Existence Theorem classify the finite abelian extensions of a local field K since they immediately imply the following Theorem :

Theorem 7. *Let K be a local field. For every finite abelian extension L of K, the map*

$$L \mapsto Nm_{L/K}(L^*)$$

is an order-reversing bijection from the set of finite abelian extensions of K to the set of subgroups of K^* of finite index.

Theorem 73 is known as the Existence Theorem because its crucial assertion is that given an open subgroup I of finite index in K^*, there exists an abelian extension L/K whose norm group $Nm_{L/K}(L^*) = I$. This field L is uniquely determined and is called the class field associated with I.

The Norm Limitation Theorem (Theorem 4) shows that there is no hope of classifying nonabelian extensions of a local field in terms of the norm groups since the nonabelian extensions do not generate any extra norm subgroups.

The Existence Theorem provides a topological characterization of norm groups, but there is also an arithmetic description of these groups :

The norm groups of K^* are precisely the groups containing

$$U_K^{(n)} \times (\pi)^f$$

for some $n \geq 0$ and some $f \geq 1$. Here $U_K^0 = U_K$, π is a prime element of K, and $(\pi)^f$ is the subgroup generated by π^f.

The collection of Local Artin Maps

$$\phi_{L/K} : K^*/Nm_{L/K}(L^*) \to Gal(L/K)$$

as L runs through the finite abelian extensions of K gives a homomorphism between the inverse systems $K^*/Nm_{L/K}(L^*)$ and $Gal(L/K)$ thereby inducing the isomorphism :

$$\widehat{\phi}_K : \widehat{K^*} \to Gal(K^{ab}/K)$$

where $\widehat{K^*}$ denotes the completion of K^* with respect to the topology for which the norm groups form a fundamental system of neighborhoods of 1. This topology on K^* is called the norm topology (see Remark 27 for details).

Since intersection of the norm groups is trivial, so K^* embeds into $\widehat{K^*}$ i.e. the natural map $K^* \to \widehat{K^*}$ is injective. Moreover, the image of K^* under this map is dense.

Chapter 2

The Cohomology of Groups

2.1 G-Modules

Definition 1. *Let G be a group. A G-module is an abelian group M together with a map*

$$(g, m) \mapsto gm : G \times M \to M$$

such that for all $g, g' \in G$, $m, m' \in M$,

(a) $g(m + m') = gm + gm'$;
(b) $(gg')m = g(g'm)$, $1m = m$.

Definition 2. *A G-module homomorphism is a map $\alpha : M \to N$ such that*

(a) $\alpha(m + m') = \alpha(m) + \alpha(m')$ *(i.e. α is a homomorphism of abelian groups)*
(b) $\alpha(gm) = g(\alpha(m))$ *for all $g \in G$, $m \in M$.*

We write $Hom_G(M, N)$ for the set of G-homomorphisms $M \to N$.

Remark 1. *The group algebra $\mathbb{Z}[G]$ of G is the free abelian group with basis the elements of G and with the multiplication provided by the group law on G. Thus the elements of $\mathbb{Z}[G]$ are the finite sums*

$$\sum_i n_i g_i, \quad n_i \in \mathbb{Z}, \quad g_i \in G$$

and

$$\left(\sum_i n_i g_i\right)\left(\sum_j n'_j g'_j\right) = \sum_{i,j} n_i n'_j (g_i g'_j)$$

A G-module structure on an abelian group extends uniquely to a $\mathbb{Z}[G]$-module structure, and a homomorphism of abelian groups is a homomorphism of G-modules if and only if it is a homomorphism of $\mathbb{Z}[G]$ modules.

If M and N are G-modules, then the set $Hom(M, N)$ of homomorphisms $\phi : M \to N$ (M and N regarded only as abelian groups) becomes a G-module with the structures

$$(\phi + \phi')(m) = \phi(m) + \phi'(m)$$

$$(g\phi)(m) = g\phi(g^{-1}m)$$

To verify this, observe that

$$(g(\phi+\phi'))(m) = g((\phi+\phi')(g^{-1}m)) = g\phi(g^{-1}m)+g\phi'(g^{-1}m) = (g\phi)(m)+(g\phi')(m) = (g\phi+g\phi')(m)$$

Hence

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

Moreover,

$$((gg')(\phi))(m) = gg'(\phi(g'^{-1}g^{-1}m)) = g(g'\phi(g'^{-1}g^{-1}m) = g(g'\phi)(g^{-1}m) = (g(g'\phi))(m)$$

Hence

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

and so we are done.

2.2 Induced Modules

Let H be a subgroup of G. For an H-module M, we define $Ind_H^G(M)$ to be the set of maps (not necessarily homomorphisms) $\phi : G \to M$ such that $\phi(hg) = h\phi(g)$ for all $h \in H$. Then $Ind_H^G(M)$ becomes a G-module with the operations

$$(\phi + \phi')(x) = \phi(x) + \phi'(x)$$

$$(g\phi)(x) = \phi(xg).$$

Firstly we need to verify that $\phi+\phi'$ and $g\phi$ so defined are actually elements of $Ind_H^G(M)$. We have

$$(\phi + \phi')(hg) = \phi(hg) + \phi'(hg) = h\phi(g) + h\phi'(g) = h(\phi + \phi')(g)$$

and

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

Now we need to verify that $Ind_H^G(M)$ is a G-module with these operations.

$$(g(\phi + \phi'))(x) = (\phi + \phi')(xg) = \phi(xg) + \phi'(xg) = (g\phi)(x) + (g\phi')(x) = (g\phi + g\phi')(x)$$

Hence

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

Moreover

$$((gg')\phi)(x) = \phi(xgg') = (g'\phi)(xg) = (g(g'\phi))(x)$$

Therefore

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

Lemma 1. *A homomorphism $\alpha : M \to M'$ of H-modules defines a homomorphism*

$$\eta : Ind_H^G(M) \to Ind_H^G(M')$$

of G-modules where $\eta(\phi) = \alpha \circ \phi$.

Proof. Firstly we need to show that if $\phi \in Ind_H^G(M)$, then $\alpha \circ \phi \in Ind_H^G(M')$. We have

$$(\alpha \circ \phi)(hg) = \alpha(\phi(hg)) = \alpha(h\phi(g)) = h(\alpha(\phi(g))) = h(\alpha \circ \phi)(g)$$

Note that in the second last equality, we have used that α is a H-module homomorphism. Now observe that

$$(\eta(\phi_1+\phi_2))(x) = (\alpha\circ(\phi_1+\phi_2))(x) = \alpha(\phi_1(x)+\phi_2(x)) = \alpha(\phi_1(x))+\alpha(\phi_2(x)) = \eta(\phi_1(x))+\eta(\phi_2(x))$$

Note that in the second last equality, we have used the fact that α is a homomorphism of abelian groups. Hence

$$\eta(\phi_1 + \phi_2) = \eta(\phi_1) + \eta(\phi_2)$$

Moreover,

$$(\eta(g\phi))(x) = \alpha((g\phi)(x)) = \alpha(\phi(xg)) = (\eta(\phi))(xg) = (g(\eta(\phi))(x)$$

Thus

$$\eta(g\phi) = g(\eta(\phi))$$

□

Theorem 8. *For every G-module M and every H-module N,*

$$Hom_G(M, Ind_H^G(N)) \cong Hom_H(M, N)$$

as abelian groups. This relation is known as Frobenius reciprocity.

Proof. Note that M is an H module as well and so $Hom_H(M, N)$ is defined.

Define the map

$$\eta_1 : Hom_G(M, Ind_H^G(N)) \to Hom_H(M, N)$$

such that for any G-module homomorphism $\alpha : M \to Ind_H^G(N)$, we have $\eta_1(\alpha) : M \to N$ given by

$$(\eta_1(\alpha))(m) = (\alpha(m))(1_G)$$

We have to verify that $\eta_1(\alpha)$ is an H-module homomorphism. For any $h \in H$,

$$\eta_1(\alpha)(hm) = \alpha(hm)(1_G) = (h\alpha(m))(1_G) = \alpha(m)(1_G h) = \alpha(m)(h1_G) = h(\alpha(m)(1_G)) = h(\eta_1(\alpha)(m))$$

Note that in the second equality, we have used that α is a G-module homomorphism and in the second last equality, we have used that $\alpha(m) \in Ind_H^G(N)$.
Now define the map

$$\eta_2 : Hom_H(M, N) \to Hom_G(M, Ind_H^G(N))$$

such that for any H-module homomorphism $\beta : M \to N$, we have $\eta_2(\beta) : M \to Ind_H^G(N)$ given by

$$(\eta_2(\beta))(m)(g) = \beta(gm)$$

Firstly we need to check that for any $m \in M$, $(\eta_2(\beta))(m)$ is actually an element of $Ind_H^G(N)$. For any $h \in H$, $g \in G$,

$$(\eta_2(\beta))(m)(hg) = \beta(hgm) = h(\beta(gm)) = h(\eta_2(\beta))(m)(g)$$

Note that in the second equality, we have used that β is an H-module homomorphism.

We also have to verify that $\eta_2(\beta)$ is a G-module homomorphism. For any $g' \in G$,

$$((\eta_2(\beta))(g'm))(g) = \beta(gg'm) = (\eta_2(\beta))(m)(gg') = (g'(\eta_2(\beta))(m))(g)$$

Thus

$$(\eta_2(\beta))(g'm) = g'(\eta_2(\beta)(m))$$

and we are done.

It is straightforward to check that η_1 is a homomorphism of abelian groups. The only thing left to show is that η_1 and η_2 are inverses of each other. For that, we will show that $\eta_1 \circ \eta_2$ and $\eta_2 \circ \eta_1$ are the identity maps.

Firstly consider the map $\eta_2 \circ \eta_1 : Hom_G(M, Ind_H^G(N)) \to Hom_G(M, Ind_H^G(N))$. For any G-module homomorphism $\alpha : M \to Ind_H^G(N)$, $g \in G$, $m \in M$, we have

$$\eta_2(\eta_1(\alpha))(m)(g) = (\eta_1(\alpha))(gm) = \alpha(gm)(1_G) = (g(\alpha(m)))(1_G) = (\alpha(m))(1_G g) = \alpha(m)(g)$$

Thus $\eta_2 \circ \eta_1$ is the identity map.

Next consider the map $\eta_1 \circ \eta_2 : Hom_H(M, N) \to Hom_H(M, N)$. For any H-module homomorphism $\beta : M \to N$, we have

$$\eta_1(\eta_2(\beta))(m) = (\eta_2(\beta))(m)(1_G) = \beta(1_G m) = \beta(m)$$

Thus $\eta_1 \circ \eta_2$ is the identity map as well. □

Let $\Phi : Ind_H^G(N) \to N$ be the map such that $\phi \mapsto \phi(1_G)$. Then Φ is an H-module homomorphism because

$$\Phi(h\phi) = (h\phi)(1_G) = \phi(1_G h) = \phi(h 1_G) = h\phi(1_G) = h(\Phi(\phi))$$

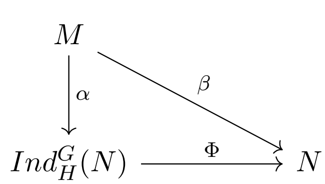
Note that the second equality follows from the action of G on $Ind_H^G(N)$ and the second last equality holds because $\phi \in Ind_H^G(N)$. The isomorphism η_1 in the proof of Theorem 8 can now be viewed in terms of Φ. For any $\alpha \in Hom_G(M, Ind_H^G(N))$ and $m \in M$, we have

$$(\eta_1(\alpha))(m) = (\alpha(m))(1_G) = \Phi(\alpha(m))$$

i.e. $\eta_1(\alpha) = \Phi \circ \alpha$.

Corollary 1. $(Ind_H^G(N), \Phi)$ *satisfies the following universal property :*

For any H-module homomorphism $\beta : M \to N$ from a G-module M to N, there exists a unique G-module homomorphism $\alpha : M \to Ind_H^G(N)$ such that $\Phi \circ \alpha = \beta$ i.e. the following diagram commutes :



(2.1)

Proof. The surjectivity of the isomorphism η_1 implies that $\beta = \eta_1(\alpha)$ for some $\alpha \in Hom_G(M, Ind_H^G(N))$. Then $\beta = \Phi \circ \alpha$ by the above discussion.

Now let $\alpha_1, \alpha_2 \in Hom_G(M, Ind_H^G(N))$ be such that $\Phi \circ \alpha_1 = \Phi \circ \alpha_2 = \beta$. Then we have $\eta_1(\alpha_1) = \eta_1(\alpha_2)$. Then injectivity of η_1 shows that $\alpha_1 = \alpha_2$ and we get the uniqueness of α such that the diagram commutes. $\square$

Theorem 9. *For any exact sequence of H-modules*

$$0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \to 0$$

the sequence of G-modules

$$0 \to Ind_H^G M \xrightarrow{\alpha'} Ind_H^G N \xrightarrow{\beta'} Ind_H^G P \to 0$$

is also exact where the maps α', β' are as defined in Lemma 1 i.e. $\alpha'(\phi) = \alpha \circ \phi$ and $\beta'(\psi) = \beta \circ \psi$

Proof. Firstly we will prove that α' is injective. Let $\alpha'(\phi) = 0$ which means that $\alpha'(\phi)(g) = 0 \ \forall \ g \in G$. Thus $\alpha(\phi(g)) = 0$ and so $\phi(g) = 0 \ \forall \ g \in G$ by the injectivity of α. Therefore $\phi = 0$ and we are done.

Next we will show that $Ker(\beta') = Im(\alpha')$. We already know that $Ker(\beta) = Im(\alpha)$. In particular, $\beta \circ \alpha = 0$. Now

$$(\beta' \circ \alpha')(\phi) = \beta'(\alpha \circ \phi) = \beta \circ (\alpha \circ \phi) = (\beta \circ \alpha) \circ \phi = 0$$

and so $Im(\alpha') \subset Ker(\beta')$.

Let $\psi \in Ker(\beta')$, then $\beta'(\psi) = 0$, so $\beta(\psi(g)) = 0 \ \forall \ g \in G$. This implies that $\psi(g) \in Ker(\beta) = Im(\alpha)$ and thus $\exists \ m_g \in M$ such that $\alpha(m_g) = \psi(g)$. Define $\phi : G \to M$ such that $\phi(g) = m_g$. Therefore,

$$\psi(g) = \alpha(\phi(g)) = (\alpha'(\phi))(g) \ \forall \ g \in G$$

and so $\psi = \alpha'(\phi)$. For any $h \in H$, $g \in G$, we have $\psi(hg) = h\psi(g)$ since $\psi \in Ind_H^G N$. Thus

$$\alpha(\phi(hg)) = h(\alpha(\phi(g)) = \alpha(h\phi(g))$$

This implies that $\phi(hg) = h\phi(g)$ by the injectivity of α and so $\phi \in Ind_H^G M$. Now $\psi = \alpha'(\phi) \in Im(\alpha')$. Hence $Ker(\beta') \subset Im(\alpha')$ and we are done.

Finally we will prove that β' is surjective. Let $\phi \in Ind_H^G P$. Now let S be a set of right coset representatives of H in G. Then every element of G can be written uniquely in the form hs for some $h \in H$ and some $s \in S$. (The uniqueness follows from the fact that any two distinct cosets are disjoint). Since the map $\beta : N \to P$ is surjective, for each $s \in S$, we can choose some $n(s) \in N$ such that $\beta(n(s)) = \phi(s)$. Now define a map $\phi' : G \to N$ such that $\phi'(hs) = h(n(s))$. Suppose we are given some $h_1 \in H$, $g_1 \in G$. Moreover, we know that $g_1 = h_2 s_2$ for some unique $h_2 \in H$, $s_2 \in S$. Then we have

$$\phi'(h_1 g_1) = \phi'(h_1 h_2 s_2) = h_1 h_2 n(s_2) = h_1 \phi'(h_2 s_2) = h_1 \phi'(g_1)$$

and so $\phi' \in Ind_H^G N$. Let $g \in G$, then we know that $g = hs$ for some unique $h \in H$, $s \in S$. Then

$$\phi(g) = \phi(hs) = h\phi(s) = h\beta(n(s)) = \beta(h(n(s))) = \beta(\phi'(hs)) = \beta'(\phi'(hs)) = \beta'(\phi'(g))$$

Hence $\phi = \beta'(\phi') \in Im(\beta')$ and we are done. $\square$

When $H = \{1\}$, an H-module is just an abelian group. In this case, we drop the H from the notation $Ind_H^G(N)$. Thus

$$Ind^G(M_0) = \{\phi : G \to M_0\}$$

where ϕ is a map and not necessarily a homomorphism.

Lemma 2. *$Ind^G(M_0) \cong Hom(\mathbb{Z}[G], M_0)$ as abelian groups where $Hom(\mathbb{Z}[G], M_0)$ denotes homomorphisms of abelian groups.*

Proof. Define the map $\kappa_1 : Hom(\mathbb{Z}[G], M_0) \to Ind^G M_0$ such that $\kappa_1(\psi) = \psi \restriction_G$. Clearly κ_1 is a homomorphism of abelian groups.

Now consider the map $\kappa_2 : Ind^G M_0 \to Hom(\mathbb{Z}[G], M_0)$ such that

$$(\kappa_2(\phi)) \left(\sum_i n_i g_i \right) = \sum_i n_i \phi(g_i)$$

We have to show that $\kappa_2(\phi)$ is actually a homomorphism of abelian groups. Let $\sum_{i=1}^k n_i g_i$ and $\sum_{i=1}^{k'} n_i' g_i'$ be two arbitrary elements of $\mathbb{Z}[G]$. Firstly suppose that the sets $\{g_1, g_2, ..., g_k\}$ and $\{g_1', g_2', ..., g_{k'}'\}$ are disjoint. Define $g_{k+i} = g_i'$ and $n_{k+i} = n_i'$ $\forall$ $1 \le i \le k'$. Then $\sum_{i=1}^k n_i g_i + \sum_i^{k'} n_i' g_i' = \sum_{i=1}^{k+k'} n_i g_i$ and so

$$\begin{aligned}(\kappa_2(\phi)) \left(\sum_{i=1}^k n_i g_i + \sum_i^{k'} n_i' g_i' \right) &= (\kappa_2(\phi)) \left(\sum_{i=1}^{k+k'} n_i g_i \right) = \sum_{i=1}^{k+k'} n_i \phi(g_i) = \sum_{i=1}^k n_i \phi(g_i) + \sum_i^{k'} n_i' \phi(g_i') \\ &= (\kappa_2(\phi)) \left(\sum_{i=1}^k n_i \phi(g_i) \right) + (\kappa_2(\phi)) \left(\sum_{i=1}^{k'} n_i' \phi(g_i' \right)\end{aligned} \tag{2.2}$$

Thus the proof is complete in this case.

Now suppose that the sets $\{g_1, g_2, ..., g_k\}$ and $\{g_1', g_2', ..., g_{k'}'\}$ have some common elements. Rearrange g_i and g_i' such that the common elements are $g_1, g_2, ...g_t$ and $g_i = g_i'$ $\forall$ $1 \le i \le t$. Then

$$\sum_{i=1}^k n_i g_i + \sum_i^{k'} n_i' g_i' = \sum_{i=1}^t (n_i + n_i') g_i + \sum_{i=t+1}^k n_i g_i + \sum_{i=t+1}^{k'} n_i' g_i'$$

and so

$$
\begin{aligned}
(\kappa_2(\phi))\left(\sum_{i=1}^{k} n_i g_i + \sum_{i=1}^{k'} n'_i g'_i\right) &= (\kappa_2(\phi))\left(\sum_{i=1}^{t}(n_i + n'_i)g_i + \sum_{i=t+1}^{k} n_i g_i + \sum_{i=t+1}^{k'} n'_i g'_i\right) \\
&= \sum_{i=1}^{t}(n_i + n'_i)\phi(g_i) + \sum_{i=t+1}^{k} n_i\phi(g_i) + \sum_{i=t+1}^{k'} n'_i\phi(g'_i) \\
&= \left(\sum_{i=1}^{t} n_i\phi(g_i) + \sum_{i=t+1}^{k} n_i\phi(g_i)\right) + \left(\sum_{i=1}^{t} n'_i\phi(g'_i) + \sum_{i=t+1}^{k'} n'_i\phi(g'_i)\right) \\
&= \sum_{i=1}^{k} n_i\phi(g_i) + \sum_{i=1}^{k'} n'_i\phi(g'_i) = (\kappa_2(\phi))\left(\sum_{i=1}^{k} n_i g_i\right) + (\kappa_2(\phi))\left(\sum_{i=1}^{k'} n'_i g'_i\right)
\end{aligned}
\tag{2.3}
$$

Thus we have shown that $\kappa_2(\phi)$ is an element of $Hom(\mathbb{Z}[G], M_0)$ and so κ_2 is well defined.

The only thing left to show is that κ_1 and κ_2 are inverses of each other. From the definition of κ_2, it is clear that $(\kappa_2(\phi)) \restriction_G = \phi$. Thus $\kappa_1(\kappa_2(\phi)) = \phi$. Also $\kappa_2(\kappa_1(\psi)) = \kappa_2(\psi \restriction_G)$ and so

$$\kappa_2(\kappa_1(\psi))\left(\sum_i n_i g_i\right) = \sum_i n_i \psi \restriction_G (g_i) = \sum_i n_i\psi(g_i) = \psi\left(\sum_i n_i g_i\right)$$

since ψ is a homomorphism of abelian groups. Thus $\kappa_2(\kappa_1(\psi)) = \psi$ and we are done.

□

INDUCED MODULES

Definition 3. *A G-module M is said to be induced if $M \cong Ind^G(M_0)$ for some abelian group M_0.*

Theorem 10. *Let G be a finite group. Then for any abelian group M_0,*

$$Ind^G M_0 \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} M_0$$

Here $\mathbb{Z}[G] \otimes_{\mathbb{Z}} M_0$ is endowed with the G-structure such that

$$g(z \otimes m) = gz \otimes m.$$

Proof. Define the map

$$\alpha : Ind^G M_0 \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} M_0$$

such that

$$\alpha(\phi) = \sum_{g \in G} g \otimes \phi(g^{-1})$$

Clearly α is a homomorphism of abelian groups. For any $g_0 \in G$,

$$\alpha(g_0\phi) = \sum_{g\in G} g \otimes (g_0\phi)(g^{-1}) = \sum_{g\in G} g \otimes \phi(g^{-1}g_0) = \sum_{g'\in G}(g_0 g') \otimes \phi(g^{-1}) = g_0\left(\sum_{g'\in G} g' \otimes \phi(g'^{-1})\right) = g_0(\alpha(\phi))$$

where we changed the index of summation by taking $g_0^{-1}g = g'$

Thus

$$\alpha(g_0\phi) = g_0(\alpha(\phi))$$

and α is also a G-module homomorphism.

Let us label $G = \{g_1, g_2, ..., g_n\}$.

Now define the map

$$\beta' : \mathbb{Z}[G] \times M_0 \to Ind^G M_0$$

such that

$$\beta' \left(\sum_{i=1}^{n} n_i g_i, m \right) = \sum_{i=1}^{n} n_i \phi_{g_i,m}$$

where $\phi_{g_i,m}(g) = m$ if $g = g_i^{-1}$ and $\phi_{g_i,m}(g) = 0$ if $g \neq g_i^{-1}$.

We have,

$$\begin{gathered} \beta' \left(\left(\sum_{i=1}^{n} n_i g_i + \sum_{i=1}^{n} n_i' g_i \right), m \right) = \beta' \left(\left(\sum_{i=1}^{n} (n_i + n_i') g_i \right), m \right) \\ = \sum_{i=1}^{n} (n_i + n_i') \phi_{g_i,m} = \beta' \left(\sum_{i=1}^{n} n_i g_i, m \right) + \beta' \left(\sum_{i=1}^{n} n_i' g_i, m \right) \end{gathered} \tag{2.4}$$

Moreover, for any $m, m' \in M$, $\phi_{g_i,m+m'}(g) = m+m'$ if $g = (g_i)^{-1}$ and $\phi_{g_i,m+m'}(g) = 0$ if $g \neq (g_i)^{-1}$.

Thus $\phi_{g_i,m+m'} = \phi_{g_i,m} + \phi_{g_i,m'}$ for any $m, m' \in M$.

Therefore,

$$\begin{gathered} \beta' \left(\sum_{i=1}^{n} n_i g_i, m + m' \right) = \sum_{i=1}^{n} n_i \phi_{g_i,m+m'} = \sum_{i=1}^{n} n_i (\phi_{g_i,m} + \phi_{g_i,m'}) \\ = \sum_{i=1}^{n} n_i \phi_{g_i,m} + \sum_{i=1}^{n} n_i \phi_{g_i,m'} = \beta' \left(\sum_{i=1}^{n} n_i g_i, m \right) + \beta' \left(\sum_{i=1}^{n} n_i g_i, m' \right) \end{gathered} \tag{2.5}$$

Hence β' is a $\mathbb{Z}$-bilinear map and so it induces the linear map

$$\beta : \mathbb{Z}[G] \otimes_{\mathbb{Z}} M_0 \to Ind^G M_0$$

such that

$$\beta \left(\left(\sum_{i=1}^{n} n_i g_i \right) \otimes m \right) = \sum_{i=1}^{n} n_i \phi_{g_i,m}$$

The only thing left to prove is that α and β are inverses of each other.

We have,

$$(\alpha\circ\beta)\left(\left(\sum_{i=1}^{n} n_i g_i\right)\otimes m\right)=\alpha\left(\sum_{i=1}^{n} n_i\beta(g_i\otimes m)\right)=\sum_{i=1}^{n} n_i\alpha(\phi_{g_i,m})$$

and,

$$\alpha(\phi_{g_i,m})=\sum_{j=1}^{n} g_j\otimes\phi_{g_i,m}(g_j^{-1})=g_i\otimes m$$

since $\phi_{g_i,m}(g_j^{-1})\neq 0$ only if $g_i=(g_j^{-1})^{-1}$ i.e. if $g_i=g_j$ and $\phi_{g_i,m}(g_i^{-1})=m$.

Thus,

$$(\alpha\circ\beta)\left(\left(\sum_{i=1}^{n} n_i g_i\right)\otimes m\right)=\sum_{i=1}^{n} n_i(g_i\otimes m)=\left(\sum_{i=1}^{n} n_i g_i\right)\otimes m$$

and so $\alpha\circ\beta$ is the identity map.

Since β is a linear map,

$$(\beta\circ\alpha)(\psi)=\beta\left(\sum_{g\in G} g\otimes\psi(g^{-1})\right)=\sum_{g\in G}\beta(g\otimes\psi(g^{-1}))$$

Thus for any $g_0\in G$,

$$(\beta\circ\alpha)(\psi)(g_0)=\sum_{g\in G}\beta(g\otimes\psi(g^{-1}))(g_0)=\sum_{g\in G}\phi_{g,\psi(g^{-1})}(g_0)$$

Now, $\phi_{g,\psi(g^{-1})}(g_0)\neq 0$ only if $g^{-1}=g_0$ in which case it is equal to $\psi(g^{-1})=\psi(g_0)$.

Hence $(\beta\circ\alpha)(\psi)(g_0)=\psi(g_0)\ \forall\ g_0\in G$ and so $(\beta\circ\alpha)(\psi)=\psi\ \forall\ \psi\in Ind^G M_0$. Thus we have shown that $\beta\circ\alpha$ is also the identity map and so we are done. □

Remark 2. *Let M and N be G-modules. Then the rule*

$$g(m\otimes n)=gm\otimes gn$$

defines a G-module structure on $M\otimes_{\mathbb{Z}} N$. Let M_0 be M regarded as an abelian group. Then the map $\eta:\mathbb{Z}[G]\otimes_{\mathbb{Z}} M_0\to\mathbb{Z}[G]\otimes_{\mathbb{Z}} M$ such that $\sum_{i=1}^{r} n_i g_i\mapsto\sum_{i=1}^{r} n_i(g_i\otimes g_i m)$ is an isomorphism of G-modules.

Proof. Define the map

$$\eta_1':\mathbb{Z}[G]\times M_0\to\mathbb{Z}[G]\otimes_{\mathbb{Z}} M$$

such that

$$\eta_1'\left(\sum n_i g_i, m\right)=\sum n_i(g_i\otimes g_i m)$$

and

$$\eta_2':\mathbb{Z}[G]\times M\to\mathbb{Z}[G]\otimes_{\mathbb{Z}} M_0$$

such that

$$\eta_2'\left(\sum n_i g_i, m\right)=\sum n_i(g_i\otimes g_i^{-1} m)$$

Arguing in the same way as in the proof of Lemma 2, it is easy to check that both η_1' and η_2' are $\mathbb{Z}$-bilinear and thus induce the linear maps

$$\eta_1 : \mathbb{Z}[G] \otimes_{\mathbb{Z}} M_0 \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} M$$

such that

$$\eta_1 \left(\left(\sum n_i g_i \right) \otimes m \right) = \sum n_i (g_i \otimes g_i m)$$

and

$$\eta_2 : \mathbb{Z}[G] \otimes_{\mathbb{Z}} M \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} M_0$$

such that

$$\eta_2 \left(\left(\sum n_i g_i \right) \otimes m \right) = \sum n_i (g_i \otimes g_i^{-1} m)$$

Now we want to show that η_1 and η_2 are inverses of each other.

$$\begin{aligned} \eta_2 \left(\eta_1 \left(\left(\sum n_i g_i \right) \otimes m \right) \right) &= \eta_2 \left(\sum n_i (g_i \otimes g_i m) \right) = \sum n_i (\eta_2 (g_i \otimes g_i m)) \\ &= \sum n_i (g_i \otimes g_i^{-1} g_i m) = \sum n_i (g_i \otimes m) = \left(\sum n_i g_i \right) \otimes m \end{aligned} \tag{2.6}$$

Hence $\eta_2 \circ \eta_1$ is the identity. Similiarly $\eta_1 \circ \eta_2$ is also the identity. The only thing left to show is that η_1 is a G-module homomorphism.

For any $g \in G$,

$$\begin{aligned} \eta_1 \left(g \left(\left(\sum n_i g_i \right) \otimes m \right) \right) &= \eta_1 \left(\left(\sum n_i (g g_i) \right) \otimes m \right) = \sum n_i (g g_i \otimes g g_i m) \\ &= \sum n_i g (g_i \otimes g_i m) = g \left(\sum n_i (g_i \otimes g_i m) \right) = g \left(\eta_1 \left(\left(\sum n_i g_i \right) \otimes m \right) \right) \end{aligned} \tag{2.7}$$

Thus η_1 is a G-module isomorphism. □

Remark 3. *If G is a finite group and M is a G-module, then $\mathbb{Z}[G] \otimes_{\mathbb{Z}} M$ with the diagonal G-action becomes an induced module.*

Proof. It follows directly from Theorem 10 and Remark 2.

□

Theorem 11. *Let G be a finite group. A G-module M is induced if and only if there exists an abelian group $M_0 \subset M$ such that*

$$M = \bigoplus_{g \in G} g M_0$$

where the direct sum is as abelian groups.

Proof. If M is an induced G-module M, then by Theorem 10, we have

$$M \cong \mathbb{Z}[G] \otimes M_0$$

for some abelian group $M_0 \in M$. But we know that

$$\mathbb{Z}[G] = \bigoplus_{g \in G} g \mathbb{Z}$$

Therefore,

$$\mathbb{Z}[G] \otimes M_0 = \bigoplus_{g \in G} g\mathbb{Z} \otimes M_0 = \bigoplus_{g \in G} g(\mathbb{Z} \otimes M_0) \cong \bigoplus_{g \in G} gM_0$$

Thus

$$M = \bigoplus_{g \in G} gM_0$$

Conversely, let there exists an abelian group $M_0 \subset M$ such that

$$M = \bigoplus_{g \in G} gM_0$$

Label $G = \{g_1, ..., g_n\}$ and define the map

$$\eta_1 : Ind^G M_0 \to \bigoplus_{g \in G} gM_0$$

such that

$$\eta_1(\phi) = (g_1\phi(g_1^{-1}), ..., g_n\phi(g_n^{-1}))$$

Clearly η_1 is a homomorphism of abelian groups. We want to show that it is also a G-module homomorphism. For any $g \in G$, we have

$$\eta_1(g\phi) = (g_1(g\phi)(g_1^{-1}), ..., g_n(g\phi)(g_n^{-1})) = (g_1\phi(g_1^{-1}g), ..., g_n\phi(g_n^{-1}g))$$

and

$$g(\eta_1(\phi)) = g(g_1\phi(g_1^{-1}), ..., g_n\phi(g_n^{-1})) = (gg_1\phi(g_1^{-1}), ..., gg_n\phi(g_n^{-1}))$$

In the last term we should rearrange the terms so that g_1 comes in the first place, g_2 in the second and so on. Therefore,

$$\eta_1(g\phi) = (g_1\phi(g_{j_1}^{-1}), ..., g_n\phi(g_{j_n}^{-1}))$$

where g_{j_i} is given as $gg_{j_i} = g_i$ and so $g_{j_i}^{-1} = g_i^{-1}g$. Thus,

$$\eta_1(g\phi) = (g_1\phi(g_1^{-1}g), ..., g_n\phi(g_n^{-1}g))$$

Hence

$$\eta_1(g\phi) = g(\eta_1(\phi))$$

Thus we have shown that η_1 is a G-module homomorphism. Now define the map

$$\eta_2 : \bigoplus_{g \in G} gM_0 \to Ind^G M_0$$

such that $\eta_2(g_1m_1, ..., g_nm_n) = \phi$ where $\phi(g_i) = m_j$ and j is defined by $g_j = g_i^{-1}$.

It is straightforward to check that η_1 and η_2 are inverses of each other.

Hence η_1 is a G-module isomorphism and we are done. □

Theorem 12. *Let M be an induced G-module and H be a subgroup of M, then M is induced as a H-module. If H is normal in G, then M^H is an induced G/H module.*

Proof. Let $M = \bigoplus_{\sigma\in G} \sigma D$. Then,

$$M = \bigoplus_{\sigma\in H} \bigoplus_{\tau} \sigma\tau D = \bigoplus_{\sigma\in H} \sigma \left(\bigoplus_{\tau} \tau D \right)$$

where τ runs over a set of coset representatives of H in G. Hence M is also induced as an H-module.

Now we define an action of G/H on M^H as

$$(gH)m = gm$$

To show that it is well defined, we have to check that for any $g \in G$, $gm \in M^H$ if $m \in M^H$. But we have for any $h \in H$,

$$h(gm) = (hg)m = (gh_1)m = g(h_1 m) = gm$$

where in the second equality we have used that H is normal in G and in the last equality that $m \in M^H$. Thus we have shown that M^H is a G/H module. Since M is an induced G-module, therefore

$$M = \bigoplus_{\sigma\in G} \sigma D$$

for some abelian group $D \subset M$. By the previous theorem, it suffices to show that

$$M^H = \bigoplus_{\tau\in G/H} \tau(N_H(D))$$

Clearly $N_H(D) \subset M^H$ and so

$$\bigoplus_{\tau\in G/H} \tau(N_H(D)) \subset M^H$$

Conversely, suppose $m \in M^H$. Then m has a unique representation in the form

$$m = \sum_{\tau\in G} \tau d_\tau$$

with $d_\tau \in D$. For any $\sigma \in H$, we have

$$m = \sigma(m) = \sum_{\tau\in G} \sigma\tau d_\tau$$

since $m \in M^H$. But note that we can also write

$$m = \sum_{\tau\in G} \tau d_\tau = \sum_{\tau\in G} \sigma\tau d_{\sigma\tau}$$

since as τ runs over G so does $\sigma\tau$. Thus by uniqueness of the expression for m, we get

$$d_\tau = d_{\sigma\tau}$$

for all $\sigma \in H$ and all $\tau \in G$. Since H is normal in G, so $= \tau\sigma = \sigma_1\tau$ for some $\sigma_1 \in H$ and so we get

$$d_{\tau\sigma} = d_\tau$$

for all $\sigma \in H$ and all $\tau \in G$. Thus we have

$$m = \sum_{\tau \in G} \tau d_\tau = \sum_{\tau \in S} \sum_{\sigma \in H} \tau\sigma d_{\tau\sigma} = \sum_{\tau \in S} \sum_{\sigma \in H} \tau\sigma d_\tau = \sum_{\tau \in S} \tau \left(\sum_{\sigma \in H} \sigma d_\tau \right) = \sum_{\tau \in S} \tau N_H(d_\tau)$$

and so

$$M^H \subset \bigoplus_{\tau \in G/H} \tau(N_H(D))$$

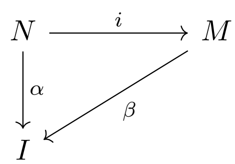
Thus

$$M^H = \bigoplus_{\tau \in G/H} \tau(N_H(D))$$

and we are done. □

INJECTIVE G-MODULES

A G-module I is said to be injective if every G-module homomorphism from a submodule of a G-module extends to the whole module. In other words, if N is a submodule of a G-module M, then every homomorphism $\alpha : N \to I$ extends to M i.e. there is a G-module homomorphism $\beta : M \to I$ such that the following diagram commutes :



(2.8)

Equivalently, I is injective if $Hom(\ ,I)$ is an exact functor.

Lemma 3. *Every abelian group can be embedded into an injective abelian group*

Proof. For an abelian group M, let $M^V = Hom(M, \mathbb{Q}/\mathbb{Z})$; choose a free abelian group F mapping onto M^V ; then M emebeds into M^{VV} which embeds into F^V. Hence M embeds into F^V which is an injective abelian group because it is the dual of a projective $\mathbb{Z}$-module since free modules are projective and dual of projective modules is injective. (Projective modules will be discussed in the section on Homology) □

Theorem 13. *Every G-module M can be embedded into an injective G-module.*

Proof. Let M_0 be M regarded as an abelian group. By Lemma 3, M_0 can be embedded into I. Then $Ind^G M_0$ can be embedded into $Ind^G I$ since Ind^G takes exact sequences to exact sequences and thus injective maps to injective maps. We also know that M_0 embeds into $Ind^G M_0$ through the map $m \mapsto \phi_m$ where $\phi_m(g) = gm$. Hence M embeds into $Ind^G I$. It only remains to show that $Ind^G I$ is an injective module if I is an injective abelian group. We prove a slightly general result in the next Lemma. □

Lemma 4. *If I is an injective H-module, then $Ind_H^G I$ is an injective G-module.*

Proof. We know by Frobenius Reciprocity (Theorem 8),

$$Hom_G(M, Ind_H^G I) \cong Hom_H(M, I)$$

as abelian groups. Let

$$0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$$

be an exact sequence of G-modules. Since I is an injective H-module, the following sequence is exact :

$$0 \to Hom_H(M', I) \xrightarrow{\alpha'} Hom_H(M, I) \xrightarrow{\beta'} Hom_H(M'', I) \to 0$$

It is straightforward to check that the following diagram commutes :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Hom_H(M', I) & \xrightarrow{\alpha'} & Hom_H(M, I) & \xrightarrow{\beta'} & Hom_H(M'', I) & \longrightarrow & 0 \\ & & \downarrow{\eta_1} & & \downarrow{\eta_2} & & \downarrow{\eta_3} & & \\ 0 & \longrightarrow & Hom_G(M', Ind_H^G I) & \xrightarrow{\alpha''} & Hom_G(M, Ind_H^G I) & \xrightarrow{\beta''} & Hom_G(M'', Ind_H^G I) & \longrightarrow & 0 \end{array} \tag{2.9}$$

This shows that the sequence

$$0 \to Hom_G(M', Ind_H^G I) \xrightarrow{\alpha''} Hom_G(M, Ind_H^G I) \xrightarrow{\beta''} Hom_G(M'', Ind_H^G I) \to 0$$

is exact as well. Hence $Hom_G(., Ind_H^G I)$ is an exact functor and so $Ind_H^G I$ is an injective G-module. □

2.3 Definition of Cohomology Groups

For a G-module M, define $M^G = \{m \in M : gm = m \ \forall \ g \in G\}$

Lemma 5. *If*

$$0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$$

is exact, then

$$0 \to M'^G \xrightarrow{\alpha'} M^G \xrightarrow{\beta'} M"^G$$

is also exact where α' and β' are just the restriction maps of α and β respectively.

Proof. Firstly we need to show that $\alpha(M'^G) \subset M^G$ and $\beta(M^G) \subset M"^G$ in order to show that α' and β' are well defined.

Let $m \in M'^G$, then $gm = m \ \forall \ g \in G$. Since α is a G-module homomorphism, so

$$g(\alpha(m)) = \alpha(gm) = \alpha(m)$$

and thus $\alpha(m) \in M^G$. Similarly we can show $\beta(M^G) \subset M"^G$.

Since α is injective and α' is just the restriction of α, so α' is also injective.

We also know that $\beta' \circ \alpha' = 0$ since $\beta \circ \alpha = 0$. Thus $Im(\alpha') \subset Ker(\beta')$. Now let $m \in Ker(\beta')$ i.e.

$m \in M^G$ such that $\beta(m) = 0$, thus $m \in Ker(\beta) = Im(\alpha)$ i.e. $m = \alpha(m')$ for some $m' \in M'$. We need to show that $m' \in M'^G$. For any $g \in G$,

$$\alpha(gm') = g\alpha(m') = gm = m$$

since $m \in M^G$. Thus

$$\alpha(gm') = m = \alpha(m')$$

Then injectivity of α shows that $gm' = m' \ \forall \ g \in G$, so $m' \in M'^G$ and we are done.

□

An injective resolution of a G-module M is a long exact sequence

$$0 \to M \to I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \to ... I^r \xrightarrow{d^r} I^{r+1} \to ...$$

such that I^i is an injective module for each $i \geq 0$.

Theorem 14. *For a G-module M, there exists an injective resolution of M.*

Proof. By Lemma 3, there is an exact sequence

$$0 \to M \xrightarrow{\alpha^0} I^0$$

for some injective module I^0. Let B^1 be the cokernel of α_0. Again by Lemma 3, B^1 can be embedded into an injective module I^1. Then the sequence

$$0 \to M \xrightarrow{\alpha^0} I^0 \xrightarrow{\alpha^1} I^1$$

is exact. Now let $B^2 = coker(\alpha^1)$ and continue in this fashion.

□

Now let M be a G-module, and choose an injective resolution

$$0 \to M \to I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \xrightarrow{d^2} ...$$

of M. By Lemma 5, we know that there are restriction maps of d^r(which we again denote by d^r) i.e. $(I^r)^G \xrightarrow{d^r} (I^{r+1})^G$ for all $r \geq 0$. Then,

$$0 \xrightarrow{d^{-1}} (I^0)^G \xrightarrow{d^0} (I^1)^G \to ... \xrightarrow{d^{r-1}} (I^r)^G \xrightarrow{d^r} (I^{r+1})^G \to ...$$

is still a complex i.e. $d^i \circ d^{i-1} = 0 \ \forall \ i \geq 0$. However it need no longer be an exact sequence and we define the r^{th} cohomology group of G to be

$$H^r(G, M) = \frac{Ker(d^r)}{Im(d^{r-1})}$$

Theorem 15. *$H^r(G, M)$ is independent of the choice of the injective resolution (upto an isomorphism) and is thus well-defined.*

Proof. See Appendix A.3, [10]. □

Cohomology groups have the following basic properties :

Lemma 6. $H^0(G,M) \cong M^G$

Proof. We know by Lemma 5 that the sequence

$$0 \to M^G \xrightarrow{i} (I^0)^G \xrightarrow{d^0} (I^1)^G$$

is exact, and thus

$$H^0(G,M) = \frac{Ker(d^0)}{Im(d^{-1})} = Ker(d^0) = Im(i) \cong M^G$$

since $Im(d^{-1}) = 0$ and i is injective. □

Lemma 7. *If I is an injective G-module, then $H^r(G,I) = 0$ for all $r > 0$*

Proof. Firstly observe that 0 is an injective module because if N is a submodule of a G-module M, then any homomorphism $\alpha : N \to 0$ can clearly be extended to a homomorphism $\beta : M \to 0$. Then,

$$0 \to I \xrightarrow{id} I \to 0 \to 0 \to ...$$

is an injective resolution of I. The resulting cohomology complex becomes

$$0 \xrightarrow{d^{-1}} I^G \xrightarrow{d^0} 0 \xrightarrow{d^1} 0 \to ...$$

Then $Ker(d^r) = 0 \;\forall\; r > 0$ and $Im(d^{r-1}) = 0 \;\forall\; r > 0$. Thus $H^r(G,I) = 0 \;\forall\; r > 0$.

□

2.4 Description of Cohomology Groups by means of Cochains

Let P_r be the free $\mathbb{Z}$-module with basis the $(r+1)$-tuples $(g_0, g_1, ..., g_r)$ of elements of G. Define the action of G on P_r as

$$g(g_0, g_1, ..., g_r) = (gg_0, gg_1, ..., gg_r)$$

Define a map $d_r : P_r \to P_{r-1}$ by the rule that

$$d_r(g_0, g_1, ..., g_r) = \sum_{i=0}^{r} (-1)^i (g_0, ...\hat{g}_i, ..., g_r)$$

where the symbol $\hat{g}_i$ means that g_i is omitted. Then d_r is a homomorphism of G-modules.

Lemma 8. $d^{r-1} \circ d^r = 0 \;\forall\; r \geq 1$

Proof.

$$d^r(g_0, g_1, ..., g_r) = \sum_{i=0}^{r} (-1)^i (g_0, ..., \hat{g}_i, ..., g_r) = \sum_{i=0}^{r} (-1)^i (G_0, ..., G_{r-1})$$

where $G_j = g_j$ if $j < i$ and $G_j = g_{j+1}$ if $j \geq i$.

Hence

$$d^{r-1}(d^r(g_0, g_1, ..., g_r)) = \sum_{i=0}^{r} (-1)^i d^r(G_0, ..., G_{r-1}) = \sum_{i=0}^{r} (-1)^i \sum_{j=0}^{r-1} (-1)^j (G_0, .., .\hat{G}_j, .., G_{r-1})$$

Note that

$$(G_0, .., .\hat{G}_j, .., G_{r-1}) = (g_0, ..., \hat{g}_j, ...\hat{g}_i, ..., g_r)$$

if $j < i$ and

$$(G_0, .., .\hat{G}_j, .., G_{r-1}) = (g_0, ..., \hat{g}_i, ...\hat{g}_{j+1}, ..., g_r)$$

if $j \geq i$. Thus

$$\sum_{j=0}^{r-1}(G_0, .., \hat{G}_j, .., G_{r-1}) = \sum_{j=0}^{i-1}(g_0, ..., \hat{g}_j, ...\hat{g}_i, ..., g_r) + \sum_{j=i}^{r-1}(g_0, ..., \hat{g}_i, ...\hat{g}_{j+1}, ..., g_r)$$

Therefore,

$$d^{r-1}(d^r(g_0, g_1, ..., g_r)) = \sum_{i=0}^{r}\sum_{j=0}^{i-1}(-1)^{i+j}(g_0, ..., \hat{g}_j, ..., \hat{g}_i, ...g_r) \ + \ \sum_{i=0}^{r}\sum_{j=i}^{r-1}(-1)^{i+j}(g_0, ..., \hat{g}_i, ...\hat{g}_{j+1}, ..., g_r)$$

We should change index in the second summation by taking $j + 1 = J$ and thus

$$\sum_{i=0}^{r}\sum_{j=i}^{r-1}(-1)^{i+j}(g_0, ..., \hat{g}_i, ...\hat{g}_{j+1}, ..., g_r) = \sum_{i=0}^{r}\sum_{J=i+1}^{r}(-1)^{i+J}(g_0, ..., \hat{g}_i, ...\hat{g}_J, ..., g_r)$$

Hence the previous equation can be rewritten as

$$d^{r-1}(d^r(g_0, g_1, ..., g_r)) = \sum_{i=0}^{r}\sum_{j<i}(-1)^{i+j}(g_0, ..., \hat{g}_i, ..., \hat{g}_j, ...g_r) \ - \ \sum_{i=0}^{r}\sum_{j>i}(-1)^{i+j}(g_0, ..., \hat{g}_i, ..., \hat{g}_j, ...g_r)$$

To prove that the RHS is zero, it suffices to show that

$$\{\{i, j\} : 0 \leq i, j \leq r \ \ and \ \ i < j\} = \{\{i, j\} : 0 \leq i, j \leq r \ \ and \ \ j < i\}$$

which is obvious. □

Let $\epsilon : P_0 \to \mathbb{Z}$ be the map such that $g \mapsto 1 \ \forall \ g \in G$

Lemma 9. *The complex*

$$...P_r \xrightarrow{d_r} P_{r-1} \to ... \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

is exact.

Proof. Firstly we need to show that this is indeed a complex. After Lemma 8, we only have to prove that $\epsilon \circ d_1 = 0$. But we find that

$$\epsilon(d_1(g_0, g_1)) = \epsilon(g_1 - g_0) = \epsilon(g_1) - \epsilon(g_0) = 1 - 1 = 0$$

Thus it is indeed a complex. To show that it is exact as well, we need to prove that $Ker(d_r) \subset Im(d_{r+1})$ for all $r \geq 1$.

Choose any element $o \in G$, and define the map

$$k_r : P_r \to P_{r+1}$$

such that

$$k_r(g_0, g_1, ..., g_r) = (o, g_0, g_1, ..., g_r)$$

We want to show that $d_{r+1} \circ k_r + k_{r-1} \circ d_r$ is the identity function. Let $(g_0, g_1, ..., g_r) \in P_r$. Then

$$k_r(g_0, g_1, ..., g_r) = (o, g_0, g_1, ..., g_r) = (G_0, G_1, ..., G_{r+1})$$

where $G_0 = o$ and $G_i = g_{i-1}$ for $i \geq 1$. We have

$$\begin{aligned} d_{r+1}(G_0, ..., G_{r+1}) &= \sum_{i=0}^{r+1}(-1)^i(G_0, ..., \hat{G}_i, ..., G_{r+1}) = (G_0, ..., G_{r+1}) + \sum_{i=1}^{r+1}(-1)^i(G_0, G_1, ..., \hat{G}_i, ..., G_{r+1}) \\ &= (g_0, ..., g_r) + \sum_{i=1}^{r+1}(-1)^i(o, g_0, ..., \hat{g}_{i-1}, ..., g_r) = (g_0, ..., g_r) - \sum_{i=0}^{r}(-1)^i(o, g_0, ..., \hat{g}_i, .., g_r) \end{aligned} \tag{2.10}$$

Thus

$$d_{r+1}(k_r(g_0, g_1, ..., g_r)) = (g_0, ..., g_r) - \sum_{i=0}^{r}(-1)^i(o, g_0, ..., \hat{g}_i, .., g_r)$$

Now we have

$$\begin{aligned} k_{r-1}(d_r(g_0, ..., g_r)) &= k_{r-1}\left(\sum_{i=0}^{r}(-1)^i(g_0, ..., \hat{g}_i, ..., g_r)\right) \\ &= \sum_{i=0}^{r}(-1)^i k_{r-1}(g_0, ..., \hat{g}_i, ..., g_r) = \sum_{i=0}^{r}(-1)^i(o, g_0, ..., \hat{g}_i, ..., g_r) \end{aligned} \tag{2.11}$$

Therefore,

$$d_{r+1}(k_r(g_0, g_1, ..., g_r)) + k_{r-1}(d_r(g_0, ..., g_r)) = (g_0, g_1, ..., g_r)$$

and so $d_{r+1} \circ k_r + k_{r-1} \circ d_r$ is the identity function.

Now if $x \in Ker(d_r)$, then $x = d_{r+1}(k_r(x)) \in Im(d_{r+1})$ and so we are done.

□

Define the maps

$$d'_r : Hom_G(P_r, M) \to Hom_G(P_{r+1}, M)$$

such that

$$d'_r(\phi) = \phi \circ d_{r+1}$$

Theorem 16. *For every G-module M,*

$$H^r(G, M) \cong H^r(Hom_G(P_\bullet, M))$$

Proof. This follows from the general theory of Ext groups and right derived functors (See Example $A.14$, page 93, [1]).

□

Let $\bar{C}^r(G, M)$ denote the abelian group

$$\{\phi : G^{r+1} \to M \ : \ \phi(gg_0, ..., gg_r) = g(\phi(g_0, ..., g_r)) \ \forall \ g, g_0, ..., g_r \in G\}$$

The elements of $\bar{C}^r(G, M)$ are called homogeneous r-cochains of G with values in M.

Lemma 10. $Hom_G(P_r, M) \cong \bar{C}^r(G, M)$ *as abelian groups.*

Proof. Recall that P_r is a free $\mathbb{Z}$-module with basis G^{r+1}.

Define the map $\eta_r : Hom_G(P_r, M) \to \bar{C}^r(G, M)$ such that

$$\eta_r(\psi) = \psi \restriction_{G^{r+1}}$$

and the map

$$\kappa_r : \bar{C}^r(G, M) \to Hom_G(P_r, M)$$

such that

$$(\kappa_r(\phi)) \left(\sum_i n_i(g_0, ..., g_r) \right) = \sum_i n_i \phi(g_0, ..., g_r)$$

Then we can proceed as in Lemma 2 to show that κ_r is well-defined and that η_r and κ_r are inverses of each other. □

It is straightforward to check that there is a commutative diagram :

$$\begin{array}{ccc} Hom_G(P_r, M) & \xrightarrow{d'_r} & Hom_G(P_{r+1}, M) \\ \downarrow{\eta_r} & & \downarrow{\eta_{r+1}} \\ \bar{C}^r(G, M) & \xrightarrow{\bar{d}^r} & \bar{C}^{r+1}(G, M) \end{array} \tag{2.12}$$

Therefore, we have

$$\frac{Ker(d_r)}{Im(d'_{r-1})} \cong \frac{Ker(\bar{d}^r)}{Im(\bar{d}^{r-1})}$$

This combined with Theorem 16 shows that

$$H^r(G, M) \cong H^r(Hom_G(P_\bullet, M)) = \frac{Ker(d_r)}{Im(d'_{r-1})} \cong \frac{Ker(\bar{d}^r)}{Im(\bar{d}^{r-1})}$$

Hence we have proven the following the following theorem :

Theorem 17. $H^r(G, M) \cong \frac{Ker(\bar{d}^r)}{Im(\bar{d}^{r-1})}$

Let $C^r(G, M)$ denote the set of functions $\{\phi : G^r \to M\}$ which is an abelian group under addition of functions. The elements of $C^r(G, M)$ are called the inhomogeneous r-cochains of G with values in M. Set the convention $G^0 = \{1\}$ and so $C^0(G, M) = M$.

Define the map

$$d^0 : C^0(G, M) \to C^1(G, M)$$

such that

$$(d^0 m)(g) = gm - m$$

and for any $r > 0$,

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

such that

$$(d^r(\phi)(g_1, g_2, ..., g_{r+1}) = g_1\phi(g_2, ..., g_{r+1}) + \sum_{j=1}^{r}(-1)^j \phi(g_1, ..., g_j g_{j+1}, ..., g_{r+1}) + (-1)^{r+1}\phi(g_1, ..., g_r)$$

Lemma 11. $\bar{C}^r(G, M) \cong C^r(G, M)$

Proof. Define the map $\beta_r : \bar{C}^r(G, M) \to C^r(G, M)$ such that

$$\beta_r(\psi)(g_1, ..., g_r) = \psi(1, g_1, g_1g_2, ..., g_1g_2...g_r)$$

Then β_r is clearly a homomorphism of abelian groups. Now we will show that β_r is injective. Let $\psi(1, g_1, g_1g_2, ..., g_1g_2...g_r) = 0$ for all $g_1, ..., g_r \in G$. Then for any $g_1, ..., g_r \in G$, let $G_1 = g_1^{-1}g_2$, $G_2 = g_2^{-1}g_3, ..., G_r = g_{r-1}^{-1}g_r$.

Since $\psi \in \bar{C}^r(G, M)$, so we have

$$\psi(g_1, ...g_r) = g_1g_2...g_r\psi(1, G_1, G_2, ..., G_r) = 0$$

Thus $\psi = 0$ and we get that the map β_r is injective. A similar argument shows that β_r is also surjective.

□

It is straightforward to show that the following diagram commutes :

$$\begin{array}{ccc} \bar{C}^r(G, M) & \xrightarrow{\bar{d}^r} & \bar{C}^{r+1}(G, M) \\ \downarrow \beta_r & & \downarrow \beta_{r+1} \\ C^r(G, M) & \xrightarrow{d^r} & C^{r+1}(G, M) \end{array} \tag{2.13}$$

This lemma shows that

$$\frac{Ker(\bar{d}^r)}{Im(\bar{d}^{r-1})} \cong \frac{Ker(d^r)}{Im(d^{r-1})}$$

Combined with Theorem 17, we get

$$H^r(G, M) \cong \frac{Ker(d^r)}{Im(d^{r-1})}$$

Define

$$Z^r(G, M) = Ker(d^r)$$

This is known as the group of r-cocycles. Also, define

$$B^r(G, M) = Im(d^{r-1})$$

This is known as the group of r-coboundaries.

DESCRIPTION OF $H^1(G, M)$

A map $\phi : G \to M$ is said to be a crossed homomorphism if $\forall\ \sigma, \tau \in G$,

$$\phi(\sigma\tau) = \sigma\phi(\tau) + \phi(\sigma)$$

In particular the condition implies that, for e the identity element of G,

$$\phi(e) = \phi(ee) = e\phi(e) + \phi(e) = 2\phi(e)$$

and so $\phi(e) = 0$. For every $m \in M$, the map $\sigma \mapsto \sigma m - m$ is a crossed homomorphism since

$$\phi(\sigma\tau) = (\sigma\tau)m - m = (\sigma(\tau m) - \sigma m) + (\sigma m - m) = \sigma(\tau(m) - m) + (\sigma m - m) = \sigma(\phi(\tau)) + \phi(\sigma)$$

and is called a principal crossed homomorphism.

Note that

$$(d^1(\phi))(\sigma, \tau) = \sigma(\phi(\tau) - \phi(\sigma\tau) + \phi(\sigma, \tau)$$

and

$$(d^0(m))(\sigma) = \sigma m - m$$

for some $m \in M$. Thus ϕ is a crossed homomorphism $\Leftrightarrow d^1(\phi) = 0 \Leftrightarrow \phi \in Ker(d^1)$.

Hence $Ker(d^1) = \{$crossed homomorphisms $G \to M\}$.

Moreover, ψ is a principal crossed homomorphism $\Leftrightarrow \psi = d^0(m)$ for some $m \in M \Leftrightarrow \psi \in Im(d^0)$.

Hence $Im(d^0) = \{$ principal crossed homomorphisms $G \to M\}$.

Therefore, $H^1(G, M) = \frac{Ker(d^1)}{Im(d^0)} = \frac{\{crossed\ homomorphisms\ G \to M\}}{\{principal\ crossed\ homomorphisms\ G \to M\}}$

If the action of G on M is trivial , then crossed homomorphisms become homomorphisms (as abelian groups) since

$$\phi(\sigma\tau) = \sigma\phi(\tau) + \phi(\sigma) = \phi(\tau) + \phi(\sigma) = \phi(\sigma) + \phi(\tau)$$

and principal crossed homomorphisms are zero since

$$\phi(\sigma) = \sigma(m) - m = m - m = 0$$

Thus, in this case

$$H^1(G, M) \cong Hom_{\mathbb{Z}}(G, M)$$

Theorem 18. *A short exact sequence*

$$0 \to M' \to M \to M'' \to 0$$

of G-modules gives rise to a long exact sequence

$$0 \to H^0(G, M') \to H^0(G, M) \to ... \to H^r(G, M') \to H^r(G, M) \to H^r(G, M'') \xrightarrow{\delta^r} H^{r+1}(G, M') \to ...$$

Proof. See Theorem 1.2.11, page 9, [6]. □

Remark 4. *Let*

$$0 \to M \xrightarrow{i} N \xrightarrow{\pi} P \to 0$$

be an exact sequence of G-modules. The proof of Theorem 18 *shows that the boundary map*

$$\delta^r : H^r(G, P) \to H^{r+1}(G, M)$$

has the following description :

Let $\gamma \in H^r(G,P)$ be represented by the r-cocycle $\phi : G^r \to P$. Since π is a surjective map, we can choose a lift $\phi' : G^r \to N$ of ϕ i.e. ϕ' is a map such that

$$\pi(\phi'(g_1,...,g_r)) = \phi(g_1,...,g_r)$$

Since ϕ is a r-cocycle, $d^r(\phi) = 0$ and so

$$\pi(d^r(\phi'(g_1,...,g_r))) = d^r(\pi(\phi'(g_1,...,g_r))) = d^r(\phi(g_1,...,g_r)) = 0$$

where in the second equality, we have used that π is a G-module homomorphism. Moreover, we have $Ker(\pi) = Im(i)$ and so $d^r(\phi'(g_1,...,g_r)) \in M$. Then, $d^r(\phi')$ is the cocycle representing $\delta^r(\gamma)$.

2.5 Shapiro's Lemma

Let M be a G-module, and regard $\mathbb{Z}$ as a G-module with trivial action i.e. $gm = m \ \forall \ g \in G$, $m \in \mathbb{Z}$.

Lemma 12. $Hom_G(\mathbb{Z}, M) \cong M^G$

Proof. Define the map

$$\eta_1 : Hom_G(\mathbb{Z}, M) \to M^G$$

such that

$$\eta_1(\phi) = \phi(1)$$

$\eta_1(\phi) \in M^G$ because for any $g \in G$, we have

$$(g\phi(1)) = \phi(g1) = \phi(1)$$

The first equality holds because ϕ is a G-module homomorphism and the second equality holds because G has trivial action on $\mathbb{Z}$.

Clearly η_1 is a homomorphism of abelian groups. It is also a G-module map since

$$\eta_1(g\phi) = (g\phi)(1) = g(\phi(g^{-1}1)) = g(\phi(1)) = g(\eta_1(\phi))$$

In the second equality we have used the action of G on $Hom_G(\mathbb{Z}, M)$ and in the third equality we have used that G has trivial action on $\mathbb{Z}$.

Now define

$$\eta_2 : M^G \to Hom_G(\mathbb{Z}, M)$$

such that

$$\eta_2(m)(k) = km$$

Moreover, $\eta_1(\eta_2(m)) = (\eta_2(m))(1) = m$ Thus $\eta_1(\eta_2(m)) = m$ and we have $\eta_1 \circ \eta_2$ is the identity map.

Also, $\eta_2(\eta_1(\phi))(k) = \eta_2(\phi(1))(k) = k\phi(1) = \phi(k)$. Thus $\eta_2(\eta_1(\phi)) = \phi$ and we have $\eta_2 \circ \eta_1$ is the identity map.

Hence η_1 is a G-module isomorphism. □

Remark 5. $H^0(G, M) \cong Hom_G(Z, M)$

Proof. It follows directly from Lemma 6 and Lemma 12. □

Theorem 19. *(Shapiro's Lemma) Let H be a subgroup of G. For every H-module N, there is a canonical isomorphism*

$$H^r(G, Ind_H^G(N)) \to H^r(H, N)$$

for all $r \geq 0$.

Proof. Firstly we prove it for the case $r = 0$. By Theorem 8, we know that

$$Hom_G(\mathbb{Z}, Ind_H^G(N)) \cong Hom_H(\mathbb{Z}, N)$$

This, combined with Remark 5 gives us that

$$H^0(G, Ind_H^G(N)) \cong H^0(H, N)$$

and we are done for this case. Now let $r > 0$.

Choose an injective resolution of N

$$0 \to M \to I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \to \dots I^r \xrightarrow{d^r} I^{r+1} \to \dots$$

where each I^r is an injective H module. Since Ind_H^G is an exact functor by Theorem 9, so

$$0 \to Ind_H^G(N) \to Ind_H^G(I^0) \to Ind_H^G(I^1) \to \dots Ind_H^G(I^r) \to Ind_H^G(I^{r+1}) \to \dots$$

is an exact sequence. We also know that if I is an injective H-module, then $Ind_H^G(I)$ is an injective G-module. Thus this sequence is an injective resolution of $Ind_H^G(N)$. Then the corresponding cohomology sequence becomes

$$0 \xrightarrow{d^{-1}} (Ind_H^G(I^0))^G \xrightarrow{d^0} (Ind_H^G(I^1))^G \to \dots (Ind_H^G(I^r))^G \xrightarrow{d^r} (Ind_H^G(I^{r+1}))^G \to \dots$$

We also know that the cohomology sequence for N is

$$0 \xrightarrow{d^{-1}} (I^0)^G \xrightarrow{d^0} (I^1)^G \xrightarrow{d^1} (I^2)^G \to \dots$$

Thus we get a diagram which can be shown to be commutative by direct verification :

$$\begin{array}{ccccc} (Ind_H^G(I^{r-1}))^G & \xrightarrow{d'^{r-1}} & (Ind_H^G(I^r))^G & \xrightarrow{d'^r} & (Ind_H^G(I^{r+1}))^G \\ \downarrow{\scriptstyle \eta_{r-1}} & & \downarrow{\scriptstyle \eta_r} & & \downarrow{\scriptstyle \eta_{r+1}} \\ (I^{r-1})^G & \xrightarrow{d^{r-1}} & (I^r)^G & \xrightarrow{d^r} & (I^{r+1})^G \end{array} \tag{2.14}$$

where the vertical maps η_i are isomorphisms given by the case $r = 0$ above. The commutativity of the diagram gives us

$$\frac{Ker(d'^r)}{Im(d'^{r-1})} \cong \frac{Ker(d^r)}{Im(d^{r-1})}$$

and thus

$$H^r(G, In_H^G(N)) \cong H^r(H, N)$$

This completes the proof of Shapiro's Lemma. □

Corollary 2. *If M is an induced G-module, then $H^r(G, M) = 0$ for all $r > 0$.*

Proof. Since M is an induced G-module, so $M \cong Ind^G(M_0)$ for some abelian group M_0. Then

$$H^r(G, Ind^G(M_0)) \cong H^r(\{1\}, M_0)$$

To complete the proof of the corollary, we need the following lemma. □

Lemma 13. *If $G = \{1\}$ and M is an abelian group (hence also a G-module), then $H^r(G, M) = 0$*

Proof. Let

$$0 \to M \to I^0 \to I^1 \to ...$$

be an injective resolution of M. In our case, $G = \{1\}$ and $M^G = M$ for any abelian group M. Thus the cohomology sequence

$$0 \xrightarrow{d^{-1}} (I^0)^G \xrightarrow{d^0} (I^1)^G \xrightarrow{d^1} (I^2)^G \to ...$$

simply becomes

$$0 \xrightarrow{d^{-1}} I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \to ...$$

Since

$$I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \to ...$$

is a part of the injective resolution and thus is exact, so $Ker(d^r) = Im(d^{r-1})$ whenever $r > 0$ (though not for $r = 0$) and thus $H^r(G, M) = 0$ whenever $r > 0$. □

Remark 6. *Consider the exact sequence*

$$0 \to M \to J \to N \to 0$$

of G-modules. If $H^r(G, J) = 0$ for all $r > 0$, then

$$H^r(G, N) \cong H^{r+1}(G, M)$$

for all $r \geq 1$.

Proof. The cohomology sequence (Theorem 18) gives the exact sequence

$$... \to H^r(G, J) \to H^r(G, N) \to H^{r+1}(G, M) \to H^{r+1}(G, J) \to ...$$

for each $r \geq 0$. But we are given that $H^r(G, J) = 0$ for all $r \geq 1$. Thus we get the exact sequence

$$0 \to H^r(G, N) \xrightarrow{\delta_r} H^{r+1}(G, M) \to 0$$

for each $r \geq 1$. The exactness of the sequence shows us that $Ker(\delta_r) = 0$ and $Im(\delta_r) = H^{r+1}(G, M)$ which show that δ_r is injective and surjective respectively. Hence δ_r is an isomorphism and we get

$$H^r(G, N) \cong H^{r+1}(G, M)$$

for all $r \geq 1$.

□

Let M be a G-module and M_0 be M regarded as an abelian group. We know that M can be embedded into $Ind^G M_0$ through the map $M \to Ind^G(M_0)$ given by $m \mapsto \phi_m$ where $\phi_m(g) = gm$. Let's denote $Ind^G(M_0)$ by M_* and define $M_\dagger = M_*/M$. Then we get the exact sequence

$$0 \to M \to M_* \to M_\dagger \to 0$$

Thus by Remark 6, we find that

$$H^r(G, M_\dagger) \cong H^{r+1}(G, M)$$

2.6 Cohomology of finite Galois extensions

2.6.1 Hilbert's Theorem 90

Let L be a finite Galois extension of a field K, and let $G = Gal(L/K)$. Then L, regarded as a group under addition is a G-module. L^*, regarded as a group under multiplication is also a G-module.

Theorem 20. *(Hilbert's Theorem 90) Let L/K be a finite Galois extension with Galois group G. Then $H^1(G, L^*) = 0$.*

Proof. Let $\phi : G \to L^*$ be a crossed homomorphism. In multiplicative notation, this means that for all $\sigma, \tau \in G$,

$$\phi(\sigma\tau) = \sigma(\phi(\tau))\phi(\sigma)$$

For any $a \in L^*$, let

$$b = \sum_{\sigma \in G} \phi(\sigma)(\sigma a)$$

Suppose $b \neq 0$. Then

$$\tau(b) = \tau\left(\sum_{\sigma \in G} \phi(\sigma)(\sigma a)\right) = \sum_{\sigma \in G} \tau(\phi(\sigma)(\sigma a)) = \sum_{\sigma \in G} \tau(\phi(\sigma))\tau(\sigma a) = \sum_{\sigma \in G} (\phi(\tau))^{-1}\phi(\tau\sigma)((\tau\sigma)(a))$$

where the last equality holds because

$$\phi(\tau\sigma) = \tau(\phi(\sigma))\ (\phi(\tau))$$

since ϕ is a crossed homomorphism. But then

$$\tau(b) = (\phi(\tau))^{-1} \sum_{\sigma \in G} \phi(\tau\sigma)((\tau\sigma)(a)) = (\phi(\tau))^{-1} \sum_{\sigma \in G} \phi(\sigma)(\sigma(a)) = (\phi(\tau))^{-1} b$$

where the second equality holds because as σ runs over G, so does $\tau\sigma$ for any $\tau \in G$.
Thus, $\tau(b) = (\phi(\tau))^{-1} b$ and so

$$\phi(\tau) = \frac{b}{\tau(b)} = \frac{\tau(b^{-1})}{b^{-1}}$$

+ which shows that ϕ is a principal crossed homomorphism and we are done.

The only thing left to be shown is that $\exists\ a \in L^*$ for which $b \neq 0$. Let's assume to the contrary that $b = 0$ for all $a \in L^*$. i.e. $\sum_{\sigma \in G} \phi(\sigma)(\sigma a) = 0\ \forall\ a \in L^*$

Recall the Dedekind's Theorem on the independence of characters :

Let L be a field and H a group; then every finite set $\{f_i\}$ of distinct homomorphism $H \to L^*$ is linearly independent over L i.e.

$$\sum a_i f_i(\alpha) = 0 \quad \forall\, \alpha \in H \quad \Rightarrow \quad a_1 = a_2 = ... = a_n = 0$$

Now we apply this theorem with $H = L^*$, the homomorphisms $\sigma : L^* \to L^*$, $\sigma \in G$ and the equation $\sum_{\sigma \in G} \phi(\sigma)(\sigma a) = 0\ \forall\ a \in L^*$, we find that $\forall\ \sigma \in G$, $\phi(\sigma) = 0$ which is a contradiction because $\phi(\sigma) \in L^*$. Hence $\exists\ a \in L^*$ for which $b \neq 0$ and we are done. □

2.6.2 Cohomology of L

Theorem 21. *Let L/K be a finite Galois extension with Galois group G. Then $H^r(G, L) = 0\ \forall\ r > 0$.*

Proof. By the Normal Basis Theorem, $\exists\ \alpha \in L$ such that $\{\sigma\alpha : \sigma \in G\}$ is a basis for L as a K-vector space. Then we get a map

$$\eta : K[G] \to L$$

such that

$$\eta\left(\sum_{\sigma \in G} a_\sigma \sigma\right) = \sum_{\sigma \in G} a_\sigma \sigma(\alpha)$$

Clearly η is a well defined homomorphism of abelian groups. η is injective since $\{\sigma\alpha : \sigma \in G\}$ is linear independent over K and η is surjective since $\{\sigma\alpha : \sigma \in G\}$ generates L over K. Finally for any $\tau \in G$, we have

$$\eta\left(\tau\left(\sum_{\sigma \in G} a_\sigma \sigma\right)\right) = \eta\left(\sum_{\sigma \in G} a_\sigma \tau\sigma\right) = \sum_{\sigma \in G} a_\sigma(\tau\sigma(\alpha)) = \tau\left(\sum_{\sigma \in G} a_\sigma \sigma(\alpha)\right) = \tau\left(\eta\left(\sum_{\sigma \in G} a_\sigma \sigma\right)\right)$$

Hence η is a G-module isomorphism. The following lemma combined with Corollary 2 will complete the proof of the theorem. □

Lemma 14. *Let L/K be a finite Galois extension with Galois group G, then $K[G] \cong Ind^G K$ as G-modules.*

Proof. Since G is a finite group, we can label it as $G = \{\tau_1, \tau_2, ..., \tau_n\}$. Now define the map

$$\eta_1 : Ind^G K \to K[G]$$

such that

$$\psi \mapsto \sum_{i=1}^{n} \psi(g_i^{-1}) g_i$$

The inverse map

$$\eta_2 : K[G] \to Ind^G K$$

is given by

$$\sum_{i=1}^{n} a_i \tau_i \mapsto \phi$$

where $\phi(\tau_i) = a_j$ and j is defined as $\tau_j = \tau_i^{-1}$ It is straightforward to show that η_1 is a G-module homomorphism and that the maps η_1 and η_2 are actually inverses of each other. □

2.7 The Cohomology of Products

A product $M = \prod_i M_i$ of G-modules M_i becomes a G-module under the diagonal action i.e. $\sigma(..., m_i, ...) = (..., \sigma m_i, ...)$.

Theorem 22. *For any G-modules M_i, $H^r(G, \prod_i M_i) \cong \prod_i H^r(G, M_i)$.*

Proof. Firstly we will prove that a product of exact sequences is exact.
Let

$$0 \to A_i \xrightarrow{\alpha_i} B_i \xrightarrow{\beta_i} C_i \to 0$$

be exact $\forall\ i \in I$ where I is some indexing set.

We need to prove that

$$0 \to \prod_i A_i \xrightarrow{\prod_i \alpha_i} \prod_i B_i \xrightarrow{\prod_i \beta_i} \prod_i C_i \to 0$$

is also an exact sequence.

Note that

$$Ker\left(\prod_i \beta_i\right) = \left\{(x)_{i\in I} : \left(\prod_i \beta_i\right)(x)_{i\in I} = 0\right\} = \{(x_i)_{i\in I} : (\beta_i)(x_i) = 0\ \forall\ i \in I\} = \prod_i Ker(\beta_i)$$

Hence

$$Ker\left(\prod_i \beta_i\right) = \prod_i Ker(\beta_i)$$

Similarly we can prove,

$$Ker\left(\prod_i \alpha_i\right) = \prod_i Ker(\alpha_i),\ Im\left(\prod_i \beta_i\right) = \prod_i Im(\beta_i)\ and\ Im\left(\prod_i \alpha_i\right) = \prod_i Im(\alpha_i)$$

Then we are done by the exactness of the individual short exact sequences.

Now we will prove that

$$I = \prod_i I_i$$

of injective G-modules I_i is again injective.

Let

$$0 \to M' \to M \to M'' \to 0$$

be an exact sequence of G-modules. Since I_i is injective, so

$$0 \to Hom_G(M', I_i) \to Hom_G(M, I_i) \to Hom_G(M'', I_i) \to 0$$

is exact $\forall\ i$. Hence,

$$0 \to \prod_i Hom_G(M', I_i) \to \prod_i Hom_G(M, I_i) \to \prod_i Hom_G(M'', I_i) \to 0$$

is exact. It is easy to verify that for any G-module N,

$$Hom_G(N, I) \cong \prod Hom_G(N, I_i)$$

through the natural map. Hence,

$$0 \to Hom_G(M', I) \to Hom_G(M, I) \to Hom_G(M'', I) \to 0$$

is exact and thus I is injective.

Let $M_i \to I_i^\bullet$ be an injective resolution of M_i. Then $\prod_i M_i \to \prod_i I_i^\bullet$ is an injective resolution of $\prod_i M_i$ by the above discussion and thus by the definition of cohomology groups,

$$H^r\left(G, \prod_i M_i\right) \cong H^r\left(\left(\prod_i I_i^\bullet\right)^G\right)$$

Moreover, it is easy to check that

$$\left(\prod_i I_i^\bullet\right)^G = \prod_i (I_i^\bullet)^G$$

and so

$$H^r\left(G, \prod_i M_i\right) \cong H^r\left(\left(\prod_i I_i^\bullet\right)^G\right) \cong H^r\left(\prod_i (I_i^\bullet)^G\right)$$

Then the fact that Kernels and Images commute with direct products (which we proved above) gives us

$$H^r\left(\prod_i (I_i^\bullet)^G\right) \cong \prod_i H^r(I_i^\bullet)^G$$

Therefore,

$$H^r\left(G, \prod_i M_i\right) \cong \prod_i H^r(I_i^\bullet)^G \cong \prod_i H^r(G, M_i)$$

where the last congruence holds by the definition of cohomology groups.

In particular for any G-modules M,N,

$$H^r(G, M \oplus N) \cong H^r(G, M) \oplus H^r(G, N)$$

□

2.8 Functorial Properties of the Cohomology Groups

Let M be a G module, M' be a G' module and let $\alpha : G' \to G$ be a group homomorphism.

Note that M naturally becomes a G' module via α.

Let

$$\beta : M \to M'$$

be a homomorphism (only as abelian groups).

α and β are said to be compatible if $\forall\, g' \in G'\ \forall\, m \in M$

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

Observe that this condition exactly means that β is a G' module homomorphism.

Then for each non-negative integer r, we get

$$\eta_r : C^r(G, M) \to C^r(G', M')$$

such that

$$\phi \mapsto \beta \circ \phi \circ \alpha^r$$

i.e.

$$\eta_r(\phi(g_1, ..`., g_r)) = \beta(\phi(\alpha(g_1), ..., \alpha(g_r)))$$

Consider the diagram :

$$\begin{array}{ccc} C^{r-1}(G, M) & \xrightarrow{d^{r-1}} & C^r(G, M) \\ \downarrow \eta_{r-1} & & \downarrow \eta_r \\ C^{r-1}(G', M') & \xrightarrow{d'^{r-1}} & C^r(G', M') \end{array} \tag{2.15}$$

Direct calculation shows that this diagram commutes i.e. $\forall r \in \mathbb{N}$

$$\eta_r \circ\ d^{r-1} = d'^{r-1} \circ \eta_{r-1}$$

Note that the compatibility condition is required in the proof of this fact.

Now

$$\eta_r \circ\ d^{r-1} = d'^{r-1} \circ \eta_{r-1}$$

which implies that

$$\eta_r(Im(d^{r-1})) \subset Im(d'^{r-1})$$

and

$$\eta_{r+1} \circ\ d^r = d'^r \circ \eta_r$$

and so

$$\eta_r(Ker(d^r)) \subset Ker(d'^r)$$

Thus η_r induces a group homomorphism (which we again denote by η_r)

$$\eta_r : \frac{Ker(d^r)}{Im(d^{r-1})} \to \frac{Ker(d'^r)}{Im(d'^{r-1})}$$

i.e. a group homomorphism

$$\eta_r : H^r(G, M) \to H^r(G', M')$$

2.8.1 Examples

1. **Shapiro's Lemma** Let H be a subgroup of G and let α be the inclusion map from H to G and $\beta : Ind_H^G M \to M$ such that $\phi \mapsto \phi(1)$. Compatibility condition is satisfied and by the above procedure we get the group homomorphism

$$H^r(G, Ind_H^G M) \to H^r(H, M)$$

This group homomorphism is infact an isomorphism which gives another proof of the Shapiro's lemma (Theorem 19). This is a fact which we will see in a later section (Theorem 37) but we are assuming it for now.

2. **Restriction maps** Let H be a subgroup of G and let α be the inclusion map from H to G and β be the identity map on M. Then by the above procedure we obtain the restriction homomorphism

$$Res : H^r(G, M) \to H^r(H, M)$$

There is another way of describing the restriction homomorphism.

Let α be the identity map on G and $\beta : M \to Ind_H^G M$ be the map such that $m \mapsto \phi_m$ where $\phi_m(g) = gm$. This gives us the homomorphism

$$H^r(G, M) \to H^r(G, Ind_H^G M)$$

Composing this homomorphism with the isomorphism of Shapiro's lemma (in Example 1 above), $H^r(G, \mathrm{Ind}_H^G M) \to H^r(H, M)$, we get the required restriction map.

3. **Inflation maps** Let H be a normal subgroup of G. Then M^H is a G/H module as seen in the proof of Lemma 12. Let α be the quotient map $G \to G/H$ and β be the inclusion $M^H \to M$. This induces the inflation homomorphism :

$$Inf : H^r(G/H, M^H) \to H^r(G, M)$$

4. **Corestriction maps** Let H be a subgroup of finite index in G, and let S be a set of left coset representatives for H in G. Let α be the identity map on G and $\beta : Ind_H^G M \to M$ such that

$$\beta(\phi) = \sum_{s \in S} s\phi(s^{-1})$$

In order to show that β is well-defined, we have to show that the sum $\sum_{s \in S} s\phi(s^{-1})$ is independent of the choice of set of left coset representatives. Let $S = \{s_1, ..., s_n\}$ and $T = \{t_1, ..., t_n\}$ be two sets of left coset representatives of H in G. We need to show that

$$\sum_{i=1}^{n} s_i\phi(s_i^{-1}) = \sum_{i=1}^{n} t_i\phi(t_i^{-1})$$

Since we can interchange S and T, so it suffices to show that

$$\sum_{i=1}^{n} s_i\phi(s_i^{-1}) \ \leq \ \sum_{i=1}^{n} t_i\phi(t_i^{-1})$$

Any $s_i \in S$ is in some coset t_jH and so we have $s_i = t_jh_{ij}$ for some $h_{ij} \in H$. This shows that $s_i^{-1} = h_{ij}^{-1}t_j^{-1}$ and so

$$\phi(s_i^{-1}) = \phi(h_{ij}^{-1}t_j^{-1}) = h_{ij}^{-1}\phi(t_j^{-1})$$

Note that in the last equality, we have used that $\phi \in Ind_H^G(M)$. Thus

$$s_i\phi(s_i^{-1}) = t_jh_{ij}h_{ij}^{-1}\phi(t_j^{-1}) = t_j\phi(t_j^{-1})$$

Hence we have shown that every element $s_i\phi(s_i^{-1})$ is of the form $t_j\phi(t_j^{-1})$ for some j. This implies that

$$\sum_{i=1}^{n} s_i\phi(s_i^{-1}) \leq \sum_{i=1}^{n} t_i\phi(t_i^{-1})$$

and so we are done. Thus β is a well defined map and induces the homomorphism

$$H^r(G, Ind_H^G M) \to H^r(G, M)$$

Composing this homomorphism with the inverse of isomorphism of Shapiro's lemma (in Example 1 above), we get the corestriction homomorphism :

$$Cor : H^r(H, M) \to H^r(G, M)$$

Remark 7. *It is important to see the description of corestriction maps in dimension* 0*. Let* G *be a finite group. For every* G*-module* M*, define the norm map*

$$Nm_G : M \to M$$

such that

$$m \mapsto \sum_{g \in G} gm$$

By the proof of Shapiro's Lemma (Theorem 19*), we know that the isomorphism*

$$H^0(H, M) \to H^0(G, Ind_H^G M)$$

is given by $m \mapsto \phi_m$ *where* $\phi_m(g) = m \ \forall \ g \in G$*. The map*

$$H^0(G, Ind_H^G M) \to H^0(G, M)$$

takes ϕ_m *to*

$$\sum_{s \in S} s\phi_m(s^{-1}) = \sum_{s \in S} sm = Nm_{G/H}m$$

Hence the corestriction map in dimension 0 *is*

$$cor_0 : M^H \to M^G$$

given by

$$cor_0(m) = \sum_{s \in S} sm = Nm_{G/H}m$$

Thus the corestriction map is given by the norm map in dimension 0*.*

2.8.2 Relations among functorial maps

Theorem 23. *Let H be a subgroup of G of finite index. The composite*

$$Cor \circ Res : H^r(G, M) \to H^r(G, M)$$

is multiplication by $(G : H)$.

Proof. Note that while taking the composition, the isomorphism of Shapiro's Lemma (in Example 1) and its inverse cancel with each other (We are using the alternate description of the restriction map).

$$Cor \circ Res : H^r(G, M) \to H^r(G, M)$$

is then simply the induced map on cohomology taking α to be the identity on G and β to be the composite

$$M \to Ind_H^G M \to M$$

such that

$$m \mapsto \phi_m \mapsto \sum_{s \in S} s\phi_m(s^{-1}) = \sum_{s \in S} s(s^{-1}m) = (G : H)m$$

Now since $\eta_r(\phi) = \beta \circ \phi \circ \alpha^r$ and α is the identity; thus $\eta_r(\phi) = \beta \circ \phi$. Since β is multiplication by $(G : H)$; so η_r is also multiplication by $(G : H)$. □

Corollary 3. *If $(G : 1) = m$, then $mH^r(G, M) = 0$.*

Proof. If we take $H = \{1\}$, by Theorem 23, we get $mH^r(G, M) = (Cor \circ Res)(H^r(G, M)$

$Res : H^r(G, M) \to H^r(\{1\}, M)$ is the zero map since $H^r(\{1\}, M) = 0$. Hence

$$mH^r(G, M) = (Cor \circ Res)(H^r(G, M) = Cor(Res(H^r(G, M))) = Cor(0) = 0$$

□

Theorem 24. *Let H be a normal subgroup of G, and let M be a G-module. Then the inflation restriction sequence*

$$0 \to H^1(G/H, M^H) \xrightarrow{Inf} H^1(G, M) \xrightarrow{Res} H^1(H, M)$$

is exact.

Proof. Firstly we will prove that the Inf map is injective.

Let ϕ_1 and ϕ_2 be crossed homomorphisms from G/H to M^H such that

$$Inf(\bar{\phi_1}) = Inf(\bar{\phi_2})$$

in $H^1(G, M)$. Thus

$$Inf(\phi_1) = Inf(\phi_2) + \eta$$

where $\eta : G \to M$ is such that $\eta(g) = gm_0 - m_0 \; \forall \; g \in G$ for some $m_0 \in M$. Therefore, $\forall \; g \in G$,

$$\phi_1(gH) = \phi_2(gH) + (gm_0 - m_0)$$

In particular $\forall\ h \in H$,

$$hm_0 = m_0$$

Thus η is zero on H and $m_0 \in M^H$. Define the map $\eta' : G/H \to M^H$ given by $\eta'(gH) = \eta(g)$. Firstly we will show that η' is well-defined. Let $g_1H = g_2H$. This means that $g_1 = g_2h$ for some $h \in H$. Thus

$$\eta(g_1) = \eta(g_2h) = g_2\eta(h) + \eta(g_2) = \eta(g_2)$$

and so η' is well-defined. Since $gm_0 - m_0 = (gH)m_0 - m_0$, so η' is a principal crossed homomorphism from G/H to M^H. Hence, $\bar{\phi_1} = \bar{\phi_2}$ and Inf is injective.

Exactness at $H^1(G, M)$:

Firstly we will prove that $Im(Inf) \subset Ker(Res)$.

Let $\bar{\psi} = Inf(\bar{\phi})$ where $\phi \in H^1(G/H, M^H)$ i.e. ϕ is a crossed homomorphism from G/H to M^H. Then $\bar{\psi}$ is represented by a crossed homomorphism ψ from G to M such that $\psi(g) = \phi(gH)$.

$\bar{\eta} = Res\ \bar{\psi}$ is represented by a crossed homomorphism η from H to M such that

$$\eta(h) = \psi(h) = \phi(hH) = \phi(H) = 0$$

Thus $Res(\bar{\psi}) = 0$, so $\bar{\psi} \in Ker(Res)$ and we are done.

Now we will prove that $Ker(Res) \subset Im(Inf)$.

Let $\bar{\phi} \in Ker(Res)$ i.e. ϕ is a crossed homomorphism from G to M such that the restriction of ϕ to H is a principal crossed homomorphism i.e.

$$\phi(h) = hm_0 - m_0$$

for some $m_0 \in M\ \forall\ h \in H$.

Define $\phi^{'} : G \to M$ such that

$$\phi^{'}(g) = \phi(g) - (gm_0 - m_0)$$

Then

$$\phi^{'}(g_1g_2) = \phi(g_1g_2) - (g_1g_2m_0 - m_0)$$

Since ϕ_1 is a crossed homomorphism,

$$\phi(g_1g_2) = g_1\phi(g_2) + \phi(g_1)$$

It follows that

$$\phi^{'}(g_1g_2) = g_1\phi^{'}(g_2) + \phi^{'}(g_1)$$

Hence $\phi^{'}$ is also a crossed homomorphism which is in the same class as ϕ in $H^1(G, M)$

Note that $\phi^{'}(h) = 0\ \forall\ h \in H$.

Define $\phi^{''} : G/H \to M$ such that $\phi^{''}(gH) = \phi^{'}(g)$.

We will show that ϕ'' is well defined.

Let $g_1H = g_2H$. Then $g_2^{-1}g_1 \in H$ i.e. $g_1 = hg_2$ for some $h \in H$ and so $g_1 = g_2h_1$ for some $h_1 \in H$ since H is normal in G.

Since ϕ' is crossed,

$$\phi'(g_1) = g_2\phi'(h_1) + \phi'(g_2) = \phi'(g_2)$$

and thus

$$\phi''(g_1H) = \phi''(g_2H)$$

Now we will prove that for any $g \in G$, $\phi''(gH) \in M^H$. Note that for $h \in H$ and $g \in G$, we have

$$\phi'(hg) = h\phi'(g) + \phi'(h)$$

and thus,

$$h\phi'(g) = \phi'(hg) - \phi'(h) = \phi'(hg) = \phi'(gh_1)$$

for some $h_1 \in H$ since H is normal in G. Therefore,

$$h\phi'(g) = g\phi'(h_1) + \phi'(g) = \phi'(g)$$

Hence,

$$h\phi'(g) = \phi'(g) \ \forall \ h \in H$$

which shows that,

$$\phi''(gH) = \phi'(g) \in M^H$$

and hence we are done.

Finally ϕ'' is a crossed homomorphism because,

$$\phi''((g_1H)(g_2H)) = \phi''((g_1g_2H) = \phi'(g_1g_2) = g_1\phi'(g_2) + \phi^{g_1} = (g_1H)\phi''(g_2H) + \phi''(g_1H)$$

Hence we have shown that the inflation restriction sequence is exact. □

Using the description of the boundary map, it is straightforward to show that the following results hold :

Theorem 25. *Let*

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

be an exact sequence of G-modules, then the diagram

$$\begin{array}{ccc} H^r(G,C) & \xrightarrow{\delta} & H^{r+1}(G,A) \\ \downarrow{\scriptstyle res_r} & & \downarrow{\scriptstyle res_{r+1}} \\ H^r(H,C) & \xrightarrow{\delta} & H^{r+1}(H,A) \end{array} \tag{2.16}$$

commutes for all $r \geq 0$.

Theorem 26. *Let*

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

be an exact sequence of G-modules, then the diagram

$$\begin{array}{ccc} H^r(H,C) & \xrightarrow{\delta} & H^{r+1}(H,A) \\ \downarrow{\scriptstyle cor_r} & & \downarrow{\scriptstyle cor_{r+1}} \\ H^r(G,C) & \xrightarrow{\delta} & H^{r+1}(G,A) \end{array} \tag{2.17}$$

commutes for all $r \geq 0$.

Theorem 27. *Let*

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

be an exact sequence of G-modules, and let H be a normal subgroup of G. If the sequence

$$0 \to A^H \to B^H \to C^H \to 0$$

is also exact, then the diagram

$$\begin{array}{ccc} H^r(G/H,C^H) & \xrightarrow{\delta} & H^{r+1}(G/H,A^H) \\ \downarrow{\scriptstyle inf_r} & & \downarrow{\scriptstyle inf_{r+1}} \\ H^r(G,C) & \xrightarrow{\delta} & H^{r+1}(G,A) \end{array} \tag{2.18}$$

commutes for all $r \geq 0$.

The main step in the proof of each of these theorems is the observation that these functorial maps commute with the maps

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

2.9 Homology

For a G-module M, let M_G be the largest quotient of M on which G acts trivially. Thus M_G is the quotient of M by the subgroup M_0 generated by

$$\{gm - m : g \in G, m \in M\}$$

Lemma 15. *If*

$$M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$$

is an exact sequence of G-modules, then

$$M'_G \xrightarrow{\alpha_1} M_G \xrightarrow{\beta_1} M''_G \to 0$$

is also exact.

Proof. The map $\alpha_1 : M'_G \to M_G$ is defined as $\overline{m'} \mapsto \overline{\alpha(m')}$. To show that α_1 is well defined we have to show that $\alpha(M'_0) \subset M_0$. But this is true since for any $m' \in M'$, we have

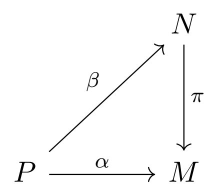
$$\alpha(gm' - m') = \alpha(gm') - \alpha(m') = g(\alpha(m')) - \alpha(m') \in M_0$$

Similarly $\beta_1 : M_G \to M''_G$ such that $\overline{m} \mapsto \overline{\beta(m)}$ is a well-defined G-module homomorphism. Clearly β_1 is surjective since β is. Since $Ker(\beta) = Im(\alpha)$, so we have $\beta(\alpha(m')) = 0$ for any $m' \in M'$. Therefore, $Im(\alpha_1) \subset Ker(\beta_1)$. Conversely let $m + M_0 \in Ker(\beta_1)$ for some $m \in M$. This means that $\beta(m) = gm'' - m''$ for some $m'' \in M''$. Since β is surjective, so $m'' = \beta(m_1)$ for some $m_1 \in M$. Therefore,

$$gm'' - m'' = g\beta(m_1) - \beta(m_1) = \beta(gm_1 - m_1)$$

Hence $\beta(m) = \beta(gm_1 - m_1)$ and so $m - (gm_1 - m_1) \in Ker(\beta) = Im(\alpha)$. Therefore, $m - (gm_1 - m_1) = \alpha(m')$ for some $m' \in M'$ which shows that $m - \alpha(m') \in M_0$ Hence $m + M_0 = \alpha(m') + M_0$. This shows that $Ker(\beta_1) \subset Im(\alpha_1)$ and we are done. □

Definition 4. *A G-module P is said to be projective if for every surjective G-module homomorphism $\pi : N \to M$ and every G-module homomorphism $\alpha : P \to M$, there exists a G-module homomorphism $\beta : P \to N$ such that $\beta \circ \pi = \alpha$ i.e. the following diagram commutes :*



(2.19)

Equivalently, P is projective if $Hom(P, \ )$ is an exact functor.

Lemma 16. *Every G-module is a quotient of a projective G-module.*

Proof. We know that every G-module is a quotient of a free G-module. By the universal property of free modules, it follows that every free G-module is projective, so every G-module is a quotient of a projective G-module. □

Definition 5. *A projective resolution of a G-module M is a long exact sequence*

$$... \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} M \to 0$$

such that P_i is a projective module for each $i \geq 0$.

We had shown that for any G-module M, there is an injective resolution. With a similar approach, one can show that

Theorem 28. *For a G-module M, there exists a projective resolution of M.*

Definition 6. *Met M be a G-module, and choose a projective resolution*

$$... \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} M \to 0$$

of M. The complex

$$... \to (P_2)_G \xrightarrow{d_2} (P_1)_G \xrightarrow{d_1} (P_0)_G \xrightarrow{d_0} 0$$

need no longer be exact and we define the r^{th} *homology group*

$$H_r(G, M) = \frac{Ker(d_r)}{Im(d_{r+1})}$$

Theorem 29. *$H_r(G, M)$ is independent of the choice of the projective resolution (upto an isomorphism) and is thus well defined.*

Proof. See Theorem 6, page 782, [7]. □

Lemma 17. $H_0(G, M) \cong M_G$

Proof. Since

$$P_1 \to P_0 \to M \to 0$$

is an exact sequence, so by Lemma 15, the following sequence is also exact :

$$(P_1)_G \xrightarrow{d_1} (P_0)_G \xrightarrow{d_0'} M_G \to 0$$

Therefore,

$$H_0(G, M) = \frac{Ker(d_0)}{Im(d_1)} = \frac{(P_0)_G}{Im(d_1)} = \frac{(P_0)_G}{Ker(d_0')} \cong Im(d_0') = M_G$$

□

Lemma 18. *If P is a projective G-module, then $H_r(G, P) = 0$ for all $r > 0$*

Proof. This follows from the fact that

$$... \to 0 \to P \to P \to 0$$

is a projective resolution of P. □

Theorem 30. *A short exact sequence*

$$0 \to M' \to M \to M'' \to 0$$

of G-modules gives rise to a long exact sequence

$$0 \to H_0(G, M') \to H_0(G, M) \to ... \to H_r(G, M') \to H_r(G, M) \to H_r(G, M'') \xrightarrow{\delta r} H_{r+1}(G, M') \to ...$$

Proof. See page 789, [7]. □

2.10 The Group $H_1(G, \mathbb{Z})$

Define the augmentation map

$$\eta : \mathbb{Z}[G] \to \mathbb{Z}[G]$$

such that

$$\eta\left(\sum n_i g_i\right) = \sum n_i$$

$I_G = Ker(\eta)$ is called the augmentation ideal.

The set

$$\{g - 1 : g \in G \ and \ g \neq 1\}$$

generates I_G as a $\mathbb{Z}$ module since,

$$\sum_{i=1}^{k} n_i g_i = \sum_{i=1}^{k} n_i (g_i - 1)$$

because $\sum n_i = 0$. Moreover,

$$H_0(G, M) \cong M_G = \frac{M}{M_0}$$

where M_0 is the submodule of M generated by all elements of the form $gm - m$ where $g \in G$ and $m \in M$. But $gm - m = (g-1)m$ and thus, $M_0 = I_G M$ which shows that $H_0(G, M) \cong \frac{M}{I_G M}$.

Consider the augmentation sequence :

$$0 \to I_G \xrightarrow{i} \mathbb{Z}[G] \xrightarrow{\eta} \mathbb{Z} \to 0$$

The G-module $\mathbb{Z}[G]$ is projective because it is a free $\mathbb{Z}[G]$ module and so $H_1(G, \mathbb{Z}[G]) = 0$ But we have an exact sequence which is a part of the long exact sequence for the homology groups.

$$H_1(G, \mathbb{Z}[G]) \to H_1(G, \mathbb{Z}) \to H_0(G, I_G) \to H_0(G, \mathbb{Z}[G]) \to H_0(G, \mathbb{Z}) \to 0$$

We also know that

$$H_0(G, \mathbb{Z}) = \mathbb{Z}$$

since the action of G on $\mathbb{Z}$ is trivial. Moreover, we have

$$H_0(G, \mathbb{Z}[G]) = \frac{\mathbb{Z}[G]}{I_G \mathbb{Z}_G} = \frac{\mathbb{Z}[G]}{I_G}$$

and,

$$H_0(G, I_G) = \frac{I_G}{I_G I_G} = \frac{I_G}{I_G^2}$$

Hence we get an exact sequence

$$0 \to H_1(G, \mathbb{Z}) \to \frac{I_G}{I_G^2} \xrightarrow{i} \frac{\mathbb{Z}[G]}{I_G} \to \mathbb{Z} \to 0$$

The map

$$\frac{I_G}{I_G^2} \xrightarrow{i} \frac{\mathbb{Z}[G]}{I_G}$$

is induced by the map $I_G \xrightarrow{i} \mathbb{Z}[G]$ and is thus the zero map as we are evaluating the image of an element of I_G modulo I_G.

Hence we have the exact sequence

$$0 \to H_1(G,\mathbb{Z}) \xrightarrow{\alpha} \frac{I_G}{I_G^2} \xrightarrow{0} \frac{\mathbb{Z}[G]}{I_G} \xrightarrow{\beta} \mathbb{Z} \to 0$$

We already knew that α is injective and β is surjective but by this exact sequence, we also have that $Im(\alpha) = Ker(0)$ and $Im(0) = Ker(\beta)$.

Thus $Im(\alpha) = \frac{I_G}{I_G^2}$ and $Ker(\beta) = 0$.

This shows that α is surjective and β is injective. Hence α and β are both bijections and thus isomorphisms.

Therefore, we have

$$H_1(G,\mathbb{Z}) \cong \frac{I_G}{I_G^2} \tag{2.20}$$

and

$$\frac{\mathbb{Z}[G]}{I_G} \cong \mathbb{Z}$$

Remark 8. *$\mathbb{Z}$ is the largest quotient of $\mathbb{Z}[G]$ on which G acts trivially.*

Remark 9. *I_G^2 is the $\mathbb{Z}$-submodule of $\mathbb{Z}[G]$ generated by elements of the form $(g-1)(g^{'}-1)$ where $g, g^{'} \in G$*

Lemma 19. *Let G^c be the commutator subgroup of G, so that G/G^c is the largest abelian quotient of G. Then the map*

$$\phi : G/G^c \to \frac{I_G}{I_G^2}$$

such that

$$\phi(gG^c) = (g-1) + I_G^2$$

is an isomorphism.

Proof. Firstly consider the map $\phi : G \to \frac{I_G}{I_G^2}$ such that $g \mapsto (g-1) + I_G^2$

For $g, g' \in G$, we have

$$\phi(gg') = (gg'-1) + I_G^2 = (g-1)(g'-1) + (g-1) + (g'-1) + I_G^2 = \phi(g) + \phi(g')$$

since $(g-1)(g'-1) \in I_G^2$ and thus ϕ is a group homomorphism. Then we have for given $g_1, g_2 \in G$,

$$\phi(g_1 g_2 g_1^{-1} g_2^{-1}) = \phi(g_1) + \phi(g_2) + \phi(g_1^{-1}) + \phi(g_2^{-1}) = 0$$

because $\frac{I_G}{I_G^2}$ is abelian. Hence there is a well defined homomorphism

$$\Phi : G^{ab} = \frac{G}{G^c} \to \frac{I_G}{I_G^2}$$

such that

$$\Phi(gG^c) = (g-1) + I_G^2$$

Similarly one can verify that there is a well defined homomorphism

$$\Psi : \frac{I_G}{I_G^2} \to G^{ab}$$

such that

$$\Psi((g-1) + I_G^2) = gG^c$$

Clearly Φ and Ψ are inverses of each other. Thus, $\frac{I_G}{I_G^2} \cong G^{ab}$ □

Theorem 31. $H_1(G, \mathbb{Z}) \cong G^{ab}$

Proof. This follows directly from equation 2.20 and Lemma 19.

Remark 10. *From the proof of Theorem 31, it follows that the isomorphism* $H_1(G, \mathbb{Z}) \cong G^{ab}$ *is the composition of the isomorphisms* $H_1(G, \mathbb{Z}) \cong I_G/I_G^2$ *and* $I_G/I_G^2 \cong G^{ab}$. *This description would be required later.*

□

2.11 Tate Groups

Throughout this section, we assume that G is a finite group.

For every G-module M, define the norm map

$$Nm_G : M \to M$$

such that

$$m \mapsto \sum_{g \in G} gm$$

Let $g' \in G$. Since we have

$$g' Nm_G(m) = g' \sum_{g \in G} gm = \sum_{g \in G} g' gm = \sum_{g \in G} gm = Nm_G(m)$$

so $Im(Nm_G) \subset M^G$. Similarly $I_G M \subset Ker(Nm_G)$

Hence the norm map can be extended to $Nm_G : \frac{M}{I_G M} \to M^G$

Since the Kernel of the norm map is $\frac{Ker(Nm_G)}{I_GM}$ and the cokernel is $\frac{M^G}{Nm_G(M)}$, so we get an exact sequence

$$0 \to \frac{Ker(Nm_G)}{I_GM} \to \frac{M}{I_GM} \xrightarrow{Nm_G} M^G \to \frac{M^G}{Nm_G(M)} \to 0$$

This can also be expressed as

$$0 \to \frac{Ker(Nm_G)}{I_GM} \to H_0(G,M) \xrightarrow{Nm_G} H^0(G,M) \to \frac{M^G}{Nm_G(M)} \to 0$$

Thus the Kernel of the norm map is $\frac{Ker(Nm_G)}{I_GM}$ and the cokernel is $\frac{M^G}{Nm_G(M)}$

We define Tate groups $H_T^r(G,M) \quad (-\infty < r < \infty) \quad$ as $\quad$:

$$\begin{cases} H^r(G,M) & r > 0 \\ M^G/Nm_G(M) & r = 0 \\ Ker(Nm_G)/I_GM & r = -1 \\ H_{-r-1}(G,M) & r < -1 \end{cases}$$

Note that in view of these definitions, our exact sequence can be rewritten as

$$0 \to H_T^{-1}(G,M) \to H_0(G,M) \xrightarrow{Nm_G} H^0(G,M) \to H_T^0(G,M) \to 0 \tag{2.21}$$

Thus the kernel of the norm map is $H_T^{-1}(G,M)$ and cokernel of the norm map is $H_T^0(G,M)$.

This interpretation will be useful in the next section.

Theorem 32. *For every given short exact sequence*

$$0 \to M' \to M \to M'' \to 0$$

there is a very long exact sequence for Tate Cohomology groups

$$... \to H_T^r(G,M') \to H_T^r(G,M) \to H_T^r(G,M'') \xrightarrow{\delta} H_T^{r+1}(G,M) \to ...$$

Proof. To prove this Theorem, we have to firstly describe the maps $\eta_2 : H^{-2}(G,M'') \to H^{-1}(G,M')$, $\eta : H_T^{-1}(G,M'') \to H_T^0(G,M')$ and $\eta_5 : H_T^0(G,M'') \to H_T^1(G,M')$ as these maps had not been defined till now.

Consider the commutative diagram :

$$\begin{array}{ccccccccc} & & H_0(G,M') & \xrightarrow{f} & H_0(G,M) & \longrightarrow & H_0(G,M'') & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle Nm_G} & & \downarrow{\scriptstyle Nm_G} & & \downarrow{\scriptstyle Nm_G} & & \\ 0 & \longrightarrow & H^0(G,M') & \longrightarrow & H^0(G,M) & \xrightarrow{g} & H^0(G,M'') & \longrightarrow & H^1(G,M') \end{array} \tag{2.22}$$

where the upper row is the long exact homology sequence and the lower row is the long exact cohomology sequence. We can apply the extended snake lemma to get an exact sequence.

$$\begin{aligned} 0 \to Ker(f) \to H_T^{-1}(G,M') \xrightarrow{\eta_3} H_T^{-1}(G,M) \to H_T^{-1}(G,M'') \xrightarrow{\eta} H_T^0(G,M') \\ \to H_T^0(G,M) \xrightarrow{\eta_4} H_T^0(G,M'') \xrightarrow{\kappa_2} Coker(g) \to 0 \end{aligned} \tag{2.23}$$

In particular, it shows that $Ker(f) \subset H_T^{-1}(G,M')$.

Note that the map $\eta : H_T^{-1}(G,M'') \to H_T^0(G,M')$ has been defined automatically by the Extended Snake Lemma.

Observe that by equation 2.21, we have

$$H_T^{-1}(G,M') \subset H_0(G,M')$$

We also have the long exact homology sequence :

$$... \to H_1(G,M') \to H_1(G,M) \to H_1(G,M'') \xrightarrow{\delta} H_0(G,M') \xrightarrow{f} H_0(G,M) \to H^0(G,M'') \to 0$$

which shows that

$$Im(\delta) = Ker(f) \subset H_T^{-1}(G,M')$$

Thus we can define

$$\eta_2 : H_T^{-2}(G,M'') \to H_T^{-1}(G,M')$$

to be the map

$$\delta : H_1(G,M'') \to H_0(G,M')$$

since $Im(\delta) \subset H^{-1}(G,M')$.

Now we want to define the map $\eta_5 : H_T^0(G,M'') \to H_T^1(G,M')$.

By equation 2.23, we have a surjective map

$$\kappa_2 : H_T^0(G,M'') \to Coker(g)$$

Moreover, we have the long exact cohomology sequence

$$H^0(G,M') \to H^0(G,M) \xrightarrow{g} H^0(G,M'') \xrightarrow{\kappa_3} H^1(G,M') \xrightarrow{\eta_6} H^1(G,M) \to H^1(G,M'') \to ...$$

which gives us an injective map

$$\kappa_1 : Coker(g) \to H^1(G,M')$$

induced by κ_3 since $Ker(\kappa_3) = Im(g)$. We define

$$\eta_5 : H_T^0(G, M'') \to H_T^1(G, M')$$

such that

$$\eta_5 = \kappa_1 \circ \kappa_2$$

Now we will prove the Theorem.

By the long exact cohomology sequence, we know that the following sequence is exact :

$$H^0(G, M') \to H^0(G, M) \xrightarrow{g} H^0(G, M'') \xrightarrow{\kappa_3} H^1(G, M') \xrightarrow{\eta_6} H^1(G, M) \to H^1(G, M'') \to ...$$

In particular we get that the following sequence is exact :

$$H_T^1(G, M') \xrightarrow{\eta_6} H_T^1(G, M) \to H_T^1(G, M'') \to ... \tag{2.24}$$

By the long exact homology sequence, we know that the following sequence is exact :

$$... \to H_1(G, M') \to H_1(G, M) \to H_1(G, M'') \xrightarrow{\delta} H_0(G, M') \xrightarrow{f} H_0(G, M) \to H^0(G, M'') \to 0$$

This can be rewritten as :

$$... \to H_T^{-2}(G, M') \to H_T^{-2}(G, M) \to H_T^{-2}(G, M'') \xrightarrow{\delta} H_0(G, M') \xrightarrow{f} H_0(G, M) \to H^0(G, M'') \to 0$$

In particular we get that the following sequence is exact :

$$... \to H_T^{-2}(G, M') \to H_T^{-2}(G, M) \to H_T^{-2}(G, M'') \tag{2.25}$$

In order to prove the Theorem, by equations 2.24 and 2.25, it suffices to prove the exactness of the following sequence :

$$\begin{aligned} H_T^{-2}(G, M) \xrightarrow{\eta_1} H_T^{-2}(G, M'') \xrightarrow{\eta_2} H_T^{-1}(G, M') \xrightarrow{\eta_3} H_T^{-1}(G, M) \to H_T^{-1}(G, M'') \\ \to H_T^0(G, M') \to H_T^0(G, M) \xrightarrow{\eta_4} H_T^0(G, M'') \xrightarrow{\eta_5} H_T^1(G, M') \xrightarrow{\eta_6} H_T^1(G, M) \end{aligned} \tag{2.26}$$

By equation 2.23, we only need to show exactness of this sequence at $H_T^{-2}(G, M'')$, $H_T^{-1}(G, M')$, $H_T^0(G, M'')$ and $H_T^1(G, M')$.

By long exact homology sequence, we have that the following sequence is exact :

$$... \to H_1(G, M') \to H_1(G, M) \xrightarrow{\eta_1} H_1(G, M'') \xrightarrow{\delta} H_0(G, M') \xrightarrow{f} H_0(G, M) \to H^0(G, M'') \to 0$$

Therefore, $Im(\eta_1) = Ker(\delta)$ but we have $Ker(\delta) = Ker(\eta_2)$ by definition of η_2. So $Im(\eta_1) = Ker(\eta_2)$.

Thus we have shown exactness at $H_T^{-2}(G, M'')$.

Now by equation 2.23, we have $Ker(\eta_3) = Ker(f)$. But we have by the exact sequence for homology, we have $Ker(f) = Im(\delta)$. Moreover, $Im(\delta) = Im(\eta_2)$ by definition of η_2. Therefore, $Ker(\eta_3) = Im(\eta_2)$ and so we have exactness at $H_T^{-1}(G, M')$.

Now $Ker(\eta_5) = Ker(\kappa_2)$ since $\eta_5 = \kappa_1 \circ \kappa_2$ and κ_1 is injective. Moreover, we have $Ker(\kappa_2) = Im(\eta_4)$ by equation 2.23. Therefore, $Im(\eta_4) = Ker(\eta_5)$.

Thus we have shown exactness at $H^0_T(G, M'')$.

Moreover, we have $Im(\eta_5) = Im(\kappa_1)$ as $\eta_5 = \kappa_1 \circ \kappa_2$ and κ_2 is surjective. But $Im(\kappa_1) = Im(\kappa_3)$ by definition of κ_1. Furthermore, we have the long exact cohomology sequence :

$$H^0(G, M') \to H^0(G, M) \xrightarrow{g} H^0(G, M'') \xrightarrow{\kappa_3} H^1(G, M') \xrightarrow{\eta_6} H^1(G, M) \to H^1(G, M'') \to ...$$

which shows that $Im(\kappa_3) = Ker(\eta_6)$. Thus we have $Im(\eta_5) = Ker(\eta_6)$ which shows the exactness at $H^1_T(G, M')$. This completes the proof of the Theorem. □

Remark 11. *The map* $\eta : H^{-1}_T(G, M'') \to H^0_T(G, M')$ *can be obtained by the diagram* 2.22*. Since kernel of the map* $Nm_G : H_0(G, M'') \to H^0(H, M'')$ *is equal to* $H^{-1}_T(G, M'')$ *and cokernel of the map* $Nm_G : H_0(G, M') \to H^0(G, M')$ *is equal to* $H^0_T(G, M')$ *by equation* 2.21*, so we get the commutative diagram :*

$$\begin{array}{ccccccccc}
 & & & & & & H^{-1}_T(G, M'') & & \\
 & & & & & & \downarrow i & & \\
 & & H_0(G, M') & \xrightarrow{f} & H_0(G, M) & \xrightarrow{\alpha} & H_0(G, M'') & \longrightarrow & 0 \\
 & & \downarrow Nm_G & & \downarrow Nm_G & & \downarrow Nm_G & & \\
0 & \longrightarrow & H^0(G, M') & \xrightarrow{\beta} & H^0(G, M) & \xrightarrow{g} & H^0(G, M'') & \longrightarrow & H^1(G, M') \\
 & & \downarrow \pi & & & & & & \\
 & & H^0_T(G, M') & & & & & &
\end{array} \tag{2.27}$$

Now since we have defined η *by Extended Snake's Lemma, to take the image of an element of* $H^{-1}_T(G, M'')$ *under the map* η*, we have to first take its image under* i*, then take some preimage under* α*, then take its image under the map* Nm_G*, then take the preimage under* β *and finally take its image under* π*.*

This description of the map $\eta : H^{-1}_T(G, M'') \to H^0_T(G, M')$ *would be required later.*

We would need the following Lemma several times :

Lemma 20. *If*

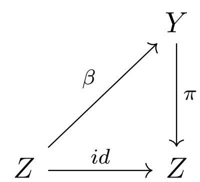
$$0 \to X \xrightarrow{\alpha} Y \xrightarrow{\pi} Z \to 0$$

is an exact sequence of free $\mathbb{Z}$*-modules and* A *is an arbitrary* $\mathbb{Z}$*-module, then the sequence*

$$0 \to X \otimes A \xrightarrow{\alpha \otimes 1} Y \otimes A \xrightarrow{\pi \otimes 1} Z \otimes A \to 0$$

is also exact.

Proof. Since we know that the tensor product is right exact, so we only have to show that the map $\alpha \otimes 1$ is injective. Since $\mathbb{Z}$ is a free module, so by the universal property, there exists a map β such that the following diagram commutes :



(2.28)

i.e. $\pi \circ \beta = id$. Now we will show that

$$Y = Im(\beta) \oplus Ker(\pi)$$

Firstly assume that $y \in Im(\beta) \cap Ker(\pi)$. Thus $y = \beta(z)$ for some $z \in Z$ and $\pi(y) = 0$. Therefore

$$z = \pi(\beta(z)) = \pi(y) = 0$$

and so $y = \beta(0) = 0$. Thus we have shown that

$$Im(\beta) \cap Ker(\pi) = 0$$

which means that it suffices to show that

$$Y = Im(\beta) + Ker(\pi)$$

Clearly

$$Im(\beta) + Ker(\pi) \subset Y$$

Now for any $y \in Y$, we have

$$\pi(y - \beta(\pi(y))) = \pi(y) - \pi(\beta(\pi(y))) = \pi(y) - \pi(y) = 0$$

where in the second equality, we have used the fact that $\pi \circ \beta = id$. Thus we have shown that

$$Y = Im(\beta) \oplus Ker(\pi)$$

Therefore,

$$Y \otimes Z \cong (Im(\beta) \otimes Z) \oplus (Ker(\pi) \otimes Z) = (Im(\beta \otimes 1)) \oplus (Ker(\pi) \otimes Z)$$

which implies that the map $\beta \otimes 1$ is injective. □

Theorem 33. *If M is induced as a G-module, then $H_T^r(G, M) = 0 \ \forall \ r \in \mathbb{Z}$.*

Proof. For $r > 0$, it was already proved in previous sections.

Now we prove it for the case $r = 0$.

Recall that $M \cong \mathbb{Z}[G] \otimes X$ for some abelian group X. So it suffices to show $H_T^r(G, \mathbb{Z}[G] \otimes X) = 0$

Lemma 21. *Every element of $\mathbb{Z}[G] \otimes X$ can be written uniquely in the form $\sum g \otimes x_g$*

Proof. Let

$$\sum_{i=1}^{m} g_i \otimes x_{g_i} = \sum_{j=1}^{n} g_{m+j} x_{g_{m+j}}$$

such that $g_i \neq g_j$ if $1 \leq i < j \leq m$ and $g_{m+i} \neq g_{m+j}$ if $1 \leq i < j \leq n$.

Apply the isomorphism $\beta : \mathbb{Z}[G] \otimes X \to Ind^G X$ (decribed in the proof of Theorem 10) on both sides to get,

$$\sum_{i=1}^{m} \phi_{g_i, x_{g_i}} = \sum_{i=1}^{n} \phi_{g_{m+i}, x_{g_{m+i}}}$$

L.H.S. is non-zero on the set $\{g_1^{-1}, g_2^{-1}, ...g_m^{-1}\}$ and R.H.S. is non-zero on the set $\{g_{m+1}^{-1}, g_{m+2}^{-1}, ...g_{m+n}^{-1}\}$ Hence $\{g_1, ...g_m\} = \{g_{m+1}, ...g_{m+n}\}$. In particular $m = n$, and so $\{g_1, ...g_m\} = \{g_{m+1}, ...g_{2m}\}$ Rearrange g_i such that $g_{m+i} = g_i \ \forall \ 1 \leq i \leq m$ and we are done. □

Now we continue our proof of the case $r = 0$ of Theorem 33.

Any element m of M can be written uniquely in the form $\sum_g g \otimes x_g$. If g' fixes m, then $g' \left(\sum_g g \otimes x_g \right) = \sum_g g \otimes x_g$ and so $\sum_g g' g \otimes x_g = \sum_g g \otimes x_g$. Comparing the terms having g' in the first coordinate, we get $g' \otimes x_e = g' \otimes x_{g'} \ \forall \ g' \in G$. Thus $x'_g = x_e$ again by Lemma 21.

Now let $x \in M^G$, then $gx = x \ \forall \ g \in G$, which implies that $x_g = x_e \ \forall \ g \in G$ by the observation in the preceding paragraph. Then

$$x = \sum_g g \otimes x_g = \sum_g g \otimes x_e = \sum_g g(e \otimes x_e) = Nm(e \otimes x_e)$$

Therefore, $M^G \subset \mathrm{Nm}_G M$ and so $H_T^0(G, M) = 0$

Next we will prove the Theorem for the case $r = -1$.

If $\sum_g g \otimes x_g \in KerNm_G$, then $Nm_G(\sum_g g \otimes x_g) = 0$ and so

$$\sum_{g'} g' \sum_g g \otimes x_g = 0$$

which implies that

$$\sum_g \sum_{g'} g' g \otimes x_g = 0$$

Calculating terms having 1 in the first coordinate (i.e. $g' = g^{-1}$), we get

$$\sum_{g \in G} 1 \otimes x_g = 0$$

by Theorem 21. Then

$$\sum_g g \otimes x_g = \sum_g (g - 1) \otimes x_g + \sum_g 1 \otimes x_g = \sum_g (g - 1) \otimes x_g \in I_G M$$

Hence we have proved that $Ker(Nm_G) \subset I_G M$ and so $H_{-1}(G, M) = 0$

Finally we prove the Theorem for the case $r < -1$.

Let $M = \mathbb{Z}[G] \otimes X$. Write X as a quotient of a free abelian group X_0. Then we have a surjective map $X_0 \to X$. The kernel of this map X_1 is also a free abelian group because every subgroup of a free abelian group is free abelian.

Hence we have an exact sequence

$$0 \to X_1 \to X_0 \to X \to 0$$

where X_0 and X_1 are free abelian groups.

Since $\mathbb{Z}[G]$ is a free $\mathbb{Z}$-module, so it is flat and therefore, upon tensoring with $\mathbb{Z}[G]$, we get an exact sequence,

$$0 \to M_1 \to M_0 \to M \to 0$$

where $M_1 = \mathbb{Z}[G] \otimes X_1$ and $M_0 = \mathbb{Z}[G] \otimes X_0$. By the previous cases, we know that $H_T^r(G, M_0) = H_T^r(G, M_1) = 0 \; \forall \; r \geq -1$.

But M_1 is a free G-module since X_1 is a free abelian group. Similarly M_0 is a free G-module. Hence M_0 and M_1 are projective as G-modules and thus $H_r(G, M_0) = H_r(G, M_1) = 0$ for all $r \geq 0$ which means that $H_T^r(G, M_0) = H_T^r(G, M_1) = 0$ for all $r \leq -2$. Since we already know by the previous cases that $H_T^r(G, M_0) = H_T^r(G, M_1) = 0$ for all $r \geq -1$, so we get $H_T^r(G, M_0) = H_T^r(G, M_1) = 0$ for all $r \in \mathbb{Z}$. Now by Theorem 32, we know that the Tate cohomology sequence

$$... \to H_T^r(G, M_0) \to H_T^r(G, M) \to H_T^{r+1}(G, M_1) \to ...$$

is exact which shows that $H_T^r(G, M) = 0$ for all $r \in \mathbb{Z}$. □

2.12 Alternative approach to Tate Cohomology

Now we describe an alternate description of Tate cohomology as described in [2]. In the later sections, we will use both the descriptions interchangeably. All cohomology groups will be Tate and we will drop the subscript T.

2.12.1 Cohomology groups

Throughout this section, we will assume that G is a finite group. For $q \geq 1$, we consider all q-tuples $(\sigma_1, ..., \sigma_q)$, where the σ_i run through the group G. We use these q-tuples to generate G-modules X_q i.e. we define

$$X_q = X_{-q-1} = \bigoplus \mathbb{Z}[G](\sigma_1, ..., \sigma_q)$$

For $q = 0$, we put

$$X_0 = X_{-1} = \mathbb{Z}[G]$$

where we choose $1 \in \mathbb{Z}[G]$ as the generator. In particular, the modules

$$..., X_{-2}, X_{-1}, X_0, X_1, X_2, ...$$

are free G-modules. For any G-module A, we set

$$A_q = Hom_G(X_q, A)$$

There is an exact sequence

$$... \xleftarrow{d_{-2}} X_{-2} \xleftarrow{d_{-1}} X_{-1} \xleftarrow{d_0} X_0 \xleftarrow{d_1} X_1 \xleftarrow{d_2} X_2 \xleftarrow{d_3} ...$$

which induces the complex

$$... \xrightarrow{\partial_{-2}} A_{-2} \xrightarrow{\partial_{-1}} A_{-1} \xrightarrow{\partial_0} A_0 \xrightarrow{\partial_1} A_1 \xrightarrow{\partial_2} A_2 \xrightarrow{\partial_3} ...$$

Contrary to the first sequence, the second sequence need not be exact.

Definition 7. *For all $q \in \mathbb{Z}$, we define the factor group*

$$H^q(G, A) = Ker(\partial_{q+1})/Im(\partial_q)$$

is called the q^{th} cohomology group with coefficients in A.

Theorem 34. *If*

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

is an exact sequence of G-modules, then there exists a canonical homomorphism

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

Detailed description of the maps d_q , ∂_q and δ_q can be found on page 13, 16 and 21 respectively of [2].

Theorem 35. *If*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & B & \xrightarrow{j} & C & \longrightarrow & 0 \\ & & \downarrow f & & \downarrow g & & \downarrow h & & \\ 0 & \longrightarrow & A' & \xrightarrow{i'} & B' & \xrightarrow{j'} & C' & \longrightarrow & 0 \end{array} \tag{2.29}$$

is a commutative diagram of G-modules with exact rows, then the following diagram is also commutative :

$$\begin{array}{ccc} H^q(G, C) & \xrightarrow{\delta_q} & H^{q+1}(G, A) \\ \downarrow \bar{h}_q & & \downarrow \bar{f}_{q+1} \\ H^q(G, C') & \xrightarrow{\delta_q} & H^{q+1}(G, A') \end{array} \tag{2.30}$$

where $\bar{h}_q$ is the map induced by h and $\bar{f}_{q+1}$ is the map induced by f on the cohomology groups of dimension q and $(q+1)$ respectively.

Proof. The proof follows immediately from the description of δ_q. See Proposition 3.5, Page 24, [2] for details. □

2.12.2 Dimension Shifting

From now onwards, we denote the element $\sum_{\sigma \in G} \sigma$ of $\mathbb{Z}[G]$ by N_G. By $N_G(a)$, we would mean $\sum_{\sigma \in G} \sigma a$. Define the homomorphism

$$\epsilon : \mathbb{Z}[G] \to \mathbb{Z}$$

with

$$\epsilon \left(\sum_{\sigma \in G} n_\sigma \sigma \right) = \sum_{\sigma \in G} n_\sigma$$

and the homomorphism

$$\mu : \mathbb{Z} \to \mathbb{Z}[G]$$

such that $\mu(n) = nN_G$ We denote by I_G the augmentation ideal (Kernel of ϵ) of $\mathbb{Z}[G]$ and J_G the factor module $\mathbb{Z}[G]/\mathbb{Z}N_G$. Then we get the exact sequences (which are known as the augmentation and coaugmentation sequence respectively)

$$0 \to I_G \to \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \to 0,$$

$$0 \to \mathbb{Z} \xrightarrow{\mu} \mathbb{Z}[G] \to J_G \to 0$$

All terms in these exact sequences are free $\mathbb{Z}$-modules (See Proposition (1.2), page 4, [2] for proof).

Lemma 22. *For all G-modules A, we have the exact sequences*

$$0 \to I_G \otimes A \to \mathbb{Z}[G] \otimes A \to A \to 0$$

and

$$0 \to A \to \mathbb{Z}[G] \otimes A \to J_G \otimes A \to 0$$

Proof. It follows directly from Lemma 20. □

We know by Theorem 10 that $\mathbb{Z}[G] \otimes M$ is an induced module and so by Theorem 33, for every q and every subgroup $H \in G$. we have isomorphisms

$$\delta : H^{q-1}(H, A^1) \to H^q(H, A)$$

where $A^1 = J_G \otimes A$ and

$$\delta^{-1} : H^{q+1}(H, A^{-1}) \to H^q(H, A)$$

where $A^{-1} = I_G \otimes A$. We can iterate this process.

For every $m \in \mathbb{Z}$ such that $m > 0$, set

$$A^m = J_G \otimes J_G \otimes ... \otimes J_G \otimes A$$

where the number of times J_G appears in the tensor product is m.

For every $m \in \mathbb{Z}$ such that $m < 0$, set

$$A^m = I_G \otimes I_G \otimes ... \otimes I_G \otimes A$$

where the number of times I_G appears in the tensor product is $|m|$.

Composition of the isomorphism δ (or δ^{-1}) with itself $|m|$ times gives us the isomorphism

$$\delta^m : H^{q-m}(H, A^m) \to H^q(H, A)$$

This technique will help us to reduce many definitions and proofs to the case of zero-dimensional cohomology which we understand better. This method is called the method of dimension shifting.

We demonstrate an immediate application of dimension shifting.

Lemma 23. *Let G be a finite group of order n and A be a G-module. Then*

$$nH^q(G, A) = 0$$

for all $q \in \mathbb{Z}$.

Proof. If $q = 0$, then $na = N_G(a)$ for any $a \in A^G$ and so $n(a + N_G A) = na + N_G A = 0$. This proves the Lemma for $q = 0$ case. The general case now follows from the commutative diagram :

$$\begin{array}{ccc} H^0(G, A^q) & \xrightarrow{\delta^q} & H^q(G, A) \\ \Big\downarrow n & & \Big\downarrow n \\ H^0(G, A^q) & \xrightarrow{\delta^q} & H^q(G, A) \end{array} \tag{2.31}$$

□

Definition 8. *An abelian group A is said to be uniquely divisible if for every $a \in A$ and every natural number n, the equation $nx = a$ has a unique solution.*

Corollary 4. *A uniquely divisible G-module A has trivial cohomology.*

Proof. Let $n = |G|$. Since A is uniquely divisible, the map $A \to A$ given by $x \mapsto nx$ is bijective and therefore induces an isomorphism

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

given by $\bar{\phi} \mapsto n\bar{\phi}$. Therefore,

$$H^q(G, A) \cong nH^q(G, A) = 0$$

□

With the help of the dimension shifting technique, we can get an analogue of the inflation restriction exact sequence (Theorem 24) for higher dimensions though only under certain conditions.

Theorem 36. *Let A be a G-module and H is a normal subgroup of G. If $H^i(H, A) = 0$ for $0 < i < q$ and $q \geq 1$, then the sequence*

$$0 \to H^q(G/H, A^H) \xrightarrow{inf} H^q(G, A) \xrightarrow{res} H^q(H, A)$$

is exact.

Proof. We prove this by induction on q. The base case $q = 1$ has already been proved (Theorem 24). Now assume $q > 1$ and set $B = \mathbb{Z}[G] \otimes A$ and $C = J_G \otimes A$. We have an exact sequence

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

By the hypothesis of the theorem, we have

$$H^1(G, A) = 0$$

and thus the long exact sequence for cohomology (Theorem 18) shows that the following sequence is also exact :

$$0 \to A^H \to B^H \to C^H \to 0$$

Now by Theorem 27 and Theorem 25, we have the following commutative diagram :

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^{q-1}(G/H, C^H) & \xrightarrow{inf} & H^{q-1}(G, C) & \xrightarrow{res} & H^{q-1}(H, C) \\
 & & \downarrow \delta & & \downarrow \delta & & \downarrow \delta \\
0 & \longrightarrow & H^q(G/H, A^H) & \xrightarrow{inf} & H^q(G, A) & \xrightarrow{res} & H^q(H, C)
\end{array} \tag{2.32}$$

Since B is an induced G-module by Theorem 10, so the middle vertical map is an isomorphism. Moreover by Theorem 12, B is an induced H-module and B^H is also an induced G/H module. Therefore, the first and third vertical maps are also isomorphisms.

Since the third vertical map is an isomorphism, so

$$H^i(H, C) \cong H^{i+1}(H, A) = 0$$

for all $0 < i < q - 1$. Thus C satisfies the hypothesis of the Theorem for $(q - 1)$ and therefore by the induction hypothesis, the sequence in the top row of the commutative diagram is exact. Since all the vertical maps are isomorphisms, so the sequence in bottom row is also exact and we are done. □

Theorem 37. *(Shapiro's Lemma) Let*

$$A = \bigoplus_{\sigma \in G/H} \sigma D$$

for some H-module $D \subset A$. Then the composition of homomorphisms

$$H^q(G, A) \xrightarrow{res} H^q(H, A) \xrightarrow{\overline{\pi}} H^q(H, D)$$

is an isomorphism where $\overline{\pi}$ is induced by the natural projection $A \xrightarrow{\pi} D$.

Proof. See Theorem 4.19, Page 43, [2]. □

If we take $A = Ind_H^G M$ and $D = M$, we know by proof of Theorem 11 that

$$A = \bigoplus_{\sigma \in G/H} \sigma D$$

Then by Theorem 37, we have

$$H^q(G, Ind_H^G(M)) \cong H^q(H, M)$$

2.12.3 Functorial Maps

We now see how the compatibility condition of Theorem 25 enables us to give a definition of restriction map on the whole Tate cohomology.

Definition 9. *Let G be a finite group and H a subgroup of G. Then restriction is the uniquely determined family of homomorphisms*

$$res_q : H^q(G, A) \to H^q(H, A)$$

with the properties :

1. If $q = 0$, then

$$res_0 : H^0(G, A) \to H^0(H, A)$$

is given by

$$a + N_G A \mapsto a + N_H A$$

2. For every exact sequence $0 \to A \to B \to C \to 0$ of G-modules, the following diagram is commutative :

$$\begin{array}{ccc} H^r(G, C) & \xrightarrow{\delta} & H^{r+1}(G, A) \\ \downarrow{\scriptstyle res_q} & & \downarrow{\scriptstyle res_{q+1}} \\ H^r(H, C) & \xrightarrow{\delta} & H^{r+1}(H, A) \end{array} \tag{2.33}$$

for all $q \in \mathbb{Z}$.

Condition 2 in the definition means that we have to define the res_q map by the commutative diagram :

$$\begin{array}{ccc} H^0(G, A^q) & \xrightarrow{\delta^q} & H^q(G, A) \\ \downarrow{\scriptstyle res_0} & & \downarrow{\scriptstyle res_q} \\ H^0(H, A^q) & \xrightarrow{\delta^q} & H^q(H, A) \end{array} \tag{2.34}$$

By Condition 1, we know the restriction maps res_0 in dimension 0. Since the horizontal maps in the diagram are isomorphisms, so we get unique maps res_q in dimension q.

Similarly we will define corestriction maps on the whole of Tate cohomology.

In case $q = -1$, we define the corestriction homomorphism

$$cor_{-1} : H^{-1}(H, A) \to H^{-1}(G, A)$$

given by

$$a + I_H A \mapsto a + I_G A$$

Lemma 24. *Let $0 \to A \to B \to C \to 0$ be an exact sequence of G-modules. Then the following diagram is commutative :*

$$\begin{array}{ccc} H^{-1}(H,C) & \xrightarrow{\delta} & H^0(H,A) \\ \Big\downarrow{\scriptstyle cor_{-1}} & & \Big\downarrow{\scriptstyle cor_0} \\ H^{-1}(G,C) & \xrightarrow{\delta} & H^0(G,A) \end{array} \tag{2.35}$$

Proof. This can be shown by using the description of the corestriction map in dimension 0 given in Remark 7 and the description of the map $H^{-1}(H,C) \to H^0(H,A)$ provided in Remark 2.21. □

Definition 10. *Let G be a finite group, and let H be a subgroup of G. Then corestriction is the uniquely determined family of homomorphisms*

$$cor_q : H^q(H,A) \to H^q(G,A)$$

with the properties :

1. If $q = 0$, then

$$cor_0 : H^0(H,A) \to H^0(G,A)$$

is given by

$$a + N_H A \mapsto N_{G/H} a + N_G A$$

2. For every exact sequence $0 \to A \to B \to C \to 0$ of G-modules, the following diagram is commutative

$$\begin{array}{ccc} H^r(H,C) & \xrightarrow{\delta} & H^{r+1}(H,A) \\ \Big\downarrow{\scriptstyle cor_q} & & \Big\downarrow{\scriptstyle cor_{q+1}} \\ H^r(G,C) & \xrightarrow{\delta} & H^{r+1}(G,A) \end{array} \tag{2.36}$$

for all $q \in \mathbb{Z}$.

Condition 2 in the definition means that we have to define the cor_q map by the commutative diagram :

$$\begin{array}{ccc} H^0(H,A^q) & \xrightarrow{\delta^q} & H^q(H,A) \\ \Big\downarrow{\scriptstyle cor_0} & & \Big\downarrow{\scriptstyle cor_q} \\ H^0(G,A^q) & \xrightarrow{\delta^q} & H^q(G,A) \end{array} \tag{2.37}$$

Theorem 38. *Let $H \subset G$ be a subgroup. The homomorphism*

$$\kappa : H^{ab} \to G^{ab}$$

induced by the corestriction homomorphism $cor_{-2} : H^{-2}(H,\mathbb{Z}) \to H^{-2}(G,\mathbb{Z})$ coincides with the canonical injective homomorphism $\sigma H^c \mapsto \sigma G^c$.

Proof. We have the exact sequence

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

By condition 2 in the definition of corestriction maps, we have a commutative diagram :

$$\begin{array}{ccc} H^{-2}(H,\mathbb{Z}) & \xrightarrow{\delta} & H^{-1}(H,I_G) \\ \downarrow{\scriptstyle cor_{-2}} & & \downarrow{\scriptstyle cor_{-1}} \\ H^{-2}(G,\mathbb{Z}) & \xrightarrow{\delta} & H^{-1}(G,I_G) \end{array} \tag{2.38}$$

Moreover by Theorem 35, we get the commutativity of the following diagram :

$$\begin{array}{ccc} H^{-2}(H,\mathbb{Z}) & \xrightarrow{\delta} & H^{-1}(H,I_H) \\ \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle f_{-1}} \\ H^{-2}(H,\mathbb{Z}) & \xrightarrow{\delta} & H^{-1}(H,I_G) \end{array} \tag{2.39}$$

where f_{-1} is the map induced by the inclusion map $I_H \to I_G$. Composition of these two diagrams gives us the following commutative diagram :

$$\begin{array}{ccc} H^{-2}(H,\mathbb{Z}) & \xrightarrow{\delta} & H^{-1}(H,I_H) \\ \downarrow{\scriptstyle cor_{-2}} & & \downarrow{\scriptstyle cor_{-1}\circ f_{-1}} \\ H^{-2}(G,\mathbb{Z}) & \xrightarrow{\delta} & H^{-1}(G,I_G) \end{array} \tag{2.40}$$

By the description of cor_{-1} and f_{-1}, we have $cor_{-1} \circ f_{-1}$ is just the inclusion map $I_H/I_H^2 \to I_G/I_G^2$. By the proof of Theorem 31, we know that the following diagram commutes :

$$\begin{array}{ccccc} H^{-2}(H,\mathbb{Z}) & \xrightarrow{\delta} & H^{-1}(H,I_H) & \longrightarrow & H^{ab} \\ \downarrow{\scriptstyle cor_{-2}} & & \downarrow{\scriptstyle cor_{-1}\circ f_{-1}} & & \downarrow{\scriptstyle i} \\ H^{-2}(G,\mathbb{Z}) & \xrightarrow{\delta} & H^{-1}(G,I_G) & \longrightarrow & G^{ab} \end{array} \tag{2.41}$$

Thus the map $H^{ab} \to G^{ab}$ induced by cor_{-2} is same as that induced by $cor_{-1} \circ f_{-1}$ which is the inclusion map. □

Definition 11. *For any abelian group A and prime number p, we define the p-primary component $A(p)$ of A to be the subgroup consisting of all elements killed by a power of p.*

Theorem 39. *Let $H \subset G$ be a subgroup. Then the composition*

$$H^q(G, A) \xrightarrow{res} H^q(H, A) \xrightarrow{cor} H^q(G, A)$$

is given as :

$$cor \circ res = (G : H)\ id$$

Proof. We have already shown this for all cohomology groups and hence it can be shown for all Tate cohomology groups using dimension shifting. □

Corollary 5. *Let G be a finite group, and let G_p be its Sylow p-subgroup. For every G-module M, the restriction map*

$$Res : H^r(G, M) \to H^r(G_p, M)$$

is injective on the p-primary component of $H^r(G, M)$.

Proof. By Theorem 39, we know that the composite

$$Cor \circ Res : H^r(G, M) \to H^r(G_p, M) \to H^r(G, M)$$

is multiplication by $(G : G_p)$. Let γ be in the p-primary component of $H^r(G, M)$ such that $Cor(Res(\gamma)) = 0$. This means that $(G : G_p)\gamma = 0$. But also $p^k\gamma = 0$ for some $k \in \mathbb{N}$ since γ is in the p-primary component of $H^r(G, M)$. Since G_p is the Sylow p-subgroup of G, so p does not divide $(G : G_p)$. This shows that $\gcd(p^k, (G : G_p)) = 1$, so there exist integers a and b such that $ap^k + b(G : G_p) = 1$. Since $p^k\gamma = (G : G_p)\gamma = 0$, so $\gamma = 0$ and thus $Cor \circ Res$ is injective on the p-primary component of $H^r(G, M)$ which in particular means that Res is injective on the p-primary component of $H^r(G, M)$. □

2.12.4 Cup Products

Let A and B be G-modules. Then $A \otimes B$ is a G-module, and the map $(a, b) \mapsto a \otimes b$ induces a canonical mapping

$$A^G \times B^G \to (A \times B)^G$$

which maps $N_G A \times N_G B$ to $N_G(A \otimes B)$. Hence the tensor product induces a bilinear mapping

$$H^0(G, A) \times H^0(G, B) \to H^0(G, A \otimes B)$$

given by

$$(\overline{a}, \overline{b}) \mapsto \overline{a \otimes b}$$

We call the element $\overline{a \otimes b} \in H^0(G, A \otimes B)$ the cup product of $\overline{a} \in H^0(G, A)$ and $\overline{b} \in H^0(G, B)$, and denote it by

$$\overline{a} \cup \overline{b} = \overline{a \otimes b}$$

Now we will show how the cup product extends to arbitrary dimensions just from this case.

Definition 12. *There exists a unique family of bilinear mappings*

$$H^p(G,A) \times H^q(G,B) \to H^{p+q}(G, A \otimes B)$$

defined for all G-modules A and B and all p, q non-negative integers satisfying the following conditions :

1. *For $p = q = 0$, the pairing is given by*

$$(\overline{a}, \overline{b}) \mapsto \overline{a \otimes b}$$

2. *If*

$$0 \to A \to A' \to A'' \to 0$$

is an exact sequence of G-modules such that

$$0 \to A \otimes B \to A' \otimes B \to A'' \otimes B \to 0$$

is also exact, then

$$\delta a'' \cup b = \delta(a'' \cup b)$$

where $a'' \in H^p(G, A''), b \in H^q(G,B)$ and δ denotes the connecting homomorphisms

$$H^p(G, A'') \to H^{p+1}(G, A)$$

and

$$H^{p+q}(G, A'' \otimes B) \to H^{p+q+1}(G, A \otimes B)$$

3. *If*

$$0 \to B \to B' \to B'' \to 0$$

is an exact sequence of G-modules such that

$$0 \to A \otimes B \to A \otimes B' \to A \otimes B'' \to 0$$

is also exact, then

$$a \cup \delta b'' = (-1)^p \delta(a \cup b'')$$

where $a \in H^p(G,A), b'' \in H^q(G, B'')$

We will use these three conditions to give the definition of cup product in arbitrary dimensions (p,q). We know the cup product map in the dimension $(0,0)$ by Condition 1. The strategy is to go from $(0,0)$ to $(p,0)$ through Condition 2 and then from $(p,0)$ to (p,q) through Condition 3.

To go from $(p,0)$ to (p,q), we would need the identification $(A \otimes B)^q$ with $(A \otimes B^q)$. To see this, observe that if $q > 0$, then

$$B^q = J_G \otimes J_G \otimes ... J_G \otimes B$$

and so

$$A \otimes B^q = A \otimes J_G \otimes J_G \otimes ...J_G \otimes B$$

which is naturally identified with

$$J_G \otimes J_G \otimes ...J_G \otimes (A \otimes B) = (A \otimes B)^q$$

Similarly if $q < 0$, then

$$B^q = I_G \otimes I_G \otimes ...I_G \otimes B$$

and so

$$A \otimes B^q = A \otimes I_G \otimes I_G \otimes ...I_G \otimes B$$

which is naturally identified with

$$I_G \otimes I_G \otimes ...I_G \otimes (A \otimes B) = (A \otimes B)^q$$

Hence in either case, $(A \otimes B)^q$ can be identified with $(A \otimes B^q)$.

Similarly we can identify $(A \otimes B^q)^p$ with $A^p \otimes B^q$. This would be required to go from $(0, 0)$ to $(p, 0)$.

For any $b \in H^0(G, B^q)$, condition 2 of the definition gives us the commutative diagram :

$$\begin{array}{ccc} H^0(G, A^p) & \xrightarrow{\cup\, b} & H^0(G, A^p \otimes B^q) \\ \Big\downarrow{\scriptstyle \delta^p} & & \Big\downarrow{\scriptstyle \delta^p} \\ H^p(G, A) & \xrightarrow{\cup\, b} & H^p(G, A \otimes B^q) \end{array} \tag{2.42}$$

Since we know the map in the $(0, 0)$ level (upper row), so we obtain a unique map in the $(p, 0)$ level (lower row).

For any $a \in H^p(G, A)$, condition 3 of the definition gives us the commutative diagram :

$$\begin{array}{ccc} H^0(G, B^q) & \xrightarrow{a\, \cup} & H^p(G, (A \otimes B)^q) \\ \Big\downarrow{\scriptstyle \delta^q} & & \Big\downarrow{\scriptstyle (-1)^{pq}\delta^q} \\ H^q(G, B) & \xrightarrow{a\, \cup} & H^{p+q}(G, A \otimes B) \end{array} \tag{2.43}$$

Since we know the map in the $(p, 0)$ level (upper row) by the previous diagram, so we get a unique map in the (p, q) level (lower row).

Note that here we get the factor $(-1)^{pq}$ because on applying δ once we get a factor of $(-1)^p$ by Condition 3 of the definition and here we are applying it $|q|$ times.

Remark 12. *We have shown how these three conditions uniquely determine the cup product but we still need to show that the cup product so defined satisfies condition* 2 *and* 3*. This is a natural but lengthy check. Please refer to Page* 46, 47, *[2] for details.*

2.12.5 Properties of Cup Products

Theorem 40. *If we denote by a_p p-cocycles of A and by b_q q-cocylces of B, and by $\overline{a_p}$ and $\overline{b_q}$ their respective cohomology classes, then*

$$\overline{a_0} \cup \overline{b_q} = \overline{a_0 \otimes b_q}$$

and

$$\overline{a_p} \cup \overline{b_0} = \overline{a_p \otimes b_0}$$

Proof. This will follow directly from a more general description of cup product for all cohomology groups i.e. $q \geq 0$. This description is provided at the end of this section. □

Lemma 25. *Let A,B be G-modules, and let H be a subgroup of G. If $\bar{a} \in H^p(G, A)$ and $\bar{b} \in H^q(G, B)$, then*

$$res(\bar{a} \cup \bar{b}) = res(\bar{a}) \cup res(\bar{b}) \in H^{p+q}(H, A \otimes B)$$

Proof. Firstly, we prove this for the case $p = q = 0$. By condition 1 in the definiton of restriction map (Definition 9), we know that $res(\bar{a}) = res(a+N_G A) = a+N_H A$ and $res(\bar{b}) = res(b+N_G A) = b + N_H B$. Therefore by condition 1 in the definition of cup product (Definition 12), we have

$$res(\bar{a}) \cup res(\bar{b}) = (a \otimes b) + N_H(A \otimes B) = res(\bar{a} \cup \bar{b})$$

Thus in the $(0, 0)$ level, we have proved that the following square commutes :

$$\begin{array}{ccc} H^0(G, A^p) & \xrightarrow{\cup\, \bar{b}} & H^0(G, A^p \otimes B^q) \\ \downarrow{\scriptstyle res} & & \downarrow{\scriptstyle res} \\ H^0(H, A^p) & \xrightarrow{\cup\, (res\, \bar{b})} & H^0(H, A^p \otimes B^q) \end{array} \tag{2.44}$$

We can extend this square to a cube of which this square becomes the bottom face. The top face is constructed as :

$$\begin{array}{ccc} H^p(G, A) & \xrightarrow{\cup\, \bar{b}} & H^p(G, A \otimes B^q) \\ \downarrow{\scriptstyle res} & & \downarrow{\scriptstyle res} \\ H^p(H, A) & \xrightarrow{\cup\, (res\, \bar{b})} & H^p(H, A \otimes B^q) \end{array} \tag{2.45}$$

The vertical maps in the cube are all boundary maps used for dimension shifting (going from dimension 0 to dimension p) and are thus isomorphisms. The vertical squares also commute because we know that the diagram 2.42 commutes. This shows that the top squares also commute which means we have proven the theorem for the $(p, 0)$ case. Similarly, one can extend this proof for (p, q) level using the commutativity of diagram 2.43. □

Lemma 26. *Let A,B be G-modules, and let H be a subgroup of G. If $\bar{a} \in H^p(H, A)$ and $\bar{b} \in H^q(G, B)$, then*

$$cor(\bar{a} \cup res\bar{b}) = \bar{a} \cup cor(\bar{b}) \in H^{p+q}(G, A \otimes B)$$

Proof. We will prove this for $p = q = 0$ and then we would be done by dimension shifting. By condition 1 of definiton of restriction maps (Definition 9), we have $\bar{a} = a + N_G A$, $\bar{b} = b + N_G B$ and so $res(\bar{b}) = b + N_H B$ which implies

$$\bar{a} \cup (res\,\bar{b}) = a \otimes b + N_H(A \otimes B)$$

Thus

$$cor(\bar{a} \cup (res\,\bar{b})) = cor(a \otimes b + N_H(A \otimes B)) = \sum_{\sigma \in G/H} \sigma(a \otimes b) + N_G(A \otimes B)$$

by condition 1 of definition of corestriction maps (Definition 10). But we have

$$\sigma(a \otimes b) = \sigma(a) \otimes \sigma(b) = a \otimes \sigma(b)$$

since $\sigma \in G$ and $a \in A^G$. Therefore,

$$cor(\bar{a} \cup (res\,\bar{b})) = \sum_{\sigma \in G/H} a \otimes \sigma(b) + N_G(A \otimes B) = a \otimes \left(\sum_{\sigma \in G/H} \sigma(b) \right) + N_G(A \otimes B) = \bar{a} \cup cor\,\bar{b}$$

□

Lemma 27. *Let $\bar{a} \in H^p(G, A)$, $\bar{b} \in H^q(G, B)$, and $\bar{c} \in H^r(G, C)$. Then*

$$\bar{a} \cup \bar{b} = (-1)^{pq}(\bar{b} \cup \bar{a})$$

and

$$(\bar{a} \cup \bar{b}) \cup \bar{c} = \bar{a} \cup (\bar{b} \cup \bar{c})$$

where we are using the natural identification of $A \otimes B$ with $B \otimes A$ and $(A \otimes B) \otimes C$ with $A \otimes (B \otimes C)$.

Proof. We will prove this for $p = q = 0$ and then we would be done by dimension shifting. By condition 1 of definition 12, we know that

$$\bar{a} \cup \bar{b} = \overline{a \otimes b} = \overline{b \otimes a} = \bar{b} \cup \bar{a}$$

where we have used the identification of $A \otimes B$ with $B \otimes A$ given by $a \otimes b \mapsto b \otimes a$. Similarly, we have

$$(\bar{a} \cup \bar{b}) \cup \bar{c} = \bar{a} \cup (\bar{b} \cup \bar{c})$$

by the associativity of the tensor product. □

Remark 13. *More precisely, one should say that $(-1)^{pq}(\bar{b} \cup \bar{a})$ is the image of $\bar{a} \cup \bar{b}$ under the canonical isomorphism $H^{p+q}(G, A \otimes B) \cong H^{p+q}(G, B \otimes A)$ induced by $A \otimes B \cong B \otimes A$, and similarly for the second formula. This description is required for the dimension shifting step.*

Now we want to compute some explicit formulas for the cup product in low dimensions. These would turn out to be very useful in Local Class Field Theory. Now we denote by a_p the p-cocycles of A and by $\bar{a}_p$ their cohomology classes in $H^p(G, A)$. Similarly we denote by b_q the q-cocycles of B and by $\bar{b}_q$ their cohomology classes in $H^q(G, B)$.

Lemma 28. $\bar{a}_1 \cup \bar{b}_{-1} = \bar{x}_0 \in H^0(G, A \otimes B)$ *where*

$$x_0 = \sum_{\tau \in G} a_1(\tau) \otimes \tau b^{-1}$$

Proof. Consider the coaugmentation sequence

$$0 \to \mathbb{Z} \to \mathbb{Z}[G] \to J_G \to 0$$

Then by Lemma 20, we get the following exact sequences

$$0 \to A \to \mathbb{Z}[G] \otimes A \to J_G \otimes A \to 0$$

and

$$0 \to A \otimes B \to \mathbb{Z}[G] \otimes (A \otimes B) \to J_G \otimes (A \otimes B) \to 0$$

We denote $\mathbb{Z}[G] \otimes A$ by A' and $J_G \otimes A$ by A''. Therefore, we can rewrite the exact sequences as

$$0 \to A \to A' \xrightarrow{\pi} A'' \to 0$$

and

$$0 \to A \otimes B \to A' \otimes B \to A'' \otimes B \to 0$$

We think of A embedded in A' and $A \otimes B$ embedded in $A' \otimes B$. Since a_1 is a 1-cocycle in $C^1(G, A)$, so a_1 is also a 1-cocycle in $C^1(G, A')$. Since $H^1(G, A') = 0$, so a_1 is a coboundary in $C^1(G, A')$ i.e. $\exists\ a_0' \in A'$ such that $\forall\ \tau \in G$

$$a_1(\tau) = \tau(a_0') - a_0$$

Let $a_0'' = \pi(a_0')$ Now $\overline{a}_1 = \delta(\overline{a_0''})$ and therefore

$$\overline{a}_1 \cup \overline{b}_{-1} = \delta(\overline{a_0''}) \cup \overline{b_{-1}} = \delta(\overline{a_0''} \cup \overline{b_{-1}}) = \delta(\overline{a_0'' \otimes b_{-1}})$$

Now we need the description of the boundary map

$$H^{-2}(G, A'' \otimes B) \to H^{-1}(G, A \otimes B)$$

described in Remark 11.

Firstly note that $a_0' \otimes b_{-1}$ is a preimage of $a_0'' \otimes b_{-1}$ in $A' \otimes B$. Then we need to calculate $N_G(a_0' \otimes b_{-1})$. We have

$$N_G(a_0' \otimes b_{-1}) = \sum_{\tau \in G} \tau(a_0') \otimes \tau(b_{-1}) = \sum_{\tau \in G} (a_1(\tau) + a_0') \otimes \tau b_{-1} = \sum_{\tau \in G} a_1(\tau) \otimes \tau b_{-1} + a_0' \otimes N_G b_{-1}$$

By definition of b_{-1}, we know that $b_{-1} \in Ker(N_G)$ and so $N_G b_{-1} = 0$. Thus

$$N_G(a_0' \otimes b_{-1}) = \sum_{\tau \in G} a_1(\tau) \otimes \tau b_{-1}$$

Since it is already in A, its preimage in A is itself, so we get

$$\overline{a}_1 \cup \overline{b}_{-1} = \delta(\overline{a_0'' \otimes b_{-1}}) = \overline{x_0}$$

where

$$x_0 = \sum_{\tau \in G} a_1(\tau) \otimes \tau b_{-1}$$

and so we are done. □

Now we restrict our attention to the case $B = \mathbb{Z}$ and identify $A \otimes \mathbb{Z}$ with A under the map $a \otimes n \mapsto na$. Recall that we have the isomorphism

$$H^{-2}(G, \mathbb{Z}) \cong G^{ab}$$

If $\sigma \in G$, let $\bar{\sigma}$ be the element in $H^{-2}(G, \mathbb{Z})$ corresponding to $\sigma G^C \in G^{ab}$

Lemma 29. $\overline{a_1} \cup \overline{\sigma} = \overline{a_1(\sigma)} \in H^{-1}(G, A)$

Proof. The first thing we have to verify is that $a_1(\sigma) \in Ker(N_G)$ because then only we can talk about its cohomology class in $H^{-1}(G, A)$. To see this, note that

$$N_G(a_1(\sigma)) = \sum_{\tau \in G} \tau(a_1(\sigma)) = \sum_{\tau \in G} \tau(\sigma(a_0') - a_0') = \sum_{\tau \in G} \tau\sigma(a_0') - \sum_{\tau \in G} \tau(a_0') = 0$$

where a_0' is as in Lemma 28. Consider the augmentation sequence

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

By Lemma 20, we get that the following sequence is also exact :

$$0 \to A \otimes I_G \to A \otimes \mathbb{Z}[G] \to A \to 0$$

Since $A \otimes \mathbb{Z}[G]$ is an induced G-module, so we get the isomorphism

$$\delta : H^{-1}(G, A) \to H^0(G, A \otimes I_G)$$

Therefore, it suffices to show that

$$\delta(\overline{a_1} \cup \overline{\sigma}) = \delta(\overline{a_1(\sigma)})$$

To calculate, $\delta(\overline{a_1(\sigma)})$, we again need the description of the boundary map

$$H^{-2}(G, A'' \otimes B) \to H^{-1}(G, A \otimes B)$$

described in Remark 11.

Firstly observe that $a_1(\sigma) \otimes 1$ is a preimage of $a_1(\sigma)$ in $A \otimes \mathbb{Z}[G]$. Now we take its norm which is

$$\sum_{\tau \in G} \tau(a_1(\sigma) \otimes 1) = \sum_{\tau \in G} \tau(a_1(\sigma)) \otimes \tau$$

Finally we have to take a preimage of

$$\sum_{\tau \in G} \tau(a_1(\sigma)) \otimes \tau$$

in $A \otimes I_G$. Note that

$$\sum_{\tau \in G} \tau(a_1(\sigma)) \otimes \tau = \sum_{\tau \in G} \tau(a_1(\sigma)) \otimes (\tau - 1) + \sum_{\tau \in G} \tau(a_1(\sigma)) \otimes 1$$

But

$$\sum_{\tau \in G} \tau(a_1(\sigma)) \otimes 1 = \left(\sum_{\tau \in G} \tau(a_1(\sigma)) \right) \otimes 1 = N_G(a_1(\sigma)) \otimes 1 = 0$$

since $a_1(\sigma) \in Ker(N_G)$. Therefore,

$$\sum_{\tau \in G} \tau(a_1(\sigma)) \otimes \tau = \sum_{\tau \in G} \tau(a_1(\sigma)) \otimes (\tau - 1) \in A \otimes I_G$$

and thus $\sum_{\tau \in G} \tau(a_1(\sigma)) \otimes \tau$ is a preimage of itself in $A \otimes I_G$ and so we have

$$\delta(\overline{a_1(\sigma)}) = \overline{x_0}$$

where

$$x_0 = \sum_{\tau \in G} \tau(a_1(\sigma)) \otimes \tau$$

Now we will calculate $\delta(\overline{a_1} \cup \overline{\sigma})$.

From the proof of Theorem 31 and the definition of $\bar{\sigma}$, we have

$$\delta(\overline{\sigma}) = \overline{\sigma - 1}$$

Thus

$$\delta(\overline{a_1} \cup \overline{\sigma})) = -(\overline{a_1} \cup \delta(\overline{\sigma}) = -(\overline{a_1} \cup \overline{\sigma - 1}) = \overline{y_0}$$

By the previous lemma, we have

$$y_0 = -\sum_{\tau \in G} a_1(\tau) \otimes \tau(\sigma - 1) = \sum_{\tau \in G} a_1(\tau) \otimes \tau - \sum_{\tau \in G} a_1(\tau) \otimes \tau\sigma$$

Since a_1 is a cocycle, so $a_1(\tau) = a_1(\tau\sigma) - \tau(a_1(\sigma))$, and therefore,

$$\sum_{\tau \in G} a_1(\tau) \otimes \tau\sigma = \sum_{\tau \in G} a_1(\tau\sigma) \otimes \tau\sigma - \sum_{\tau \in G} \tau(a_1(\sigma)) \otimes \tau\sigma = \sum_{\tau \in G} a_1(\tau) \otimes \tau - \sum_{\tau \in G} \tau(a_1(\sigma)) \otimes \tau\sigma$$

Hence

$$y_0 = \sum_{\tau \in G} \tau(a_1(\sigma)) \otimes \tau\sigma = \sum_{\tau \in G} \tau(a_1(\sigma) \otimes \sigma)$$

Thus

$$y_0 - x_0 = \sum_{\tau \in G} \tau(a_1(\sigma) \otimes (\sigma - 1)) = N_G\left(a_1(\sigma) \otimes (\sigma - 1)\right)$$

which means

$$\overline{y_0} = \overline{x_0}$$

and so we are done. □

In fact for cohomology groups (i.e. $q \geq 0$), one can give an explicit description of the cup product.

Define the cup product pairing as

$$\Phi : H^r(G, M) \times H^s(G, N) \to H^{r+s}(G, M \otimes N)$$

such that

$$(m, n) \mapsto m \cup n$$

where $m \cup n$ is defined as follows.

Let ϕ be a cocycle representing m and ψ be a cocycle representing n.

Then $m \cup n$ is represented by the cocycle η of $H^{r+s}(G, M \otimes N)$ where η is given as :

$$\eta : G^{r+s} \to M \otimes N$$

such that

$$\eta(g_1, .., g_{r+s}) = \phi(g_1, .., g_r) \otimes (g_1, .., g_r \psi(g_{r+1}, .., g_{r+s}))$$

Firstly we will prove that η is infact a cocycle i.e. $d^{r+s}(\eta) = 0$ We have

$$\begin{aligned}(d^{r+s}(\eta))(g_1, g_2, ..., g_{r+s+1}) = g_1\eta(g_2, ..., g_{r+s+1}) + \sum_{j=1}^{r+s}(-1)^j \eta(g_1, ..., g_j g_{j+1}, ..., g_{r+s+1}) \\ +(-1)^{r+s+1}\eta(g_1, ..., g_{r+s})\end{aligned} \tag{2.46}$$

Now

$$\begin{aligned}g_1\eta(g_2, ..., g_{r+s+1}) &= g_1(\phi(g_2, ..., g_{r+1}) \otimes g_2...g_{r+1}(\psi(g_{r+2}, ..., g_{r+s+1}))) \\ &= g_1(\phi(g_2, ..., g_{r+1})) \otimes g_1...g_{r+1}\psi(g_{r+2}, ..., g_{r+s+1})\end{aligned} \tag{2.47}$$

and

$$\begin{aligned}\sum_{j=1}^{r+s}(-1)^j \eta(g_1, ..., g_j g_{j+1}, ..., g_{r+s+1}) = \sum_{j=1}^{r}(-1)^j \phi(g_1, ..., g_j g_{j+1}, ..., g_{r+1}) \otimes g_1...g_{r+1}\psi(g_{r+2}, ..., g_{r+s+1}) \\ + \sum_{j=r+1}^{r+s}(-1)^j \phi(g_1, ..., g_r) \otimes g_1...g_r\psi(g_{r+1}, ...g_j g_{j+1}, ..., g_{r+s})\end{aligned} \tag{2.48}$$

Making a change of variables $j = J + r$ in the second summation, we get

$$\begin{aligned}\sum_{j=1}^{r+s}(-1)^j \eta(g_1, ..., g_j g_{j+1}, ..., g_{r+s+1}) = \sum_{j=1}^{r}(-1)^j \phi(g_1, ..., g_j g_{j+1}, ..., g_{r+1}) \otimes g_1...g_{r+1}\psi(g_{r+2}, ..., g_{r+s+1}) \\ + (-1)^r \sum_{j=1}^{s}(-1)^j \phi(g_1, ..., g_r) \otimes g_1...g_r\psi(g_{r+1}, ...g_{r+j} g_{r+j+1}, ..., g_{r+s})\end{aligned} \tag{2.49}$$

Combining these equations together, we get

$$\begin{aligned}(d^{r+s}\eta)(g_1, g_2, ..., g_{r+s+1}) = g_1(\phi(g_2, ..., g_{r+1})) \otimes g_1...g_{r+1}\psi(g_{r+2}, ..., g_{r+s+1}) \\ + \sum_{j=1}^{r}(-1)^j \phi(g_1, ..., g_j g_{j+1}, ..., g_{r+1}) \otimes g_1...g_{r+1}(\psi(g_{r+2}, ..., g_{r+s+1})) + (-1)^r \phi(g_1, ...g_r) \otimes \\ g_1...g_r \left(\sum_{j=1}^{s}(-1)^j \phi(g_1, ..., g_r) \otimes g_1...g_r\psi(g_{r+1}, ...g_{r+j} g_{r+j+1}, ..., g_{r+s}) + (-1)^{s+1}\psi(g_{r+1}, ..., g_{r+s}) \right)\end{aligned} \tag{2.50}$$

The term in the big paranthesis becomes equal to

$$-g_{r+1}\psi(g_{r+2},...,g_{r+s+1})$$

since ψ is a cocycle. Therefore, we get $(d^{r+s}\eta)(g_1, g_2, ..., g_{r+s+1}) =$

$$\left(g_1(\phi(g_2,...,g_{r+1}) + \sum_{i=1}^{r}(-1)^j\phi(g_1,...,g_jg_{j+1},...,g_{r+s+1} + (-1)^{r+1}\phi(g_1,...,g_r)\right) \otimes g_1...g_{r+1}\psi(g_{r+2},...,g_{r+s+1}) \tag{2.51}$$

which is 0 since ϕ is also a cocycle.

Condition 1 is an immediate consequence of the definition of the cup product and the identification $C^0(G, M)$ with M. Conditions 2 and 3 can be proven by a direct but very lengthy check.

2.13 The Cohomology of Finite Cyclic Groups

$\mathbb{Q}, \mathbb{Z}$ and $\mathbb{Q}/\mathbb{Z}$ are regarded as G-modules with trivial action.

Lemma 30. *For every finite group G.*
1. $H^r_T(G,\mathbb{Q}) = 0 \ \forall \ r \in \mathbb{Z}$
2. $H^0_T(G,\mathbb{Z}) = \frac{Z}{(G:1)\mathbb{Z}}$
3. $H^1_T(G,\mathbb{Z}) = 0$
4. $H^2(G,\mathbb{Z}) \cong Hom(G,\mathbb{Q}/\mathbb{Z})$

Proof. Statement 1 is an immediate consequence of Corollary 4 since $\mathbb{Q}$ is a uniquely divisible group.

Clearly

$$H^0_T(G,\mathbb{Z}) = \frac{\mathbb{Z}^G}{Nm_G\mathbb{Z}} = \frac{\mathbb{Z}}{(G:1)\mathbb{Z}}$$

We also know that

$$H^1_T(G,\mathbb{Z}) = H^1(G,\mathbb{Z}) = Hom(G,\mathbb{Z})$$

Let $\phi : G \to \mathbb{Z}$ be a homomorphism. Take any $g \in G$. Then $g^n = e$ where $n = |G|$. Thus, $\phi(g^n) = n\phi(g) = 0$ which means that $\phi(g) = 0 \ \forall \ g \in G$. Therefore, $\phi = 0$ and we get $H^1(G,\mathbb{Z}) = 0$.

Consider the exact sequence

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

This sequence gives rise to a very long exact sequence

$$... \to H^1(G,\mathbb{Q}) \longrightarrow H^1(G,\mathbb{Q}/\mathbb{Z}) \longrightarrow H^2(G,\mathbb{Z}) \longrightarrow H^2(G,Q) \to ...$$

Since $H^1(G,\mathbb{Q}) = H^2(G,\mathbb{Q}) = 0$, we get

$$H^2(G,\mathbb{Z}) \cong H^1(G,\mathbb{Q}/\mathbb{Z}) = Hom(G,\mathbb{Q}/\mathbb{Z})$$

□

Theorem 41. *Let G be a cyclic group of finite order. A choice of a generator for G determines isomorphisms*

$$H_T^r(G, M) \to H_T^{r+2}(G, M)$$

for all G-modules M and all $r \in \mathbb{Z}$.

Proof. We have the augmentation sequence

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

Therefore by Lemma 20, we get that the sequence

$$0 \to I_G \otimes M \to \mathbb{Z}[G] \otimes M \to M \to 0$$

is also exact.

For any generator σ of G, it is straightforward to show that the sequence

$$0 \to \mathbb{Z} \xrightarrow{\eta_1} \mathbb{Z}[G] \xrightarrow{\eta_2} I_G \to 0$$

is also exact where $\eta_1(n) = nN_G = \sum_{g \in G} gn$ and $\eta_2(x) = (\sigma(x) - x)$ for all $x \in \mathbb{Z}[G]$.

Therefore by Lemma 20, we get that the sequence

$$0 \to M \xrightarrow{\eta_1 \otimes 1} \mathbb{Z}[G] \otimes M \xrightarrow{\eta_2 \otimes 1} I_G \otimes M \to 0$$

is also exact. Now we know that

$$\mathbb{Z}[G] \otimes M$$

is an induced G-module by Theorem 10 and so has trivial Tate cohomology by Theorem 33 i.e.

$$H_T^r(G, \mathbb{Z}[G] \otimes M) = 0$$

for all $r \in \mathbb{Z}$. From these two exact sequences, we get the isomorphisms

$$\delta : H_T^r(G, M) \to H_T^{r+1}(G, I_G \otimes M)$$

and

$$\delta : H_T^{r+1}(G, I_G \otimes M) \to H_T^{r+2}(G, M)$$

Combining these two isomorphisms, we get

$$H_T^r(G, M) \cong H_T^{r+2}(G, M)$$

for all $r \in \mathbb{Z}$. □

Let G be a finite cyclic group and let M be a G-module. If the cohomology groups $H^r(G, M)$ are finite (which means that all Tate cohomology groups are finite by Theorem 41), we define the Herbrand quotient of M to be

$$h(M) = \frac{|H_T^0(G, M)|}{|H_T^{-1}(G, M)|}$$

Theorem 42. *Let*

$$0 \to M' \to M \to M'' \to 0$$

be an exact sequence of G-modules. If any two of the Herbrand quotients $h(M')$, $h(M)$ and $h(M'')$ are defined, then the third is also defined and

$$h(M) = h(M')h(M'')$$

Proof. By Theorem 32, we know that there is a very long exact sequence

$$... \to H_T^{-1}(M) \to H_T^{-1}(M'') \to H_T^0(M') \to H_T^0(M) \to H_T^0(M'') \to H^1(M') \to H^1(M) \to H^1(M'') \to ...$$

The first statement in the proof now follows immediately.

We can truncate this sequence to get another exact sequence

$$0 \to K \to H_T^0(M') \to H_T^0(M) \to H_T^0(M'') \to H^1(M') \to H^1(M) \to H^1(M'') \to K' \to 0$$

where K is the cokernel of the map

$$H_T^{-1}(M) \to H_T^{-1}(M'')$$

and K' is the cokernel of the map

$$H_T^1(M) \to H_T^1(M'')$$

We know by Theorem 41 that $H_T^{-1}(M) \cong H_T^1(M)$ and $H_T^{-1}(M'') \cong H_T^1(M'')$. Under the same isomorphism, we get $K \cong K$.

To complete the proof of the second statement, we need a helping lemma :

Lemma 31. *Let*

$$A_0 \to A_1 \to .... \to A_r \to 0$$

be an exact sequence of finite groups. Then

$$\frac{|A_0|\ |A_2|\ |A_4|\ ...}{|A_1|\ |A_3|\ |A_5|\ ...} = 1$$

Proof. Firstly we prove it for $r = 2$ i.e. for short exact sequences.

Then we are given an exact sequence

$$0 \to A_0 \to A_1 \to A_2 \to 0$$

Thus

$$A_2 \cong \frac{A_1}{A_0}$$

which shows that

$$\frac{|A_0|\ |A_2|}{|A_1|} = 1$$

and we are done.

Now we prove the result in generality.

Note that if

$$A_0 \xrightarrow{\alpha_0} A_1 \xrightarrow{\alpha_1} \ldots \to A_{r-1} \xrightarrow{\alpha_{r-1}} A_r \to 0$$

is exact, then cokernel of the map α_{i-1} is

$$\frac{A_i}{Im(\alpha_{i-1})} = \frac{A_i}{Ker(\alpha_i)}$$

which by the first isomorphism theorem is isomorphic to

$$Im(\alpha_i) = Ker(\alpha_{i+1})$$

Hence for each i,

$$Coker(\alpha_{i-1}) = Ker(\alpha_{i+1})$$

We denote it by C_i i.e.

$$C_i = Coker(\alpha_{i-1}) = Ker(\alpha_{i+1})$$

The exact sequence can be broken into short exact sequences,

$$0 \to A_0 \to A_1 \to C_1 \to 0$$

$$0 \to C_1 \to A_2 \to C_2 \to 0$$

and so on till

$$0 \to C_{r-1} \to A_{r-1} \to A_r \to 0$$

We have

$$1 = \frac{|A_0|\ |C_1|}{|A_1|} = \frac{|A_0|\ |A_2|}{|A_1|\ |C_2|}$$

since $|C_1| = \frac{|A_2|}{|C_2|}$. Similarly

$$1 = \frac{|A_0|\ |A_2|\ |C_3|}{|A_1|\ |A_3|}$$

and so on. This completes the proof of Lemma 31. □

Now we continue our proof of Theorem 42. Applying this Lemma 31 to the exact sequence

$$0 \to K \to H^0_T(M') \to H^0_T(M) \to H^0_T(M'') \to H^1(M') \to H^1(M) \to H^1(M'') \to K' \to 0$$

we find that,

$$|H^0_T(M')|\ |H^0_T(M'')|\ |H^1(M)|\ |K'| = |K|\ |H^0_T(M)|\ |H^1(M')|\ |H^1(M'')|$$

Since $K \cong K'$, so $|K| = |K'|$ and the equation reduces to

$$|H^0_T(M')|\ |H^0_T(M'')|\ |H^1(M)| = |H^0_T(M)|\ |H^1(M')|\ |H^1(M'')|$$

Thus,

$$\frac{|H^0_T(M')|}{|H^1(M')|}\frac{|H^0_T(M'')|}{|H^1(M'')|} = \frac{|H^0_T(M)|}{|H^1(M)|}$$

Therefore,

$$h(M) = h(M')\ h(M'')$$

and we are done. □

Theorem 43. *If M is a finite module, then $h(M) = 1$.*

Proof. It is easy to verify that the sequence

$$0 \to M^G \xrightarrow{i} M \xrightarrow{\sigma - 1} M \xrightarrow{\pi} M_G \to 0$$

is exact where i is the inclusion map and π is the projection map. By Lemma 31, we obtain $|M^G| = |M_G|$. By the section on Tate groups (Equation 2.21), we know that there is an exact sequence

$$0 \to H_T^{-1}(M) \to M_G \xrightarrow{Nm_G} M^G \to H_T^0(M) \to 0$$

By Lemma 31 again, we get $|H_T^{-1}(M)| = |H_T^0(M)|$.

Hence $h(M) = 1$. □

Corollary 6. *Let $\alpha : M \to N$ be a homomorphism of G-modules with finite kernel and cokernel. If either $h(M)$ or $h(N)$ is defined, then so also is the other, and they are equal.*

Proof. Note that since $Ker(\alpha)$ and $Coker(\alpha)$ are finite, so $h(Ker(\alpha)) = h(Coker(\alpha)) = 1$. Suppose that $h(N)$ is defined. Consider the short exact sequence

$$0 \to \alpha(M) \to N \to Coker(\alpha) \to 0$$

Since $h(N)$ and $h(\text{Coker}(\alpha))$ are defined, so $h(\alpha(M))$ is also defined and is equal to $h(N)$ by Theorem 42. Also the following sequence is exact

$$0 \to Ker(\alpha) \to M \to \alpha(M) \to 0$$

Since $h(\alpha(M))$ and $h(\text{Ker}(\alpha))$ are defined, so $h(M)$ is also defined and equal to $h(N)$ by Theorem 42. □

2.14 Tate's Theorem

From now onwards all cohomology groups will be Tate groups and so we drop the subscript T except for the main statements.

Theorem 44. *Let G be a finite group and let M be a G-module. If $H^i(H, M) = H^{i+1}(H, M) = 0$ for all subgroups H of G for some $i \in \mathbb{Z}$, then $H_T^r(G, M) = 0 \ \forall\ r \in \mathbb{Z}$.*

Proof. If G is cyclic, this follows directly from Theorem 41 as $H^r(G, M) \cong H^1(G, M)$ if r is odd and $H^r(G, M) \cong H^2(G, M)$ if r is even.

Now let us assume that G is solvable. We will prove the theorem in this case by induction on $|G|$. Since G is a finite solvable group, so G has a finite composition series $G = G_0 \supset G_1 \supset ... \supset G_n$ such that G_{i+1} is normal in G_i and G_i/G_{i+1} is abelian for all i. Moreover, we can choose a refinement of the composition series such that G_i/G_{i+1} is a simple group for every i. Since a finite simple abelian group is cyclic, so G_i/G_{i+1} is a cyclic group for all i.

Therefore, G contains a proper normal subgroup H such that G/H is cyclic. Since $|H| < |G|$, $H^r(H, M) = 0 \ \forall\ r \in \mathbb{Z}$ by the induction hypothesis. Now we have the restriction - inflation exact sequences $\forall\ r \in \mathbb{N}$

$$0 \to H^r(G/H, M^H) \xrightarrow{Inf} H^r(G, M) \xrightarrow{Res} H^r(H, M)$$

Since $H^i(G,M) = 0$ and $H^{i+1}(G,M) = 0$, so $H^i(G/H, M^H)$ and $H^{i+1}(G/H, M^H)$ are also 0. Moreover, G/H is cyclic, thus $H^r(G/H, M^H) = 0 \; \forall\, r \in \mathbb{Z}$. Also since $H^r(H,M) = 0 \; \forall\, r \in \mathbb{Z}$, so by the exact sequence we get $H^r(G,M) = 0 \; \forall\, r \in \mathbb{N}$. Now we will show that $H^0_T(G,M) = 0$. Firstly we will use $Nm_G = Nm_{G/H} \circ Nm_H$ to prove this fact. Then we will prove $Nm_G = Nm_{G/H} \circ Nm_H$.

We know that

$$H^0_T(G,M) = \frac{M^G}{Nm_G M}$$

Take any $x \in M^G$, we want to show that $x \in Nm_G(M)$. We know that $H^0_T(G/H, M^H) = 0$. So,

$$(M^H)^{G/H} = Nm_{G/H} M^H$$

Note that

$$(M^H)^{G/H} = \{m \in M^H : gm = m \;\; \forall g \in G\} = M^G$$

Thus, $M^G = Nm_{G/H} M^H$ and so $x \in Nm_{G/H} M^H$. Therefore, $x = Nm_{G/H} y$ for some $y \in M^H$ Now $M^H = Nm_H M$ since $H^0(H,M) = 0$ and so $y = Nm_H z$ for some $z \in M$. Hence,

$$x = Nm_{G/H} Nm_H z = Nm_G z \in Nm_G(M)$$

since $Nm_{G/H} \circ Nm_H = Nm_G$,

Now we will prove $Nm_{G/H} \circ Nm_H = Nm_G$

We have,

$$Nm_{G/H} Nm_H z = Nm_{G/H} \left(\sum_{h \in H} hz \right) = \sum_{s \in S} s \sum_{h \; in H} hz = \sum_{s \in S} \sum_{h \in H} shz = \sum_{g \in G} gz = Nm_G z$$

where S is a set of coset representatives of H in G.

Now we have proved $H^r(G,M) = 0 \; \forall\, r \geq 0$.

We have the exact sequence

$$0 \to M' \to \mathbb{Z}[G] \otimes M \to M \to 0$$

from the previous section. Since $\mathbb{Z}[G] \otimes M$ is induced as a G-module, so it is also induced as an H-module by Theorem 12, thus $\forall\, r \in \mathbb{Z}$ and for all H' subgroup of G,

$$H^r(H', \mathbb{Z}[G] \otimes M) = 0$$

by Theorem 33. Thus $\forall\, r \in \mathbb{Z}$ and for all H' subgroup of G,

$$H^r(H', M) \cong H^{r+1}(H', M')$$

Since $H^i(H', M) = H^{i+1}(H', M) = 0$, so $H^{i+1}(H, M') = H^{i+2}(H, M') = 0$ and thus M' satisfies the hypothesis of the theorem.

Therefore, $H^r(G, M') = 0$ for all $r \geq 0$ because we had proved that whenever G is a solvable group and (G, M) satisfy the hypothesis of the Theorem, then $H^r(G, M) = 0 \ \forall \ r \geq 0$.

The isomorphism now proves that whenever G is a solvable group and (G, M) satisfy the hypothesis of the Theorem, then $H^r(G, M) = 0 \ \forall \ r \geq -1$.

Again since (G, M') satisfies the hypothesis, so $H^r(G, M') = 0 \ \forall \ r \geq -1$. But using the isomorphism again, we get $H^r(G, M) = 0 \ \forall \ r \geq -2$ and so on. Hence we have proved the theorem in the case when G is solvable.

Now consider the case of an arbitrary group G. Let G_p denote a Sylow p-subgroup. We know that G_p is solvable. If (G, M) satisfy the hypothesis of the theorem, so do $(G_p, M) \ \forall \ p$ since subgroups of G_p are also subgroups of G. Hence by Corollary 5, we know that p-primary component of $H^r(G, M)$ is $0 \ \forall \ p$. But since $H^r(G, M)$ has finite order as $|G|H^r(G, M) = 0$ by Theorem 23, so $H^r(G, M) = 0 \ \forall \ r \in \mathbb{Z}$ and we are done.

□

Theorem 45. *(Tate's Theorem) Let G be a finite group and let C be a G-module. Suppose that for all subgroups H of G,*
1. $H^1(H, C) = 0$, and
2. $H^2(H, C)$ is a cyclic group of order equal to $(H : 1)$. Then, for all r, there is an isomomorphism

$$H^r(G, \mathbb{Z}) \to H^{r+2}(G, C)$$

depending only on the choice of generator for $H^2(G, C)$.

Proof. Choose a generator γ for $H^2(G, C)$. We will show that $Res(\gamma)$ generates $H^2(H, C)$ for any subgroup H of G.

For any $i < |H|$, we have $i(G : H) < |G|$ and thus

$$Cor(iRes(\gamma)) = iCor(Res(\gamma)) = i(G : H)\gamma \neq 0$$

since γ is a generator for G. This shows that for any $i < |H|$,

$$iRes(\gamma) \neq 0$$

so $Res(\gamma)$ is a generator for $H^2(H, C)$ since we are given in the hypothesis that $H^2(H, C)$ is a cyclic group of order equal to $(H : 1)$.

Let ϕ be a cocycle representing γ.

Define

$$C(\phi) = C \oplus C_0(\phi)$$

where $C_0(\phi)$ is the free abelian group having basis symbols x_σ one for each $\sigma \in G$, $\sigma \neq 1$ and extend the action of G on C to an action on $C(\phi)$ as :

$$\sigma x_\tau = x_{\sigma\tau} - x_\sigma + \phi(\sigma, \tau)$$

The symbol x_1 is to be interpreted as $\phi(1,1)$. By this statement we mean that as σ, τ vary over G ($\tau \neq 1$), if $\sigma\tau = 1$, then $x_{\sigma\tau}$ is defined as $\phi(1,1)$. Also, if $\sigma = 1$, then x_σ is defined as $\phi(1,1)$. We will show that $C(\phi)$ is a G-module. We have

$$\rho(\sigma x_\tau) = \rho(x_{\sigma\tau} - x_\sigma + \phi(\sigma,\tau))$$

But

$$\rho(x_{\sigma\tau}) = x_{\rho\sigma\tau} - x_\rho + \phi(\rho, \sigma\tau)$$

and

$$\rho(x_\sigma) = x_{\rho\sigma} - x_\rho + \phi(\rho, \sigma)$$

Hence

$$\rho(\sigma x_\tau) = x_{\rho\sigma\tau} - x_{\rho\sigma} + \phi(\rho, \sigma\tau) - \phi(\rho,\sigma) + \rho(\phi(\sigma,\tau))$$

Since ϕ is a cocycle,

$$\rho(\phi(\sigma,\tau)) + \phi(\rho,\sigma\tau) = \phi(\rho,\sigma) + \phi(\rho\sigma,\tau)$$

Thus

$$\rho(\sigma x_\tau) = x_{\rho\sigma\tau} - x_{\rho\sigma} + \phi(\rho\sigma,\tau) = (\rho\sigma)(x_\tau)$$

Also

$$1x_\tau = x_\tau - x_1 + \phi(1,1)$$

Since x_1 is interpreted as $\phi(1,1)$, so $1x_\tau = x_\tau$.

We will show that ϕ is coboundary of a 1-cochain in $C(\phi)$. Define

$$\psi : G \to C(\phi)$$

such that

$$\psi(\sigma) = x_\sigma$$

Then we get the map

$$d^1\psi : G^2 \to C(\phi)$$

such that

$$d^1\psi(\sigma,\tau) = \sigma\psi(\tau) - \phi(\sigma\tau) + \psi(\sigma) = \sigma x_\tau - x_{\sigma\tau} + x_\sigma = \phi(\sigma,\tau)$$

Therefore, $\phi = d^1\psi \in Im(d^1)$ and so $\bar{\phi} = 0$ in $H^2(G, C(\phi))$ which means that $\gamma \mapsto 0$ under the natural map $H^2(G,C) \to H^2(G,C(\phi))$. That is why $C(\phi)$ is called the splitting module for γ. We will now show that the hypothesis of the theorem implies that

$$H^1(H, C(\phi)) = H^2(H, C(\phi)) = 0$$

for all subgroups H of G.

We have the exact augmentation sequence

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

$\mathbb{Z}[G]$ is an induced G-module as $\mathbb{Z}[G] \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Z}$ and hence also an induced H-module by Theorem 12 which shows that $\forall\ r \in \mathbb{Z}$,

$$H^r(H, \mathbb{Z}[G]) = 0$$

by Theorem 33. Hence by the very long exact sequence for Tate groups,

$$H^1(H, I_G) \cong H^0(H, \mathbb{Z})$$

and

$$H^2(H, I_G) \cong H^1(H, \mathbb{Z})$$

Thus

$$H^1(H, I_G) \cong \frac{\mathbb{Z}}{|H|\mathbb{Z}}$$

and

$$H^2(H, I_G) = 0$$

by Lemma 30. Define the map

$$\alpha : C(\phi) \to \mathbb{Z}[G]$$

such that

$$\alpha(C) = 0, \;\; \alpha(x_\sigma) = \sigma - 1 \;\; \forall\, \sigma \in G, \; \sigma \neq 1$$

Clearly $\alpha(C(\phi)) \subset I_G$. We will show that

$$0 \to C \to C(\phi) \xrightarrow{\alpha} I_G \to 0$$

is an exact sequence. We only need to prove that $Ker(\alpha) = C$. Clearly $C \subset Ker(\alpha)$

Now let

$$\alpha\left(c + \sum_{i=1}^{K} n_i x_{\sigma_i}\right) = 0$$

Then

$$\alpha(c) + \alpha\left(\sum_{i=1}^{K} n_i x_{\sigma_i}\right) = 0$$

and therefore by definition of α,

$$\alpha\left(\sum_{i=1}^{K} n_i x_{\sigma_i}\right) = 0$$

which means that $\sum_{i=1}^{K} n_i \alpha(x_{\sigma_i}) = 0$ and so $\sum_{i=1}^{K} n_i(\sigma - 1) = 0$. Since I_G is a free $\mathbb{Z}$ module with basis $\{\sigma - 1 : \sigma \in G \text{ and } \sigma \neq 1\}$, so $n_i = 0 \;\forall\, i$ and hence $Ker(\alpha) \subset C$. This completes the proof that

$$0 \to C \to C(\phi) \xrightarrow{\alpha} I_G \to 0$$

is an exact sequence. The short exact sequence leads to a very long exact sequence, a part of which is as follows

$$H^1(H, C) \to H^1(H, C(\phi)) \to H^1(H, I_G) \to H^2(H, C) \to H^2(H, C(\phi)) \to H^2(H, I_G)$$

Since by the hypothesis, $H^1(H, C) = 0$ and we have shown that $H^2(H, I_G) = 0$
Thus the exact sequence reduces to

$$0 \to H^1(H, C(\phi)) \to H^1(H, I_G) \xrightarrow{\eta} H^2(H, C) \xrightarrow{\beta} H^2(H, C(\phi)) \to 0$$

It is straightforward to check that the following diagram commutes :

$$\begin{array}{ccc} H^2(G,C) & \longrightarrow & H^2(G,C(\phi)) \\ \Big\downarrow{\scriptstyle res} & & \Big\downarrow{\scriptstyle res} \\ H^2(H,C) & \longrightarrow & H^2(H,C(\phi)) \end{array} \tag{2.52}$$

where the horizontal arrows are induced by the inclusion map $C \to C(\phi)$.

Since we already know that $\gamma \mapsto 0$ under the map $H^2(G,C) \to H^2(G,C(\phi))$, so $Res(\gamma) \mapsto 0$ under the the map $H^2(H,C) \to H^2(H,C(\phi))$. Since $H^2(H,C)$ is generated by Res(γ), thus β is the zero map and so η is onto.

But we also know that $H^1(H,I_G) \cong \frac{\mathbb{Z}}{|H|\mathbb{Z}}$ and therefore, $|H^1(H,I_G)| = (H:1)$. Since we are also given in the hypothesis that $|H^2(H,C)| = (H:1)$, so $|H^1(H,I_G)| = |H^2(H,C)|$ and the map η is infact an isomorphism.

Hence $Ker(\eta) = Coker(\eta) = 0$ i.e,

$$H^1(H,C(\phi)) = H^2(H,C(\phi)) = 0$$

Thus by Theorem 44, $\forall\ r \in \mathbb{Z}$

$$H^r(G,C(\phi)) = 0$$

We have two exact sequences

$$0 \to C \to C(\phi) \xrightarrow{\alpha} I_G \to 0$$

$$0 \to I_G \xrightarrow{i} \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

Now $H^r(G,C(\phi)) = H^r(G,\mathbb{Z}[G]) = 0\ \forall\ r \in \mathbb{Z}$,

The second exact sequence gives us the isomorphism

$$\delta : H^r(G,\mathbb{Z}) \to H^{r+1}(G,I_G)$$

while the first exact sequence gives us the isomorphism

$$\delta : H^{r+1}(G,I_G) \to H^{r+2}(G,C)$$

Composing these maps, we get the isomorphism

$$H^r(G,\mathbb{Z}) \to H^{r+2}(G,C)$$

□

2.15 Another proof of Tate's Theorem

Using the alternative approach to Tate cohomology, we can obtain another description of the isomorphism in Tate's Theorem using cup products which would be very useful for Local Class Field Theory.

Theorem 46. *Let A be a G-module with the following properties. For each subgroup H of G, we have*

1. $H^{-1}(H, A) = 0$,
2. $H^0(H, A)$ *is a cyclic group of order* $|H|$.

If a generates the group $H^0(G, A)$, then the cup product map

$$a \cup : H^q(G, \mathbb{Z}) \to H^q(G, A)$$

given by

$$x \mapsto a \cup x$$

is an isomorphism for all $q \in \mathbb{Z}$.

Proof. Define

$$B = A \oplus \mathbb{Z}[G]$$

Consider the short exact sequence

$$0 \to A \xrightarrow{i} B \xrightarrow{\pi} \mathbb{Z}[G] \to 0$$

Since $\mathbb{Z}[G]$ is cohomologically trivial, so the map

$$\bar{i} : H^q(H, A) \to H^q(H, B)$$

is an isomorphism. Choose $a_0 \in A^G$ such that $a_0 + N_G A = a$. Define the map $f : \mathbb{Z} \to B$ such that

$$f(n) = na_0 + nN_G$$

Note that f is injective since $nN_G = 0$ clearly implies that $n = 0$.

f induces the homomorphism

$$\bar{f} : H^q(H, \mathbb{Z}) \to H^q(H, B)$$

We want to show that the following diagram is commutative :

$$\begin{array}{ccc} H^q(G, \mathbb{Z}) & \xrightarrow{a \cup} & H^q(G, A) \\ & \searrow^{\bar{f}} & \downarrow \bar{i} \\ & & H^q(G, B) \end{array} \tag{2.53}$$

By Theorem 40, we know that cup with a is same thing as tensoring with a. But the tensor product of a_0 with an element n of $\mathbb{Z}$ is the same thing as na_0 (i.e. via action of $n \in \mathbb{Z}$ on $a_0 \in A$). Thus the only thing left is to show that nN_G is a coboundary and thus 0 in $H^q(G, B)$. But nN_G is a q-cocycle in $C^q(G, \mathbb{Z}[G])$ and is thus a $(q-1)$-coboundary in $C^q(G, \mathbb{Z}[G])$ since $\mathbb{Z}[G]$ is cohomologically trivial and thus nN_G is a $(q-1)$-coboundary in $C^q(G, B)$.

Hence, to prove Theorem 46, it suffices to show that $\bar{f}$ is bijective.

Since the map $f : \mathbb{Z} \to B$ is injective, so there is an exact sequence of G-modules

$$0 \to \mathbb{Z} \xrightarrow{f} B \to C \to 0$$

for some G-module C. Now by the hypothesis,

$$H^{-1}(H, A) = 0$$

which immediately implies that

$$H^{-1}(H, B) = 0$$

since the map $\bar{i}$ is an isomorphism. Moreover by Lemma 30, we know that

$$H^1(H, \mathbb{Z}) = 0$$

Therefore the very long exact sequence of Tate Cohomology groups (Theorem 32) shows that the following sequence is exact :

$$0 \to H^{-1}(H, C) \to H^0(H, \mathbb{Z}) \xrightarrow{\bar{f}} H^0(H, B) \to H^0(H, C) \to 0 \tag{2.54}$$

If $q = 0$, then we will show that $\bar{f}$ is injective. We have $\bar{f} : \mathbb{Z}/|H|\mathbb{Z} \to B^H/N_H B$ given by

$$\bar{f}(n) = na_0 + nN_G$$

$\bar{f}(n) = 0$ means that $na_0 = N_H a_1$ for some $a_1 \in A$. This shows that $res(na) = nres(a) = 0$ in $H^0(H, A)$. Since $res(a)$ is a generator for $H^0(H, A)$ (as shown in the proof of Theorem 45) and $|H^0(H, A)| = |H|$, so n is a multiple of $|H|$. Thus $\bar{f}$ is injective.

Moreover, by Lemma 30 and the hypothesis of this theorem, we have

$$H^0(H, \mathbb{Z}) = |H| = H^0(H, B)$$

Therefore, $\bar{f}$ is bijective and

$$H^{-1}(H, C) = H^0(H, C) = 0$$

By Theorem 44, we get

$$H^q(H, C) = 0$$

for all $q \in \mathbb{Z}$. The very long exact sequence for Tate Cohomology (Theorem 32) gives us the exact sequence

$$H^{q-1}(G, C) \to H^q(G.\mathbb{Z}) \xrightarrow{\bar{f}} H^q(G, B) \to H^q(G, C)$$

But since $H^q(G, C) = 0$ for all $q \in \mathbb{Z}$, so we have the exact sequence

$$0 \to H^q(G, \mathbb{Z}) \xrightarrow{\bar{f}} H^q(G, B) \to 0$$

which shows that $\bar{f}$ is bijective and we are done. □

Theorem 47. *(Tate's Theorem) Assume that A is a G-module with the following properties :*

For each subgroup H of G, we have

1. $H^1(H, A) = 0$,
2. $H^2(H, A)$ *is a cyclic group of order* $|H|$.

If a generates the group $H^2(G, A)$, then the cup product map

$$a \cup : H^q(G, \mathbb{Z}) \to H^{q+2}(G, A)$$

given by

$$x \mapsto a \cup x$$

is an isomorphism for all $q \in \mathbb{Z}$.

Proof. For all $q \in \mathbb{Z}$ and for each subgroup H of G, there is an isomorphism

$$\delta^2 : H^q(H, A^2) \to H^{q+2}(H, A)$$

as used in the section on dimension shifting. For any subgroup H of G, Condition 1 shows that $H^{-1}(H, A^2) = 0$ and Condition 2 shows that $H^0(H, A^2)$ is a cyclic group of order $|H|$. Thus the hypothesis of Theorem 46 is satisfied. Moreover (by taking $H = G$ and $q = -2$), we have an isomorphism

$$\delta^2 : H^{-2}(G, A^2) \to H^0(G, A)$$

This shows that $\delta^{-2}(a)$ is a generator of $H^0(G, A^2)$. Therefore by Theorem 46, the map

$$H^q(G, \mathbb{Z}) \xrightarrow{\delta^{-2}a\,\cup} H^{q+2}(G, A^2)$$

is an isomorphism. Moreover, we will show that the following diagram commutes :

$$\begin{array}{ccc} H^q(G, \mathbb{Z}) & \xrightarrow{\delta^{-2}a\,\cup} & H^q(G, A^2) \\ \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \delta^2} \\ H^q(G, \mathbb{Z}) & \xrightarrow{a\,\cup} & H^{q+2}(G, A) \end{array} \tag{2.55}$$

To see this, take any $x \in H^q(G, \mathbb{Z})$. Then we have

$$\delta^2(\delta^{-2}a \cup x) = \delta^2(\delta^{-2}(a)) \cup x = a \cup x$$

and so we are done. Since the map $\delta^{-2}a \cup$ is an isomorphism, so the map $a \cup$ is also an isomorphism. □

2.16 Galois Cohomology

2.16.1 Profinite groups

In this subsection, we state the important properties of profinite groups. For detailed proofs, please refer to Section 2.1, [6].

Definition 13. *A topological group G is group endowed with a topology with respect to which both the multiplication map $G \times G \to G$ and the inversion map $G \to G$ that takes an element to its inverse are continuous.*

Definition 14. *A homomorphism $\phi : G \to G'$ between topological groups G and G' is a topological isomorphism if it is both an isomorphism and a homeomorphism.*

Lemma 32. *Let G be a topological group and $g \in G$. Then the map $m_g : G \to G$ with $m_g(a) = ga$ for all $a \in A$ is a topological isomorphism.*

Lemma 33. *Let G be a topological group. Then any open subgroup of G is closed and any closed subgroup of finite index in G is open.*

Lemma 34. *Every open subgroup of a compact group G is of finite index in G.*

Recall the definitions of a directed set, inverse system, and the inverse limit.

Definition 15. *A directed set $I = (I, \geq)$ is a partially ordered set such that for every $i, j \in I$, there exists $k \in I$ such that $k \geq i$ and $k \geq j$.*

Definition 16. *Let I be a directed set. An inverse system $(G_i, \phi_{i,j})$ of groups over the indexing set I is a set*

$$\{G_i : i \in I\}$$

of groups and a set

$$\{\phi_{i,j} : G_i \to G_j : i, j \in I, i \geq j\}$$

of group homomorphisms such that for any $i \geq j \geq k$, we have

$$\phi_{i,k} = \phi_{j,k} \circ \phi_{i,j}$$

and $\phi_{i,i} = id$.

Definition 17. *Let $(G_i, \phi_{i,j})$ be an inverse system of groups over an indexing set I. Then the inverse limit of the system is given as the group*

$$G = \left\{ (g_i)_i \in \prod_{i \in I} G_i : \phi_{i,j}(g_i) = g_j \right\}$$

and the maps $\pi_i : G \to G_i$ for $i \in I$ are the compositions of $G \to \prod_{i \in I} G_i \to G_i$ of inclusion followed by projection. Moreover, for any $i \geq j$, we have

$$\pi_j = \pi_{i,j} \circ \pi_i$$

We may endow an inverse limit of groups with a topology as follows :

Definition 18. *Let $(G_i, \phi_{i,j})$ be an inverse system of groups over an indexing set I. Then the inverse limit topology on the inverse limit G is the subspace topology for the product topology on $\prod_{i \in I} G_i$.*

Definition 19. *A profinite group is an inverse limit of a system of finite groups, endowed with the inverse limit topology for the discrete topology on the finite groups.*

Theorem 48. *A profinite topological group is compact, Hausdorff and totally disconnected*

Theorem 49. *A compact Hausdorff and totally disconnected topological group has a basis of neighborhoods consisting of open normal subgroups.*

Corollary 7. *A profinite topological group has a basis of neighborhoods consisting of open normal subgroups.*

Theorem 50. *Let G be a profinite group, and let U be the set of all open normal subgroups of G. Then the canonical homomorphism*

$$G \to \varprojlim_{N \in U} G/N$$

is also a homeomorphism.

Definition 20. *A subset S of a topological group G is said to be a topological generating set of G if G is the closure of the subgroup generated by S.*

Definition 21. *We say that a topological group is (topologically) finitely generated if it has a finite set of topological generators.*

2.16.2 Cohomology of Profinite Groups

In this section, G will denote a topological group.

Definition 22. *A topological G-module A is an abelian topological group such that the map $G \times A \to A$ defining the G-action on A is continuous.*

Definition 23. *A G-module A is a discrete module if it is a topological G-module for the discrete topology on A.*

For the proofs of Theorem 51, Lemma 35 and Theorem 52, please refer to Section 2.2, [6].

Theorem 51. *Let G be a profinite group, and let A be a G-module. The following are equivalent :*

1. *A is discrete.*
2. *$A = \cup_{N \in U}$, where U is the set of open normal subgroups of G.*
3. *The stabilizer of each $a \in A$ is open in G.*

Definition 24. *For a topological G-module A and $i \in \mathbb{Z}$, the group of continuous i-cochains of G with A-coefficients is*

$$C^i_{cts}(G, A) = \{f : G^i \to A, \quad f \text{ is continuous}\}.$$

Lemma 35. *Let A be a topological G-module. The usual differential d^i on $C^i(G, A)$ restricts to a map*

$$d^i_{cts} : C^i_{cts}(G, A) \to C^{i+1}_{cts}(G, A)$$

Thus, $(C^{\bullet}_{cts}(G, A), d_{cts})$ is a cochain complex.

Definition 25. *Let G be a profinite group and A a discrete G-module. The i^{th} profinite cohomology group of G with coefficients in A is*

$$H^i(G, A) = H^i(C^{\bullet}_{cts}(G, A))$$

where A is endowed with the discrete topology.

Theorem 52. *Suppose that*

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

is a short exact sequence of discrete G-modules. Then there is a long exact sequence of abelian groups

$$0 \to H^0(G,A) \xrightarrow{i'} H^0(G,B) \xrightarrow{\pi'} H^0(G,C) \xrightarrow{\delta^0} H^1(G,A) \to ...$$

Theorem 53. *Let G be a profinite group, and let U be the set of open normal subgroups of G. For each discrete G-module A, we have an isomorphism*

$$C^r(G,A) \cong \varinjlim_{N \in U} C^r(G/N, A^N)$$

Proof. Let $N_1, N_2 \in U$, we define $N_1 \leq N_2$ by $N_2 \subset N_1$.

For $N_1, N_2 \in U$, we have $N_1 \cap N_2 \in U$. Also we have $N_1 \leq N_1 \cap N_2$ and $N_2 \leq N_1 \cap N_2$. Thus $(U, \leq)$ is a directed set. Let

$$G_N = C^r(G/N, A^N)$$

and for $N_1 \leq N_2$ (i.e. $N_2 \subset N_1$), we have the natural map

$$\alpha_{N_2 N_1} : G_{N_1} \to G_{N_2}$$

Also we have the natural maps

$$\alpha_N : G_N \to S$$

We define

$$S = \varinjlim_{N \in U} G_N$$

and

$$T = C^r_{cts}(G,A)$$

Also we have the inflation maps

$$\beta_N : C^r(G/N, A^N) \to C^r_{cts}(G,A)$$

It is straightforward to check that for $N_1 \leq N_2$, $\beta_{N_1} = \beta_{N_2} \circ \alpha_{N_2 N_1}$.

Hence by the universal property of the direct limit, there exists a unique map $\beta : S \to T$ such that $\beta_N = \beta \circ \alpha_N$.

Firstly we will show that β is surjective.

Let $f : G^i \to A$ be a continuous map. Since G is compact, so is $f(G)$. But we are given that A has the discrete topology. Since compact subset of a discrete space is finite, we get $Im(f)$ is finite. Also we know that since A is a discrete module, so

$$A = \bigcup_{N \in U} A^N$$

Hence for any $a \in Im(f)$, $\exists\ M_a \in U$ such that $a \in A^{M_a}$.

Therefore,

$$Im(f) \subset A^M$$

where

$$M = \bigcap_{a \in Im(f)} M_a$$

Note that M is open since $Im(f)$ is finite. Also M is normal in G. Hence $M \in U$.

For any $x \in G^i$, continuity of f implies that $V = f^{-1}\{f(x)\}$ is open in G^i and f is constant on V (Infact $f(V) = \{f(x)\}$). Let $V_1 = x^{-1}V$. Then V_1 is an open subset of G^i because multiplication by a fixed element is a homeomorphism for topological groups. Hence V_1 is an open neighborhood of 1.

Since G^i has the product topology, V_1 is a product of sets open in G and containing 1 (i.e. neighborhoods of 1_G). Also since the open normal subgroups form a neighborhood base for 1, so V_1 contains a neighborhood of the form $\prod_{j=1}^{i} H_j(x)$ where $H_j(x)$ is an open normal subgroup of G. Define

$$H(x) = \bigcap_{j=1}^{i} H_j(x)$$

$H(x)$ is again an open normal subgroup of G. Since

$$xH(x)^i \subset x\left(\prod_{j=1}^{i} H_j(x)\right) \subset xV_1 = V$$

so f is constant on $xH(x)^i$.

Now G^i is covered by the $xH(x)^i$ for $x \in G^i$ since $H(x)$ contains 1_G. Since G is a profinite group, thus G is compact and hence so is G^i. Thus there is a finite subcover of $xH(x)^i$ corresponding to some $x_1, .., x_n \in G^i$.

Now define

$$H = \bigcap_{k=1}^{n} H(x_k)$$

For any $y \in G^i$, we have $y \in x_k H(x_k)^i$ for some k. Since $H \subset H(x_k)$ and $H(x_k)$ is a subgroup of G, thus $yH \subset x_k H(x_k)^i$ and f is constant on yH since it is constant on $x_k H(x_k)^i$. Hence f factors through $(G/H)^i$.

We have shown that f is the inflation of a map $(G/H)^i \to A^M$ (Since we had earlier shown that Im(f) $\subset A^M$). Now if we take $N = H \cap M$, then $N \subset H$ and $A^M \subset A^N$. Hence f factors through a map $(G/N)^i \to A^N$ and we are done.

Now we will prove that β is injective. Let Φ be an element of S such that $\beta(\Phi) = 0$. We know that

$$\Phi = \alpha_N(\phi_N)$$

for some $N \in U$. Thus $\beta(\alpha_N(\phi_N)) = 0$ for some $N \in U$ and so

$$\beta_N(\phi_N) = 0$$

since $\beta \circ \alpha_N = \beta_N$ by the universal property of direct limit.

It is straightforward to check that the inflation maps β_N are injective (though the inflation maps at the level of cohomology need not be injective but they are injective at the cochain level).

Hence $\phi_N = 0$ and so $\Phi = \alpha(\phi_N) = 0$. Thus β is injective as well and so β is an isomorphism. $\square$

Theorem 54. *Let G be a profinite group, and let U be the set of open normal subgroups of G. For each discrete G-module A, we have an isomorphism*

$$H^r(G, A) \cong \varinjlim_{N \in U} H^r(G/N, A^N)$$

where the direct limit is taken with respect to inflation maps.

Proof. We know that the following diagram commutes :

$$\begin{array}{ccc} C^r(G/N, A^N) & \xrightarrow{d^r_N} & C^{r+1}(G/N, A^N) \\ \Big\downarrow \alpha^r_{N,N'} & & \Big\downarrow \alpha^{r+1}_{N,N'} \\ C^r(G/N', A^{N'}) & \xrightarrow{d^r_{N'}} & C^{r+1}(G/N', A^{N'}) \end{array} \tag{2.56}$$

This shows that

$$\alpha_{N,N'}(Ker(d^r_N)) \subset Ker(d'^r_N)$$

and

$$\alpha_{N,N'}(Im(d^r_N)) \subset Im(d'^r_N)$$

Therefore $Ker(d^r_N)$ and $Im(d^r_N)$ form direct systems.

Moreover, $\alpha_{N,N'}$ induces the map

$$\alpha_{N,N'} : \frac{Ker(d^r_N)}{Im(d^r_N)} \to \frac{Ker(d^r_{N'})}{Im(d^r_{N'})}$$

i.e. the map

$$\alpha_{N,N'} : H^r(G/N, A^N) \to H^r(G/N', A^{N'})$$

Thus $H^r(G/N, A^N)$ also forms a direct system. Now we have an exact sequence

$$0 \to Im(d^{r-1}_N) \to Ker(d^r_N) \to H^r(G/N, A^N) \to 0$$

Since direct limit preserves exactness, so

$$0 \to \varinjlim_{N \in U} Im(d^{r-1}_N) \to \varinjlim_{N \in U} Ker(d^r_N) \to \varinjlim_{N \in U} H^r(G/N, A^N) \to 0$$

is also exact and we have

$$\varinjlim_{N \in U} H^r(G/N, A^N) = \frac{\varinjlim_{N \in U} Ker(d^r_N)}{\varinjlim_{N \in U} Im(d^{r-1}_N)}$$

Since diagram 2.56 commutes, so there exists a map

$$\varinjlim_{N \in U} d^r_N : \varinjlim_{N \in U} C^r(G/N, A^N) \to \varinjlim_{N \in U} C^{r+1}(G/N, A^N)$$

such that the following diagram commutes :

$$\begin{array}{ccc} C^r(G/N, A^N) & \xrightarrow{d_N^r} & C^{r+1}(G/N, A^N) \\ \downarrow{\alpha_N^r} & & \downarrow{\alpha_N^{r+1}} \\ \varinjlim_{N\in U} C^r(G/N, A^N) & \xrightarrow{\varinjlim_{N\in U} d_N^r} & \varinjlim_{N\in U} C^{r+1}(G/N, A^N) \end{array} \tag{2.57}$$

Moreover by the previous theorem, we have

$$C^r(G, A) \cong \varinjlim_{N\in U} C^r(G/N, A^N)$$

This shows that

$$H^r(G, A) \cong \frac{Ker(\varinjlim_{N\in U} d^r)}{Im(\varinjlim_{N\in U} d^{r-1})}$$

Thus to complete the proof of the theorem, it suffices to show that

$$\frac{Ker(\varinjlim_{H\in U} d_H^r)}{Im(\varinjlim_{H\in U} d_H^{r-1})} = \frac{\varinjlim_{H\in U} Ker(d_H^r)}{\varinjlim_{H\in U} Im(d_H^{r-1})}$$

We have an exact sequence

$$0 \to Ker(d_H^R) \to C^r(G/H, M^H) \xrightarrow{d_H^r} C^{r+1}(G/H, M^H)$$

Since direct limit preserves exactness,

$$0 \to \varinjlim_{H\in U} Ker(d_H^r) \to \varinjlim_{H\in U} C^r(G/H, M^H) \xrightarrow{\varinjlim_{H\in U} d_H^r} \varinjlim_{H\in U} C^{r+1}(G/H, M^H)$$

is exact and thus

$$Ker(\varinjlim_{H\in U} d_H^r) = \varinjlim_{H\in U} Ker(d_H^r)$$

Similarly we have an exact sequence

$$C^r(G/H, M^H) \xrightarrow{d_H^r} C^{r+1}(G/H, M^H) \xrightarrow{\pi_H} Coker(d_H^r) \to 0$$

Again passing to the direct limits, we get an exact sequence

$$\varinjlim_{H\in U} C^r(G/H, M^H) \xrightarrow{\varinjlim_{H\in U} d_H^r} \varinjlim_{H\in U} C^{r+1}(G/H, M^H) \xrightarrow{\varinjlim_{H\in U} \pi_H} \varinjlim_{H\in U} Coker(d_H^r) \to 0$$

Thus we get

$$Im(\varinjlim_{H\in U} d_H^r) = Ker(\varinjlim_{H\in U} \pi_H) = \varinjlim_{H\in U} Ker(\pi_H) = \varinjlim_{H\in U} Im(d_H^r)$$

Note that the second equality follows from the fact that kernels commute with direct limits which we had already shown above.

Hence

$$\frac{Ker(\varinjlim_{H\in U} d_H^r)}{Im(\varinjlim_{H\in U} d_H^{r-1})} = \frac{\varinjlim_{H\in U} Ker(d_H^r)}{\varinjlim_{H\in U} Im(d_H^{r-1})}$$

This completes the proof that $H^r(G, A) \cong \varinjlim_{N\in U} H^r(G/N, A^N)$ □

Chapter 3

Local Class Field Theory

3.1 Recap of Local Fields

Throughout this chapter, we would use several properties of local fields which we state here. Easy and detailed proofs of these results can be found in Ch. 4 and Ch. 7 of [9]. Ch.7 of [3] is also a good reference.

Definition 26. *A local field K is a field which is locally compact with respect to a nontrivial valuation.*

Lemma 36. *Let $K, ||$ be a non-archimedean local field. Then the following are equivalent :*
1. K is a local field.
2. O_K is compact.
3. K is complete, w.r.t $||$ which is discrete and the residue field $k = O_K/m_K$ is finite.

Lemma 37. *Let K be a non-archimedean local field, then O_K is compact and the residue field $k = O_K/m_K$ is finite and since $||$ is discrete, so m_K is a principal ideal.*

Theorem 55. *If K is a non-archimedean local field such that $char(K) = 0$, then K is a finite extension of Q_p.*

Theorem 56. *Suppose $K, ||$ is a complete non-archimedean field and L is a finite extension of K such that $[L : K] = n$. Then there is a unique absolute value $||_L$ on L extending $||$ on K, and L is complete non-archimedian with respect to this valuation. Explicitly $|x|_L = |Nm_{L/K}(x)|^{1/n}$. Also $||$ is discrete $\Leftrightarrow ||_L$ is discrete. This (along with Lemma 36) shows that if K is a discrete non-archimedian local field, then so is L.*

Theorem 57. *Finite,unramified extensions of a local field K are in one to one correspondence with finite extensions of the residue field k.*

Lemma 38. *Suppose L/K is a finite, unramified extension. Then L/K is Galois if and only if l/k is Galois, and in this case $Gal(L/K) \cong Gal(l/k)$.*

Theorem 57 implies that any local field K has a unique unramifed extension of degree n which is $L_n = K(\mu_{p^n-1})$ and this shows that there is a maximal unramified extension K^{un} obtained by adjoining (to K) n^{th} roots of unity for all n coprime to the characteristic of the residue field k.

3.2 Properties of Frobenius Element

3.2.1 Finite Extensions

For a local field K, we denote the cardinality of its residue field by q_K. For an extension L/K, we denote the Frobenius element by $\sigma_{L/K}$.

Let $E \supset L \supset K$ be a tower of finite unramified extensions of local fields. Then we have the following properties :

Lemma 39. $\sigma_{L/K} = \sigma_{E/K} \restriction_L = \sigma_{E/K} Gal(E/L) \in Gal(L/K)$

Proof. We know that $\sigma_{L/K}$ is the unique element of $Gal(L/K)$ such that $\sigma_{L/K}(x) \equiv x^{q_K} \pmod{m_L}$ $\forall\ x \in O_L$. Now note that $\sigma_{E/K} \restriction_L \in Gal(L/K)$ and we have $\sigma_{E/K}(x) \equiv x^{q_K} (\text{mod } m_E)$ $\forall\ x \in O_E$ and hence also $\forall\ x \in O_L$. Now for any $x \in O_L$, we have $\sigma_{E/K}(x) \in L$ (since L is galois over K). Thus $\frac{\sigma_{E/K}(x)}{x^{q_K}} \in L \cap m_E = m_L$ i.e. $\sigma_{E/K}(x) \equiv x^{q_K} \pmod{m_L}$. By the uniqueness for $\sigma_{L/K}$, we get $\sigma_{L/K} = \sigma_{E/K} \restriction_L$.

Since we have the isomorphism

$$\frac{Gal(E/K)}{Gal(E/L)} \cong Gal(L/K)$$

which is given by

$$\tau Gal(E/L) \mapsto \tau \restriction_L$$

for any $\tau \in Gal(E/K)$. So

$$\sigma_{E/K} Gal(E/L) \mapsto \sigma_{E/K} \restriction_L = \sigma_{L/K}$$

and thus we can say $\sigma_{E/K} \restriction_L = \sigma_{E/K} Gal(E/L) \in Gal(L/K)$. □

Lemma 40. $\sigma_{E/L} = \sigma_{E/K}^{[L:K]}$

Proof. We know that $\left|\frac{Gal(E/K)}{Gal(E/L)}\right| = [L : K]$, so $(\sigma_{E/K} Gal(E/L))^{[L:K]}$ is identity in $\frac{Gal(E/K)}{Gal(E/L)}$ i.e. $\sigma_{E/K}^{[L:K]} \in Gal(E/L)$. Now for any $x \in O_E$, we have $\sigma_{E/K}(x) \equiv x^{q_K} (\text{mod } m_E)$ and thus $\sigma_{E/K}^{[L:K]}(x) \equiv x^{q_L} (\text{mod } m_E)$ since $q_L = q_K^{[L:K]}$. By the uniqueness for $\sigma_{E/L}$, we get $\sigma_{E/L} = \sigma_{E/K}^{[L:K]}$. □

3.2.2 Infinite Extensions

Let L be a galois extension of K and let K_1, K_2 be finite galois subextensions of L over K. Then K_1K_2 is again a finite galois extension of K. Thus the finite galois subextensions of L over K form a directed set. For $K_1 \subset K_2$, define

$$\beta_{K_1,K_2} : Gal(K_2/K) \to Gal(K_1/K)$$

to be the restriction maps. Thus we get an inverse system $(Gal(K'/K), \beta_{K',K''})$. Let

$$\beta_{K_1} : \varprojlim_{K'} Gal(K'/K) \to Gal(K_1, K)$$

be the projection map. Then for any $K_1 \subset K_2$, we have $\beta_{K_1,K_2} \circ \beta_{K_2} = \beta_{K_1}$. Now let $\gamma_{K'} : Gal(L/K) \to Gal(K'/K)$ be the restriction map. Then for any $K_1 \subset K_2$,

$$\beta_{K_1,K_2} \circ \gamma_{K_2} = \gamma_{K_1}$$

Thus by the universal property of inverse limits, we get a map

$$\beta : Gal(L/K) \to \varprojlim_{K'} Gal(K'/K)$$

such that

$$\beta_{K'} \circ \beta = \gamma_{K'}$$

By infinite galois theory, it can be shown that the map β is infact an isomorphism of topological groups.

Thus for an infinite galois extension L/K, we have

$$Gal(L/K) \cong \varprojlim_{K'} Gal(K'/K)$$

where $K^{'}$ runs over finite galois extensions of K in L. Note that

$$\sigma_0 = (\sigma_{K'/K})_{K'}$$

is a well-defined element in the inverse limit because if $K_1 \subset K_2$, then

$$\beta_{K_1,K_2}(\sigma_{K_2/K}) = \sigma_{K_2/K} \restriction_{K_1} = \sigma_{K_1/K}$$

Now we can define the Frobenius element $\sigma_{L/K} \in Gal(L/K)$ to be the unique preimage of σ_0 under this isomorphism β.

Let $E \supset L \supset K$ be a tower of unramified (possibly infinite) extensions.

Lemma 41. $\sigma_{L/K} = \sigma_{E/K} \restriction_L = \sigma_{E/K} Gal(E/L) \in Gal(L/K)$

Proof. Let $x \in L$. Thus $x \in K^{'}$ for some finite subextension of L over K. Since

$$\beta_{K'} \circ \beta = \gamma_{K'}$$

so

$$\beta_{K'}(\beta(\sigma_{L/K})) = \gamma_{K'}(\sigma_{L/K})$$

which implies that

$$\beta_{K'}(\sigma_0) = \sigma_{L/K} \restriction_{K'}$$

i.e.

$$\sigma_{L/K} \restriction_{K'} = \sigma_{K'/K}$$

Hence

$$\sigma_{L/K}(x) = \sigma_{K'/K}(x)$$

Since $L \subset E$, so $x \in L$. Then by repeating the whole argument, we have

$$\sigma_{E/K}(x) = \sigma_{K'/K}(x)$$

Thus we have shown that for any $x \in L$,

$$\sigma_{L/K}(x) = \sigma_{E/K}(x)$$

Hence

$$\sigma_{L/K} = \sigma_{E/K} \restriction_L$$

Finally

$$\sigma_{E/K} \restriction_L = \sigma_{E/K} Gal(E/L)$$

follows in exactly the same way as in the proof of Lemma 39. □

Theorem 58. *The subgroup generated by $\sigma_{L/K}$ in $Gal(L/K)$ is dense.*

Proof. We will use a result from infinite galois theory :

Let L be galois over K with Galois group G. Then for any subgroup H of G, $Gal(L/L^H)$ is the closure of H. (see Proposition 7.11, page 94, [5] for proof)

In our case $H = <\sigma_{L/K}>$.

Thus it suffices to show that $L^H = K$. Let $x \in L$ such that $\sigma_{L/K}(x) = x$. Again, let $x \in K'$ for some finite subextension of L in K. Then

$$\sigma_{K'/K}(x) = \sigma_{L/K}(x) = x$$

Thus x is in the fixed field of $Gal(K'/K)$ which is K and we are done. □

Lemma 42. *Let L be a finite extension of K of degree n. Let σ_K denote the Frobenius element of the extension K^{un}/K and σ_L denote the Frobenius element of the extension L^{un}/L. Then $\sigma_L \restriction_{K^{un}} = \sigma_K^f$*

Proof. We know that $\sigma_L(x) \equiv x^{q_L} \pmod{m_{L^{un}}}$ for all $x \in O_{L^{un}}$ and $\sigma_K(x) \equiv x^{q_K} \pmod{m_{K^{un}}}$ for all $x \in O_{K^{un}}$. Therefore $\sigma_L(x) \equiv \sigma_K^f(x) \pmod{m_{L^{un}}}$ for all $x \in O_{K^{un}}$ which shows that $\sigma_L \restriction_{K^{un}} = \sigma_K^f$ □

3.3 The Cohomology of Unramified Extensions

Let K be a discrete non-archimedean local field and let L be a finite extension of K. Then we know that there is a unique extension of valuation of K to valuation of L. Also under this valuation, L is a discrete non-archimedean local field by Theorem 56. Since L and K are local fields, so the residue fields $l = O_L/m_L$ and $k = O_K/m_K$ are finite. Let $|k| = p$ and $|l| = q$ where q is some power of p. All cohomology groups will be Tate cohomology groups and the subscript T will be dropped.

Since l/k is a finite extension of a finite field, L/K is Galois and $Gal(L/K)$ is a cyclic group generated by the Frobenius element $Frob_{L/K}$ which is characterized uniquely by

$$\sigma(\alpha) \equiv \alpha^p \ \ (mod\, m_L)$$

For a Galois extension L/K of fields, we set

$$H^2(L/K) = H^2(Gal(L/K), L^*)$$

Theorem 59. *Let L/K be a finite unramified extension with Galois group G, and let U_L be the group of units in L. Then $H^r(G, U_L) = 0 \; \forall \; r$.*

Proof. Since L is a non-archimedian field, O_L is a local ring with unique maximal ideal m_L. Similarly O_K is a local ring with unique maximal ideal m_K. Since L and K are discrete, so m_L and m_K are principal ideals. Thus m_K is an ideal generated by some prime $\pi \in O_K$. Then since L/K is an unramified extension, π remains prime in O_L and hence is also a generator for m_L. Thus every element α of L^* can be written uniquely in the form $\alpha = u\pi^m$ for some $u \in U_L$ and $m \in \mathbb{Z}$

Define $f : L^* \to U_L \times Z$ such that

$$f(u\pi^m) = (u, m)$$

f is well defined because of uniqueness of the expression $u\pi^m$. f is clearly one-one and onto. Moreover,

$$f((u_1\pi^{m_1})(u_2\pi^{m_2})) = f(u_1u_2\pi^{m_1+m_2}) = (u_1u_2, m_1 + m_2) = (u_1, m_1) * (u_2, m_2)$$

Thus f is a homomorphism of abelian groups.

Now for any $\tau \in G$, we have

$$f(\tau(u\pi^m)) = f(\tau(u)\pi^m) = (\tau(u), m) = (\tau(u), \tau(m)) = \tau(u, m) = \tau(f(u\pi^m))$$

The first equality follows from the fact that $\pi \in K$ and is hence fixed by any $\tau \in Gal(L/K)$. The third equality follows from the fact that G acts trivially on $\mathbb{Z}$.

Hence f is a G-module homomorphism and thus a G-module isomorphism. Therefore by Theorem 22, for any $r \geq 0$,

$$H^r(G, L^*) \cong H^r(G, U_L) \oplus H^r(G, \mathbb{Z})$$

By Hilbert's Theorem 90 (Theorem 20), we know that $H^1(G, L^*) = 0$ and thus $H^1(G, U_L) = 0$.

Because G is cyclic, we know that cohomology groups are periodic with periodicity 2 by Theorem 41. Hence to prove our theorem, it suffices to show that $H^0(G, U_L) = 0$ which will follow from the next few lemmas.

Lemma 43. *For $m > 0$, let $U_L^m = 1 + m_L^m$. Then $U_L/U_L^{(1)} \cong l^*$ and $U_L^{(m)}/U_L^{(m+1)} \cong l$ as G-modules.*

Proof. Note that $U_L^{(m)} = \{1 + a\pi^m : a \in O_L\}$.

Define the map $\phi_L : U_L \to l^*$ such that $\phi(u) = u + m_L$.

Since $U_L = O_L - m_L$, we know ϕ_L is well-defined. Now ϕ_L is also surjective because for any $x \in O_L$ such that $\bar{x} \neq \bar{0}$ (i.e. $x \notin m_L$), we have $x \in U_L$ again because of $U_L = O_L - m_L$ and thus $x + m_L = \phi_L(x)$.

ϕ_L is also a G-module map since

$$\phi_L(\tau(u)) = \tau(u) + m_L = \tau(u + m_L) = \tau(\phi_L(u))$$

Moreover,

$$Ker(\phi_L) = \{u \in U_L : \bar{u} = \bar{1}\} = 1 + m_L = U_L^{(1)}$$

Hence we get an isomorphism $\Phi_L : U_L/U_L^{(1)} \to l^*$ of G-modules.

Similarly define the maps $\psi_L : U_L^{(m)} \to l$ such that $\psi(1 + a\pi^m) = a + m_L$.

ψ_L is well defined because if $1 + a\pi^m = 1 + b\pi^m$ for some $a, b \in O_L$, then $(a - b)\pi^m = 0$ and thus $a = b$ (since π is invertible in K though not in O_K) and so $a + m_L = b + m_L$ .Moreover,

$$\begin{aligned} \psi_L((1 + a\pi^m)(1 + b\pi^m)) &= \psi_L(1 + (a + b)\pi^m + ab\pi^{2m}) = \psi_L(1 + (a + b + \pi^m ab)\pi^m) \\ &= a + b + \pi^m ab + m_L = a + b + m_L = \psi_L(1 + a\pi^m) + \psi_L(1 + b\pi^m) \end{aligned} \tag{3.1}$$

Note that in the second last equality, we have used that $\pi \in m_L$.

Thus ψ_L is a group homomorphism. For any $\tau \in G$, we have

$$\psi_L(\tau(1 + a\pi^m)) = \psi_L(1 + \tau(a)\pi^m) = \tau(a) + m_L = \tau(a + m_L) = \tau(\psi_L(1 + a\pi^m))$$

Hence ψ_L is a G-module homomorphism. Now

$$Ker(\psi_L) = \{1 + a\pi^m : a \in m_L\} = \{1 + b\pi^{m+1} : b \in O_L\} = U_L^{(m+1)}$$

Thus we get an isomorphism $\Psi_L : U_L^{(m)}/U_L^{(m+1)} \to l$ of G-modules.

□

Lemma 44. *$H^r(G, l^*) = 0 \;\forall\; r \in \mathbb{Z}$. In particular the norm map $l^* \to k^*$ is surjective.*

Proof. By Hilbert's Theorem 90, $H^1(G, l^*) = 0$. We know that l^* is finite and so the Herbrand quotient $h(l^*) = 1$. Hence $H^0(G, l^*) = 0$ and so $H^r(G, l^*) = 0 \;\forall\; r \in \mathbb{Z}$ by the periodicity of the Tate cohomology for cyclic groups. In particular $H^0(G, l^*) = 0$ and thus $(l^*)^G = Nm_{l/k}(l^*)$.

Since l/k is galois, $(l^*)^G = k^*$ and so $Nm_{l/k}(l^*) = k^*$ which implies that the norm map $l^* \to k^*$ is surjective. □

Lemma 45. *$H^r(G, l) = 0 \;\forall\; r \in \mathbb{Z}$. In particular, the trace map $l \to k$ is surjective.*

Proof. We know that $H^r(G, l) = 0 \;\forall\; r > 0$ by Theorem 21. Hence $H^r(G, L) = 0 \;\forall\; r \in \mathbb{Z}$ by Theorem 41. In particular $H^0(G, l) = 0$ and so $l^G = \mathrm{Tr}(l)$.

Since l/k is galois, so $l^G = k$ and we get $\mathrm{Tr}(l) = k$ which implies that the trace map $l \to k$ is surjective. □

Theorem 60. *For every finite unramified extension L/K, the norm map $Nm_{L/K} : U_L \to U_K$ is surjective.*

Proof. For all $m > 0$, the following diagrams commute :

$$\begin{array}{ccc} U_L & \xrightarrow{\phi_L} & l^* \\ \downarrow{\scriptstyle Nm_{L/K}} & & \downarrow{\scriptstyle Nm_{l/k}} \\ U_K & \xrightarrow{\phi_K} & k^* \end{array} \qquad \begin{array}{ccc} U_L^{(m)} & \xrightarrow{\psi_L} & l \\ \downarrow{\scriptstyle Nm_{L/K}} & & \downarrow{\scriptstyle Tr_{l/k}} \\ U_K^{(m)} & \xrightarrow{\psi_K} & k \end{array} \tag{3.2}$$

Consider $u \in U_K$. Then $\phi_K(u) \in k^*$. Because the norm map $l^* \to k^*$ and ϕ_L are surjective, $\exists$ $v_0 \in U_L$ such that

$$Nm_{L/K}(\phi_L(v_0)) = \phi_K(u)$$

Since the diagram commutes, we get

$$\phi_K(Nm(v_0)) = \phi_K(u)$$

Since $Ker(\phi_K) = U_K^{(1)}$, we get

$$\frac{u}{Nm(v_0)} \in U_K^{(1)}$$

Similarly commutativity of the diagram and surjectivity of the trace map $l \to k$ imply that $\exists$ $v_1 \in U_L^{(1)}$ such that

$$Nm(v_1) \equiv \frac{u}{Nm(v_0)} \; mod \; U_K^{(2)}$$

Continuing in this fashion, we obtain a sequence of elements $v_0, v_1, ..., v_i \in U_L^{(i)}$ such that

$$\frac{u}{Nm(v_0...v_i)} \in U_K^{(i+1)}$$

Consider the sequence $\prod_{j=0}^{m} v_j$.

Now

$$\left|\prod_{j=0}^{m} v_j - \prod_{j=0}^{m+1} v_j\right| = \left|\prod_{j=0}^{m} v_j(1 - v_{m+1})\right| < |\pi|^{m+1}$$

since $|v_i| = 1 \; \forall \; i$ (as $v_i \in U_L$) and $|1 - v_{m+1}| < |\pi|^{m+1}$ (as $v_{m+1} \in U_L^{m+1} = 1 + m_L^{m+1}$).

Since L is non-archimedian, the above analysis shows that the sequence $\prod_{j=0}^{m} v_j$ is cauchy. Moreover L is a locally compact field, so it is complete and the sequence $\prod_{j=0}^{m} v_j$ converges.

Let $v = \lim_{m\to\infty} \prod_{j=0}^{m} v_j$. Since L is non-archimedean, we have

$$|v| \leq \max\left(\left|v - \prod_{j=0}^{m} v_j\right|, \left|\prod_{j=0}^{m} v_j\right|\right) = \max\left(\left|v - \prod_{j=0}^{m} v_j\right|, 1\right) \; \forall \; m \in \mathbb{N}$$

Also we know that for large enough m,

$$\left|v - \prod_{j=0}^{m} v_j\right| < 1$$

since $v = \lim_{m\to\infty} \prod_{j=0}^{m} v_j$. Thus $|v| \leq 1$ and so $v \in O_L$. Moreover,

$$\left|\prod_{j=0}^{m} v_j\right| \leq \max\left(\left|\prod_{j=0}^{m} v_j - v\right|, |v|\right) \; \forall \; m \in \mathbb{N}$$

This shows that $|v| \geq 1$ and hence $|v| = 1$ i.e. $v \in U_L$. We also have

$$\left|\frac{u}{Nm_{L/K}(v)} - 1\right| \leq \max\left(\left|\frac{u}{Nm_{L/K}(v)} - \frac{u}{Nm_{L/K}(v_0...v_i)}\right|, \left|\frac{u}{Nm_{L/K}(v_0...v_i)} - 1\right|\right) \; \forall \; i \in \mathbb{N}$$

It is easy to show that

$$\lim_{i\to\infty} \frac{u}{Nm_{L/K}(v_0...v_i)} = \frac{u}{Nm_{L/K}(v)}$$

and so

$$\lim_{i\to\infty} \left| \frac{u}{Nm_{L/K}(v)} - \frac{u}{Nm_{L/K}(v_0...v_i)} \right| = 0$$

Now we have

$$\frac{u}{Nm_{L/K}(v_0...v_i)} \in U_k^{i+1}$$

so

$$\frac{u}{Nm_{L/K}(v_0...v_i)} - 1 \in m_k^{i+1}$$

and thus

$$\left| \frac{u}{Nm_{L/K}(v_0...v_i)} - 1 \right| < |\pi|^{i+1}$$

Hence

$$\lim_{i\to\infty} \left| \frac{u}{Nm_{L/K}(v_0...v_i)} - 1 \right| = 0$$

Combining all these together, we get

$$\left| \frac{u}{Nm_{L/K}(v)} - 1 \right| = 0$$

and thus

$$u = Nm_{L/K}(v)$$

which implies that the norm map is surjective and we are done. □

□

Theorem 61. *Let L/K be an infinite unramified extension with Galois Group G. Then $H^r(G, U_L) = 0 \;\forall\; r > 0$.*

Proof. The field L is a union of finite extensions K' of K. Thus L is a discrete $Gal(L/K)$ module and by Theorem 54, we get

$$H^r(Gal(L/K), U_K) \cong \varinjlim_{K'} H^r(Gal(K'/K), U_K^{'})$$

Since L is unramified, any finite subextension $K^{'}$ of L is also unramified by definition of an infinite unramified extension. By the above result, we know that $H^r(Gal(K'/K), U_K^{'}) = 0 \;\forall\; K^{'}$. Thus $H^r(G, U_L) = 0$ for all $r \geq 0$. □

3.4 Invariant Map and Local Artin Map

3.4.1 Finite Extensions

Let L be a finite unramified extension of K with $[L : K] = n$, and let $G = Gal(L/K)$. Consider the short exact sequence

$$0 \to U_L \to L^* \xrightarrow{ord_L} \mathbb{Z} \to 0$$

where the ord_L map is given by

$$ord_L(u\pi^m) = m$$

Since U_L is cohomologically trivial, we get an isomorphism

$$H^2(G, L^*) \to H^2(G, \mathbb{Z})$$

An explicit description of this map as well as its inverse would be required later.

The map $\eta_1 : H^2(G, L^*) \to H^2(G, \mathbb{Z})$ is given as $\bar{\phi} \mapsto \bar{\psi}$ where

$$\psi(g_1, g_2) = ord_L(\phi(g_1, g_2))$$

The inverse map $\eta_2 : H^2(G, \mathbb{Z}) \to H^2(G, L^*)$ is given by $\bar{\Psi} \mapsto \bar{\Phi}$ where

$$\Phi(g_1, g_2) = \pi^{\Psi(g_1, g_2)}$$

We want to verify that the maps η_1 and η_2 are inverses of each other. It is clear that $\eta_1 \circ \eta_2$ is the identity map on $H^2(G, \mathbb{Z})$. The proof that $\eta_2 \circ \eta_1$ is the identity map on $H^2(G, L^*)$ is somewhat more intricate. $(\eta_2 \circ \eta_1)(\bar{\phi}) = \bar{\gamma}$ where

$$\gamma(g_1, g_2) = \pi^{ord_L(\phi(g_1, g_2))}$$

To show that $\bar{\phi} = \bar{\gamma}$, it suffices to show that $\psi := \phi/\gamma$ is $d^1(\kappa)$ for some 1-cochain κ. But note that $Im(\psi) \subset U_L$. It can be directly verified that ψ is a cocycle in $C^2(G, U_L)$. Since U_L is cohomologically trivial, ψ is infact a 1-coboundary in $C^1(G, U_L)$ and hence also in $C^1(G, L^*)$.

The short exact sequence

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

gives rise to the isomorphism

$$H^1(G, Q/Z) \to H^2(G, \mathbb{Z})$$

since $\mathbb{Q}$ is cohomologically trivial by Lemma 30. We also know that $H^1(G, \mathbb{Q}/\mathbb{Z}) = Hom_{cts}(G, \mathbb{Q}/\mathbb{Z})$. Let σ be the Frobenius element (which is a generator of G).

Now define a map

$$\psi : Hom_{cts}(G, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}$$

such that

$$\psi(f) = f(\sigma)$$

Note that ψ is an injection and Im$(\psi) = \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ because

$$n(\psi(f)) = n(f(\sigma)) = f(\sigma^n) = f(1) = 0 + \mathbb{Z}$$

and thus $\psi(f) \in \frac{1}{n}\mathbb{Z}/\mathbb{Z}$.

Definition 27. *The composite of the maps*

$$H^2(L/K) \xrightarrow{ord_L} H^2(G,\mathbb{Z}) \xrightarrow{\delta^{-1}} Hom_{cts}(G,\mathbb{Q}/\mathbb{Z}) \xrightarrow{f\mapsto f(\sigma)} \mathbb{Q}/\mathbb{Z} \tag{3.3}$$

is called the invariant map.

$$inv_{L/K} : H^2(L/K) \to \mathbb{Q}/\mathbb{Z} \tag{3.4}$$

Remark 14. *Infact $inv_{L/K}$ is an isomorphism from $H^2(L/K)$ onto $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$.*

Definition 28. *The local fundamental class is the element of $H^2(L,K)$ mapped to the generator $\frac{1}{n}+\mathbb{Z}$ under the invariant map $inv_{L/K}$.*

Remark 15. *Let H be a subgroup of G and E be its fixed field. Then $H = Gal(L/E)$ and L is a galois extension of E. Thus by Hilbert's Theorem 90 (Theorem 20), we have $H^1(H,L^*) = 0$. Also $H^2(H,L^*)$ is a cyclic group with order equal to $[L:E] = |H|$ because of Remark 14. Thus hypothesis of the Tate's theorem (Theorem 45) is satisfied.*

Remark 16. *By Tate's Theorem (Theorem 45), $\forall\ r \in \mathbb{Z}$, there is an isomorphism $H^r(G,\mathbb{Z}) \to H^{r+2}(G,L^*)$ which is cup-product with the local fundamental class. In particular for $r = -2$, we get the isomorphism $H^{-2}(G,\mathbb{Z}) \to H^0(G,L^*)$ i.e. an isomorphism $G \to K^*/Nm(L^*)$.*

Definition 29. *By Remark 16, there is an isomorphism $G \to K^*/Nm(L^*)$ given by cup product with the local fundamental class. The inverse isomorphism*

$$K^*/Nm(L^*) \to G$$

is known as the Local Artin Map.

We now compute the Local Artin Map explicitly using the proof of Tate's theorem. To achieve this goal, we have to firstly find an explicit description of the local fundamental class (because the proof of Tate's theorem requires us to know a generator of $H^2(L/K)$). Firstly we need to find a map $f : G \to \mathbb{Q}/\mathbb{Z}$ such that $f(\sigma) = \frac{1}{n} + \mathbb{Z}$. But then the map f is uniquely characterized by this condition.

Now we have to find the image of f under the boundary map δ. We will use the explicit description of the boundary map provided in Remark 4. We first need to choose a lift of f to 1-cochain $\bar{f} : G \to \mathbb{Q}$. Define $\bar{f} : G \to \mathbb{Q}$ such that $\bar{f}(\sigma) = \frac{1}{n}$. Clearly $\bar{f}$ is a lift of f. Then $\delta\bar{f} \in H^2(G,\mathbb{Z})$ such that

$$\delta\bar{f}(\sigma^i,\sigma^j) = \sigma^i\bar{f}(\sigma^j) - \bar{f}(\sigma^{i+j}) + \bar{f}(\sigma^i)$$

Since G acts trivially on $\mathbb{Q}$, we get $\delta\bar{f}(\sigma^i,\sigma^j) =$

$$\begin{cases} 0 & i+j < n \\ 1 & i+j \geq n \end{cases}$$

Now let us get back to $H^2(G,L^*)$ from $H^2(G,\mathbb{Z})$ via the inverse map η_2. The local fundamental class is the image of $\delta(\bar{f})$ in $H^2(G,L^*)$. Thus the local fundamental class $u_{L/K}$ is represented by the cocycle ϕ in $H^2(L/K)$ where $\phi(\sigma^i,\sigma^j) =$

$$\begin{cases} 1 & i+j < n \\ \pi & i+j \geq n \end{cases}$$

Remark 17. *Let π_1 and π_2 be two different primes in O_K. This means that they both generate the same ideal m_K in O_K. Thus they are associates i.e. $\pi_1 = u\pi_2$ for some $u \in U_K$. By Theorem 60, we know that $u = Nm_{L/K}u'$ for some $u' \in U_L$. Therefore π_1 and π_2 have the same class in $Nm_{L/K}(L^*)$. Hence the class of uniformizer is independent of the chosen prime element π.*

Theorem 62. *Under the inverse of Local Artin Map $G \to K^*/Nm_{L/K}(L^*)$, the Frobenius element $\sigma \in G$ maps to the class of π in $K^*/Nm_{L/K}(L^*)$.*

Proof. We will basically trace through the isomorphisms in the proof of Tate's theorem.

Firstly we need to find the image of σ in $H^{-1}(G, I_G)$. Recall from the proof of Theorem 32 that the map $H^{-2}(G,\mathbb{Z}) \to H^{-1}(G, I_G)$ is given as the boundary map $\eta : H_1(G,\mathbb{Z}) \to H_0(G, I_G)$ corresponding to the short exact sequence

$$0 \to I_G \to \mathbb{Z}[\mathbb{G}] \to \mathbb{Z} \to 0$$

Also by Remark 10, the map $G^{ab} \to H_1(G,\mathbb{Z})$ is given by composing the maps $G^{ab} \to I_G/I_G^2$ and $I_G/I_G^2 \xrightarrow{\eta^{-1}} H_1(G,\mathbb{Z})$.

Thus for finding the image of σ under the map $G \to H^{-1}(G, I_G)$, the maps η and η^{-1} cancel and we just get the image of σ in I_G/I_G^2 which is $(\sigma - 1) + I_G^2$.

Now we need to calculate the image of $(\sigma - 1) + I_G^2$ under the map $H^{-1}(G, I_G) \to H^0(G, L^*)$ which was described in Remark 11. Consider the following diagram :

$$\begin{array}{ccccccccc} & & & & & & H^{-1}(G,I) & & \\ & & & & & & \downarrow & & \\ & & (L^*)_G & \longrightarrow & L^*(\phi)_G & \longrightarrow & (I)_G & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & L^{*G} & \longrightarrow & L^*(\phi)^G & \longrightarrow & I^G & & \\ & & \downarrow & & & & & & \\ & & H^0(G,L^*) & & & & & & \end{array} \tag{3.5}$$

Firstly we have to find a preimage of $(\sigma - 1) + I_G^2$ under the map

$$(L^*(\phi))_G \to I_G/I_G^2$$

Consider the element $x_\sigma + I_G L^*(\phi) \in L^*(\phi)_G$. Then under this map (which we called α during the proof of Tate's theorem),

$$x_\sigma + I_G L^*(\phi) \mapsto (\sigma - 1) + I_G/I_G^2$$

Now we want to find the image of this element under the norm map $L^*(\phi)_G \to L^*(\phi)^G$ (which is given by $Nm_G = \sum_{i=0}^{n-1} \sigma^i$) i.e. the image is equal to $\sum_{i=0}^{n-1} \sigma^i x_\sigma$. But the way action of G is defined on $L^*(\phi)$, we get

$$\sigma^i(x_\sigma) = x_{\sigma^{i+1}} - x_{\sigma^i} + \phi(\sigma^i, \sigma)$$

Thus

$$\sum_{i=0}^{n-1} \sigma^i x_\sigma = \sum_{i=0}^{n-1} \phi(\sigma^i, \sigma) = \pi$$

by the description of ϕ given just before Remark 17. Note that in the last equality, we have used the fact that L^* is a group under multiplication. So the symbol + actually means multiplication.

Since π is infact an element of K^*, thus π is the preimage of π under the inclusion $K^* \to L^*(\phi)^G$ and the image of π under the map $K^* \to H^0(G, L^*)$ is $\pi\ Nm_{L/K}(L^*)$ which completes the proof. $\square$

Corollary 8. *Under the Local Artin Map $K^*/Nm_{L/K}(L^*) \to G$, the class of the uniformizer maps to the Frobenius element.*

Now we want to define the invariant map for infinite unramified extensions as well. We need to be careful about the definition of the ord_L.

Let π be a generator of the maximal ideal m_K of O_K. Then for any $x \in L$, $x \in K'$ for some finite extension K' of K (eg. take $K' = K(x)$). Then K' is also unramified over K and we get $x = u\pi^n$ for some $u \in U_{K'}$ and some $n \in \mathbb{Z}$. Hence every element of L can be written in the form $u\pi^n$ for some $u \in U_L$ and some $n \in \mathbb{Z}$. Uniqueness of this expression is also immediate. Now we can define the ord_L map in the same way as for finite unramified extensions as we have got a short exact sequence

$$0 \to U_L \to L^* \xrightarrow{ord_L} \mathbb{Z} \to 0$$

3.4.2 Infinite Extensions

Consider a tower of field extensions

$$E \supset L \supset K$$

with both E and L unramified over K. Then E and L are also Galois over K because E is unramified over K means that any finite subextension of E over K is unramified which is then also galois (infact cyclic). Since E is a union of its finite subextensions, so E is a union of Galois extensions which shows that E is also Galois over K.

We denote $G = Gal(E/K)$, $H = Gal(E/L)$ is a subgroup of G. By infinite galois theory, we know that $G/H \cong Gal(L/K)$. For convenience, we denote G/H by G_1.

Theorem 63. *The following diagram commutes :*

$$\begin{array}{ccc} H^2(L/K) & \xrightarrow{inv_{L/K}} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle Inf} & & \downarrow{\scriptstyle Id} \\ H^2(E/K) & \xrightarrow{inv_{E/K}} & \mathbb{Q}/\mathbb{Z} \end{array} \tag{3.6}$$

Proof. To check the commutativity of this diagram, one has to check the commutativity of the following diagram :

$$\begin{array}{ccccccc} H^2(L/K) & \xrightarrow{ord_L} & H^2(G_1,\mathbb{Z}) & \xrightarrow{\delta_L^{-1}} & H^1(G_1,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{g\mapsto g(\sigma_{L/K})} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle Inf} & & \downarrow{\scriptstyle Inf} & & \downarrow{\scriptstyle Inf} & & \downarrow{\scriptstyle Id} \\ H^2(E/K) & \xrightarrow{ord_E} & H^2(G,\mathbb{Z}) & \xrightarrow{\delta_E^{-1}} & H^1(G,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{g\mapsto g(\sigma_E)} & \mathbb{Q}/\mathbb{Z} \end{array} \tag{3.7}$$

We want to show the commutativity of the first square. Let $\phi : G_1^2 \to L^*$ be a 2-cocycle. Then $Inf(ord_L(\phi))(g_1,g_2) = ord_L(\phi(g_1H,g_2H))$. Now $Inf(\phi)(g_1,g_2) = \phi(g_1H,g_2H)$ and thus $ord_E(Inf(\phi(g_1,g_2))) = ord_E(\phi(g_1H,g_2H)) = ord_L(\phi(g_1H,g_2H))$ since $\phi(g_1H,g_2H) \in L^*$ and E is unramified over L.

Now we want to show the commutativity of the second square. Note that we have already shown that the following diagram commutes :

$$\begin{array}{ccc} H^1(G_1,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\delta_L} & H^2(G_1,\mathbb{Z}) \\ \downarrow{\scriptstyle Inf_1} & & \downarrow{\scriptstyle Inf_2} \\ H^1(G,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\delta_E} & \mathbb{Q}/\mathbb{Z} \end{array} \tag{3.8}$$

Hence we have $Inf_2 \circ \delta_L = \delta_E \circ Inf_1$ which implies $\delta_E^{-1} \circ Inf_2 = Inf_1 \circ \delta_L^{-1}$ by precomposition with δ_E^{-1} and postcomposition with δ_L^{-1} . This completes the proof of commutativity of the second square.

Finally we will show the commutativity of the third square. Let $\phi \in Hom(G_1,\mathbb{Z})$. Then for any $\tau \in G$, we have $(Inf(\phi))(\tau)) = \phi(\tau H)$ and thus by Lemma 41,

$$Inf(\phi) \mapsto (Inf(\phi))(\sigma_{E/K}) = \phi(\sigma_{E/K}H) = \phi(\sigma_{L/K})$$

This completes the proof of commutativity of the third square. □

Theorem 64. *There exists a unique isomorphism*

$$inv_K : H^2(K^{un}/K) \to \mathbb{Q}/\mathbb{Z}, \tag{3.9}$$

with the property that, for every $L \subset K^{un}$ of finite degree n over K, inv_K induces the isomorphism

$$inv_{L/K} : H^2(L/K) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \tag{3.10}$$

Proof. We have already shown that $inv_{L/K} : H^2(L/K) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ is an isomorphism. Moreover, by Theorem 63, we have a commutative diagram :

$$\begin{array}{ccc} H^2(L/K) & \xrightarrow{inv_{L/K}} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle Inf} & & \downarrow{\scriptstyle Id} \\ H^2(K^{un}/K) & \xrightarrow{inv_K} & \mathbb{Q}/\mathbb{Z} \end{array} \tag{3.11}$$

Suppose that inv_K is not surjective. Hence there exists $\frac{i}{n} \in \mathbb{Q}$ such that $\frac{i}{n} + \mathbb{Z} \notin \mathrm{Im}(inv_K)$. Take L to be the unramified extension of K of degree n. Since $\frac{i}{n} + \mathbb{Z} \in \frac{1}{n}\mathbb{Z}/\mathbb{Z} = \mathrm{Im}(inv_{L/K})$, so $\frac{i}{n} + \mathbb{Z} \in \mathrm{Im}(inv_K)$ by the commutativity of diagram which is a contradiction. Hence inv_K is surjective.

Now we will prove that inv_K is injective. Let $\bar{\phi} \in H^2(K^{un}/K)$ such that $inv_K(\bar{\phi}) = 0$.

For any L finite unramified over K, we have $Inf(H^2(L/K)) \subset H^2(K^{un}/K)$. We also have that for any finite unramified extensions L_1 and L_2 of K, $Inf(H^2(L_1/K)) \subset Inf(H^2(L_1L_2/K))$ and $Inf(H^2(L_2/K)) \subset Inf(H^2(L_1L_2/K))$. This follows from the commutativity of the following diagram (which can be verified directly) :

$$\begin{array}{ccc} H^2(L_1/K) & & \\ \Big\downarrow{\scriptstyle Inf'} & \overset{Inf}{\searrow} & \\ H^2(L_1L_2/K) & \xrightarrow{Inf} & H^2(K^{un}/K) \end{array} \tag{3.12}$$

Hence we have

$$H^2(K^{un}/K) \cong \varinjlim_L H^2(L/K) \cong \varinjlim_L Inf(H^2(L/K)) \cong \bigcup_L Inf(H^2(L/K))$$

The second congruence follows from the fact that the inflation map is injective and thus for each L, we have $H^2(L/K) \cong Inf(H^2(L/K))$. For the last congruence, see Ex. 17, Ch. 2, page 33 of [12].

Thus for any $\bar{\phi} \in H^2(K^{un}/K)$, we have $\bar{\phi} = Inf(\bar{\psi})$ for some $\bar{\psi} \in H^2(L, K)$ for some finite unramified extension L over K.

Therefore by commutativity of diagram 3.11, we have

$$inv_{L/K}(\bar{\psi}) = inv_K(Inf(\bar{\psi})) = inv_K(\bar{\phi}) = 0$$

Since $inv_{L/K}$ is an isomorphism, so $\bar{\psi} = 0$ and thus $\bar{\phi} = 0$. This completes the proof that inv_K is injective. Thus we have shown that :

There exists an isomorphism

$$inv_K : H^2(K^{un}/K) \to \mathbb{Q}/\mathbb{Z}, \tag{3.13}$$

with the property that, for every $L \subset K^{un}$ of finite degree n over K, inv_K induces the isomorphism

$$inv_{L/K} : H^2(L/K) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \tag{3.14}$$

given as $inv_{L/K} = inv_K \circ Inf$. □

Now we have to check the uniqueness of such an isomorphism inv_K. Let

$$\Psi_K : H^2(K^{un}/K) \to \mathbb{Q}/\mathbb{Z}$$

be an isomorphism with the property that, for every $L \subset K^{un}$ of finite degree over K, Ψ_K induces the isomorphism

$$inv_{L/K} : H^2(L/K) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \tag{3.15}$$

i.e. $inv_{L/K} = \Psi_K \circ Inf$.

We know that for any $\bar{\phi} \in H^2(K^{un}/K)$, we have $\bar{\phi} = Inf(\bar{\psi})$ for some $\bar{\psi} \in H^2(L, K)$ for some finite unramified extension L over K. Hence

$$\Psi_K(\bar{\phi}) = \Psi_K(Inf(\bar{\psi})) = inv_{L/K}(\bar{\psi}) = inv_K(Inf(\bar{\psi})) = inv_K(\bar{\phi})$$

for any $\bar{\phi} \in H^2(K^{un}/K)$. Thus $inv_K = \Psi_K$ which completes the proof of uniqueness of the isomorphism.

Theorem 65. *Let L be a finite extension of K of degree n, and let K^{un} and L^{un} be the largest unramified extensions of K and L. Then the following diagram commutes :*

$$\begin{array}{ccc} H^2(K^{un}/K) & \xrightarrow{Res} & H^2(L^{un}/L) \\ \Big\downarrow{\scriptstyle inv_K} & & \Big\downarrow{\scriptstyle inv_L} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \end{array} \tag{3.16}$$

Proof. Since $L^{un} = LK^{un}$, so the map $Gal(L^{un}/L) \to Gal(K^{un}/K)$ given by $\tau \mapsto \tau \restriction_{K^{un}}$ is injective. Hence we can treat $Gal(L^{un}/L)$ as a subgroup of $Gal(K^{un}/K)$ and obtain the restriction maps $H^2(K^{un}/K) \to H^2(L^{un}/L)$. Note that these maps are not strictly restriction maps according to our earlier definitions as the modules are different, but since $K^{un*} \subset L^{un*}$, they are essentially restriction maps and we will see that they satisfy all properties of restriction maps.

To ease the notation, let's denote $Gal(K^{un}/K)$ by Γ_K and $Gal(L^{un}/L)$ by Γ_L.

We have to check the commutativity of the following diagram :

$$\begin{array}{ccccccc} H^2(K^{un}/K) & \xrightarrow{ord_K} & H^2(\Gamma_K, \mathbb{Z}) & \xrightarrow{\delta_K^{-1}} & H^1(\Gamma_K, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{g \mapsto g(\sigma_K)} & \mathbb{Q}/\mathbb{Z} \\ \Big\downarrow{\scriptstyle Res} & & \Big\downarrow{\scriptstyle eRes} & & \Big\downarrow{\scriptstyle eRes} & & \Big\downarrow{\scriptstyle fe} \\ H^2(L^{un}/L) & \xrightarrow{ord_L} & H^2(\Gamma_l, \mathbb{Z}) & \xrightarrow{\delta_L^{-1}} & H^1(\Gamma_L, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{g \mapsto g(\sigma_L)} & \mathbb{Q}/\mathbb{Z} \end{array} \tag{3.17}$$

where e is the ramification degree and f is the residual class degree.

In order to prove the commutativity of the first square, note that the following diagram commutes :

$$\begin{array}{ccc} K^{un*} & \xrightarrow{ord_K} & \mathbb{Z} \\ \Big\downarrow & & \Big\downarrow{\scriptstyle e} \\ L^{un*} & \xrightarrow{ord_L} & \mathbb{Z} \end{array} \tag{3.18}$$

Let m_K be generated by a prime element $\pi_K \in O_K$. Since ramification index for L/K is e, we have $\pi_K O_L = m_L^e$. Now let π_L be a generator for m_L. Thus $m_L = \pi_L O_L$ and so $\pi_K O_L = \pi_L^e O_L$ ie. $\pi_K = \pi_L^e u_0$ for some $u_0 \in U_L$. Now let $x \in K^{un*}$. Thus $x = u\pi_K^m$ for some $u \in O_{K^{un}}$ and some $m \in \mathbb{Z}$. The above discussion shows that $x = u(u_0\pi_L^e)^m$. Thus $ord_L(x) = em = eord_K(x)$ and we are done.

Now we use this diagram to prove the commutativity of the first square. Let $\phi : \Gamma_K^2 \to K^{un*}$ be a 2-cocyle representing an element of $H^2(K^{un}/K)$. Then $ord_K(\bar{\phi})$ is represented by a 2-cocycle $\psi : \Gamma_K^2 \to \mathbb{Z}$ where $\psi(\sigma_1.\sigma_2) = ord_K(\phi(\sigma_1, \sigma_2))$.Then $Res(\bar{\psi})$ is represented by a 2-cocylce $\eta : \Gamma_L^2 \to \mathbb{Z}$ where $\eta(\sigma_1, \sigma_2) = ord_K(\phi(\sigma_1, \sigma_2))$ and thus $(eRes)(\bar{\psi})$ is represented by a 2-cocylce $\eta^{'} : \Gamma_L^2 \to \mathbb{Z}$ where

$$\eta^{'}(\sigma_1, \sigma_2) = e(ord_K(\phi(\sigma_1, \sigma_2))) = ord_L(\phi(\sigma_1, \sigma_2))$$

by the commutativity of the above diagram. Also $Res(\bar{\phi})$ is represented by a 2-cocycle $\kappa : \Gamma_L^2 \to L^{un*}$ where $\kappa(\sigma_1, \sigma_2) = \phi(\sigma_1, \sigma_2)$ and so $ord_L(Res(\bar{\phi}))$ is represented by a 2-cocycle $\beta : \Gamma_L^2 \to \mathbb{Z}$ where $\beta(\sigma_1, \sigma_2) = ord_L(\phi(\sigma_1, \sigma_2))$. This shows that

$$(eRes)(ord_K(\bar{\phi})) = ord_L(Res(\bar{\phi}))$$

i.e. $eRes \circ ord_K = ord_L \circ Res$ and thus completes the proof of commutativity of the first square.

Now we want to show that the second square commutes. We have already shown that restriction map commutes with the boundary map and thus the following diagram is commutative :

$$\begin{array}{ccc} H^1(\Gamma_K, \mathbb{Z}) & \xrightarrow{\delta_K} & H^2(\Gamma_K, \mathbb{Z}) \\ \downarrow{\scriptstyle Res} & & \downarrow{\scriptstyle Res} \\ H^1(\Gamma_L, \mathbb{Z}) & \xrightarrow{\delta_L} & H^2(\Gamma_L, \mathbb{Z}) \end{array} \tag{3.19}$$

Multiplying both the vertical arrows by e does not affect the commutativity of the diagram i.e. we get a commutative diagram :

$$\begin{array}{ccc} H^1(\Gamma_K, \mathbb{Z}) & \xrightarrow{\delta_K} & H^2(\Gamma_K, \mathbb{Z}) \\ \downarrow{\scriptstyle eRes} & & \downarrow{\scriptstyle eRes} \\ H^1(\Gamma_L, \mathbb{Z}) & \xrightarrow{\delta_L} & H^2(\Gamma_L, \mathbb{Z}) \end{array} \tag{3.20}$$

i.e. $(eRes) \circ \delta_K = \delta_L \circ (eRes)$. Again precomposition with δ_L^{-1} and postcomposition with δ_K^{-1} gives us $\delta_L^{-1} \circ (eRes) = (eRes) \circ \delta_K^{-1}$. So we have shown that the second square also commutes.

Now we want to show that the third square commutes. Consider the following diagram :

$$\begin{array}{ccc} Hom(\Gamma_K, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{g \mapsto g(\sigma_K)} & \mathbb{Q}/\mathbb{Z} \\ \Big\downarrow {\scriptstyle g \mapsto g \restriction_{\Gamma_L}} & & \Big\downarrow {\scriptstyle f} \\ Hom(\Gamma_L, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{g \mapsto g(\sigma_L)} & \mathbb{Q}/\mathbb{Z} \end{array} \tag{3.21}$$

Let g be a continuous homomorphism from Γ_K to $\mathbb{Q}/\mathbb{Z}$. To show the commutativity of this diagram, we have to show that $fg(\sigma_K) = g \restriction_{\Gamma_L} (\sigma_L)$ but this is true since $\sigma_L \restriction_{K^{un}} = \sigma_K^f$ by Lemma 42. Multiplying the vertical maps with e does not disturb the commutativity of the diagram and we get that the third square also commutes. □

3.5 Ramified Extensions

Let $E \supset L \supset K$ be a tower of Galois extensions. Note that E is automatically Galois over K since E is Galois over K. Also let $G = Gal(E/K), H = Gal(E/L)$. Then $G/H \cong Gal(L/K)$. By Hilbert's Theorem 90, we know that $H^1(H, E^*) = H^1(Gal(E/L), E^*) = 0$ (by treating L as the base field instead of K). Hence by the inflation - restriction exact sequence (for $r = 2$), we get that the sequence

$$0 \to H^2(L/K) \xrightarrow{Inf} H^2(E/K) \xrightarrow{Res} H^2(E/L)$$

is exact. In particular, the Inf map in this setting is injective. This general setting would be used again and again in this section by taking different fields E, L and K.

Theorem 66. *For every local field K, there exists a canonical isomorphism*

$$inv_K : H^2(K^{al}/K) \to \mathbb{Q}/\mathbb{Z}.$$

Moreover, if L is a finite extension of K with $[L : K] = n$, then the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2(L/K) & \xrightarrow{Inf} & H^2(K^{al}/K) & \xrightarrow{Res} & H^2(K^{al}/L) \\ & & & & \Big\downarrow {\scriptstyle inv_K} & & \Big\downarrow {\scriptstyle inv_L} \\ 0 & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \end{array} \tag{3.22}$$

commutes. Furthermore, if L/K is Galois, then there is an isomorphism

$$inv_{L/K} : H^2(L/K) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

such that

$$inv_K \circ Inf = inv_{L/K}$$

Remark 18. *At the first sight, it might seem that there is a discrepancy in the notation inv_L as one would expect it to denote $inv_L : H^2(L^{al}/L) \to \mathbb{Q}/\mathbb{Z}$ instead of $inv_L : H^2(K^{al}/L) \to \mathbb{Q}/\mathbb{Z}$ but this problem is easily overcome by the the observation that $L^{al} \cong K^{al}$ since $L \subset K^{al}$ and so K^{al} is also an algebraic closure for L.*

Remark 19. *$m_L^n = B(0, |\pi_L|^n)$ is an open neighborhood of 0. Moreover, if U is an open set containing 0, then U contains some ball $B(0,r)$. Choose n such that $|\pi_L|^n < r$ and thus $B(0,|\pi_L|^n) \subset B(0,r) \subset U$. Thus $\{m_L^n : n \in \mathbb{N}\}$ is a neighborhood base at 0. Similarly $\{U_L^n : n \in \mathbb{N}\}$ is a neighborhood base at 1 where $U_L^n = 1 + m_L^n = B(1, |\pi_L|^n)$.*

Note that the top row is obtained by taking the tower of Galois extensions $K^{al} \supset L \supset K$. The proof will require a few lemmas which we now prove.

Lemma 46. *If L/K is Galois of finite degree n, then $H^2(L/K)$ contains a subgroup canonically isomorphic to $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$.*

Proof. Consider the diagram :

$$\begin{array}{ccccccc} 0 & \longrightarrow & Ker(Res) & \xrightarrow{i} & H^2(K^{un}/K) & \xrightarrow{Res} & H^2(L^{un}/L) \\ & & \downarrow{\scriptstyle \eta} & & \downarrow{\scriptstyle Inf} & & \downarrow{\scriptstyle Inf} \\ 0 & \longrightarrow & H^2(L/K) & \xrightarrow{Inf} & H^2(K^{al}/K) & \xrightarrow{Res} & H^2(K^{al}/L) \end{array} \tag{3.23}$$

It is straightforward to show that the diagram commutes (since all the maps are canonical).

Note that the inflation maps $H^2(K^{un}/K) \to H^2(K^{al}/K)$ and $H^2(L^{un}/L) \to H^2(L^{al}/L)$ are injective. This can be shown by taking the tower of Galois extensions $K^{al} \supset K^{un} \supset K$ and $L^{al} \supset L^{un} \supset L$ respectively.

Since the first square is commutative and the maps i and Inf are injective, so η is injective as well. Thus $H^2(L/K)$ contains a subgroup which is isomorphic to $Ker(Res)$. In Theorem 65, we have proved that the following diagram commutes :

$$\begin{array}{ccc} H^2(K^{un}/K) & \xrightarrow{Res} & H^2(L^{un}/L) \\ \downarrow{\scriptstyle Inv_K} & & \downarrow{\scriptstyle Inv_L} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \end{array} \tag{3.24}$$

Since inv_K and inv_L are isomorphisms, $Ker(Res) \cong Ker(n) = \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. □

In order to prove Theorem 66, we need to show that $H^2(L/K)$ is infact isomorphic to $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Due to Lemma 46, it suffices to prove that $|H^2(L/K)| \leq n$.

Lemma 47. *Let L be a finite Galois extension of K with Galois group G. Then there exists an open subgroup V of O_L such that $H^r(G,V) = 0$ for all $r > 0$.*

Proof. By Normal Basis Theorem, there exists a basis $\{\tau x : \tau \in G\}$ of L over K. Since G is a finite group, $\min(ord_L(\tau x)) \in \mathbb{Z}$, say $m = \min(ord_L(\tau x))$. Choose $n \geq |m|$, then $\forall\ \tau \in G$,

$$ord_L(\tau(\pi_K^n x)) = ord_L(\pi_K^n \tau(x)) \geq 0$$

which means that $\pi_K^n \tau(x) \in O_L \ \forall \ \tau \in G$. Since

$$\{\tau(\pi^n x) : \tau \in G\}$$

is also a basis of L over K, without loss of generality we can assume that the basis $\{\tau x : \tau \in G\}$ of L over K is inside O_L. Define

$$V = \sum_{\tau \in G} \tau(x) O_K$$

Clearly V is a subgroup of O_L which is stable under G. Then $V \cong O_K[G]$ where the map $V \to O_K[G]$ is given as

$$\sum_{\tau \in G} \tau(x) u_\tau \mapsto \sum_{\tau \in G} \tau u_\tau$$

where $u_\tau \in O_K$. This map is well defined because of the linear independence of the basis $\{\tau x : \tau \in G\}$ of L over K. Since G is a finite group, we can label it as

$$G = \{\tau_1, \tau_2, ..., \tau_n\}$$

Now $O_K[G] \cong Ind^G O_K$ given by the noncanonical map $\eta : O_K[G] \to Ind^G O_K$ such that $\sum_{i=1}^n u_i \tau_i \mapsto \phi$ where

$$\phi(\tau_i) = u_j$$

and j is defined as $\tau_j = \tau_i^{-1}$. The inverse map $\eta^{'} : Ind^G O_K \to O_K[G]$ is given by

$$\psi \mapsto \sum_{i=1}^n \psi(g_i^{-1}) g_i$$

It is straightforward to show that the maps η and $\eta^{'}$ are actually inverses of each other. The map η is also a G-module map since

$$\eta\left(\tau\left(\sum_{j=1}^n u_j \tau_j\right)\right) = \eta\left(\sum_{j=1}^n u_j(\tau\tau_j)\right) = \phi^{'}$$

where $\phi^{'}(\tau_i) = u_k$ where k is defined as $\tau\tau_k = \tau_i^{-1}$ i.e. $\tau_k = \tau^{-1}\tau_i^{-1}$ and

$$\tau\left(\eta\left(\sum_{j=1}^n u_j(\tau_j\right)\right) = \tau(\phi)$$

Now $(\tau(\phi))(\tau_i) = \phi(\tau_i\tau) = u_l$ where l is defined as $\tau_l = (\tau_i\tau)^{-1} = \tau^{-1}\tau_i^{-1}$. Hence $\tau_k = \tau_l$ which means that $k = l$ and so $u_k = u_l$.

Therefore the map η is a G-module isomorphism. Thus $O_K[G]$ is an induced G module and so $H^r(G, O_K[G]) = 0 \ \forall \ r > 0$ which implies that $H^r(G, V) = 0 \ \forall \ r > 0$.

We are only left to prove that V is open in O_L. It suffices to show that V is open in L.

Since L is a finite dimensional vector space over K with basis $\{\tau_1(x), ..., \tau_n(x)\}$, so we have a K-vector space isomorphism

$$\phi : L \to \prod_{\tau \in G} K$$

given by

$$\sum_{i=1}^{n} \alpha_i \tau_i(x) \mapsto (\alpha_1, ..., \alpha_n)$$

Let $|\,|_\infty$ be a metric on $\prod_{\tau \in G} K$ defined such that

$$|(\alpha_1, ..., \alpha_n)|_\infty = \max_{1 \le i \le n} |\alpha_i|$$

Then ϕ is a homeomorphism between $(\prod_{\tau \in G} K, |\,|_\infty)$ and $(L, |\,|)$. This follows from a basic fact in Functional Analysis which says that any two norms on a finite dimensional Banach space are equivalent. Now observe that

$$\phi\left(\prod_{\tau \in G} O_K\right) = V$$

Since $\prod_{\tau \in G} O_K$ is an open subset of $\prod_{\tau \in G} K$, so V is open subset of L and we are done. □

Lemma 48. *Let L, K and G, be as in the last lemma. Then there exists an open subgroup V of U_L stable under G such that $H^r(G, V) = 0 \ \forall\ r > 0$.*

Proof. We prove this only for the case char$(K) = 0$. We know that $m_L^n \cong U_L^{(n)}$ as abelian groups whenever $n > \frac{ord(p)}{p-1}$. The isomorphism $m_L^n \to U_L^{(n)}$ is given by

$$x \mapsto \exp x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

with the inverse map $U_L^{(n)} \to m_L^n$ given by

$$x \mapsto \log x = \sum_{n=1}^{\infty} (-1)^{(n-1)} x^n$$

It is infact a G-module isomorphism because the action of G is continuous and so

$$\sigma(\exp x) = \sigma\left(\lim_{n\to\infty} \sum_{i=0}^{n} \frac{x^i}{i!}\right) = \lim_{n\to\infty}\left(\sigma \sum_{i=0}^{n} \frac{x^i}{i!}\right) = \lim_{n\to\infty}\left(\sum_{i=0}^{n} \frac{(\sigma x)^i}{i!}\right) = \exp(\sigma(x))$$

Choose an open subgroup V' of O_L stable under G such that $H^r(G, V') = 0 \ \forall\ r > 0$. Choose M such that $M > \frac{ord(p)}{p-1}$. Then $\pi_K^M V'$ is stable under G since $\sigma(\pi_K) = \pi_K$. Moreover, we have

$$\pi_K^M V' = \pi_L^{eM} V'$$

Also V' is an open neighborhood of 0, so $V' = \cup_n m_L^n$ which implies that $\pi_L^{eM} V' = \cup_n m_L^{n+eM}$ is also an open subgroup of O_L. Moreover, there is a G-module isomorphism $V' \to \pi_K^M V'$ such that $x \mapsto \pi_K^M x$ with the inverse map $\pi_K^M V' \to V'$ given by $\pi_K^m x \mapsto x$. Thus $H^r(G, \pi_K^M V') \cong H^r(G, V) = 0$. Since

$$ord(\pi_K^M V') = M + ord(V') \ge M > \frac{ord(p)}{p-1}$$

so we can take the exponential

$$V = \exp(\pi_L^{eM} V')$$

under the isomorphism $\exp : m_L^{eM} \to U_L^{(M)}$. It is easy to verify that V is stable under G. Also $H^r(G, V) = 0$ since $H^r(G, \pi_L^{eM} V') = 0$. Moreover, we had $\pi_L^{eM} V' = \cup_n m_L^{n+eM}$, and so

$$V = \exp(\pi_L^{eM} V') = \cup_n \exp(m_L^{n+eM}) = \cup_n U_L^{n+eM}$$

is an open subgroup of U_L. □

Lemma 49. *Let L/K be a cyclic extension of degree n; then $h(U_L) = 1$ and $h(L^*) = n$.*

Proof. Let V be an open subgroup of U_L with $H^r(G, V) = 0 \ \forall\ r \in \mathbb{Z}$ as in Lemma 48. Take the cosets of V in U_L. We have $U_L = \bigcup_S gV$ where S is a set of coset representatives of V in U_L. Since V is open, so is each gV because the map "multiplication by g" is a topological isomorphism. Since U_L is compact, there must be a finite subcover i.e. S is finite. Hence U_L/V is finite, which implies $h(U_L/V) = 1$ by Theorem 43. Since

$$h(U_L) = h(V)h(U_L/V)$$

by Lemma 42, so $h(U_L) = h(V)$. But note that

$$h(V) = \frac{|H^0(G, V)|}{|H^1(G, V)|} = \frac{1}{1} = 1$$

Also we have the exact sequence $0 \to U_L \to L^* \to \mathbb{Z} \to 0$. Thus

$$h(L^*) = h(U_L)h(\mathbb{Z}) = h(\mathbb{Z}) = \frac{|H^0(G, \mathbb{Z})|}{|H^1(G, \mathbb{Z})|} = \frac{n}{1} = n$$

□

Lemma 50. *Let L be a finite Galois extension of order n, then $H^2(L/K)$ has order n.*

Proof. We prove by induction on $[L : K]$. Clearly the base case ($n = 1$) is true. Now let L be an extension of K such that $L \neq K$. If L/K is cyclic we are done by Lemma 49 and periodicity of cohomology groups. So we assume that L/K is not cyclic. We know that the group $Gal(L/K)$ is solvable, thus it has a finite composition series

$$G = G_0 \supset G_1 \supset G_2 ...... \supset G_n = \{1\}$$

where each G_i/G_{i+1} is nontrivial, finite abelian and simple (so cyclic). Note that since G is not cyclic, so $n \neq 1$ i.e. $n \geq 2$ and thus G contains a proper nontrivial normal subgroup G_1. By Galois theory, there exists a Galois extension $K' \subset L$ over K such that $K' \neq K$ and $K' \neq L$.

Thus we can apply the induction hypothesis to conclude that $H^2(K'/K) = [K'/K]$ and $H^2(L/K') = [L : K']$. Since we have an exact sequence

$$0 \to H^2(K'/K) \to H^2(L/K) \to H^2(L/K')$$

so

$$\frac{|H^2(L/K)|}{|H^2(K'/K)|} \ \leq \ |H^2(L/K')|$$

i.e.

$$|H^2(L/K)| \ \leq \ |H^2(K'/K)|\,|H^2(L/K')| = [K' : K]\,[L : K'] \ = \ [L : K]$$

and thus we are done since by Lemma 46, we know that $|H^2(L/K)| \geq n$.

□

Proof. Now let us complete the proof of Theorem 66. We know by the proof of Theorem 64 that

$$H^2(K^{al}/K) = \bigcup Inf(H^2(L/K))$$

where L runs over finite extensions of K. We now want to show that it suffices to take the union over finite Galois extensions of K. Let Ω_1 be the collection of all finite extensions of K and Ω_2 be the collection of all finite Galois extensions of K. We want to show that

$$\bigcup_{L\in\Omega_1} Inf(H^2(L/K)) = \bigcup_{L\in\Omega_2} Inf(H^2(L/K))$$

Since $\Omega_2 \subset \Omega_1$ so it is clear that

$$\bigcup_{L\in\Omega_2} Inf(H^2(L/K)) \subset \bigcup_{L\in\Omega_1} Inf(H^2(L/K))$$

Conversely if we take L to be any finite extension of K, then we can take a finite Galois extension L' over K containing L. We know that the following diagram commutes :

$$\begin{array}{ccc} H^2(L/K) & \xrightarrow{Inf} & \\ \downarrow{\scriptstyle Inf'} & \searrow & \\ H^2(L'/K) & \xrightarrow{Inf} & H^2(K^{al}/K) \end{array} \tag{3.25}$$

This shows that

$$Inf(H^2(L/K)) \subset Inf(H^2(L'/K))$$

Thus we have that

$$\bigcup_{L\in\Omega_1} Inf(H^2(L/K)) \subset \bigcup_{L\in\Omega_2} Inf(H^2(L/K))$$

This completes the proof that

$$H^2(K^{al}/K) = \bigcup Inf(H^2(L/K))$$

where L runs over finite Galois extensions of K. Hence an arbitrary element $\bar{\phi}$ of $H^2(K^{al}/K)$ is of the form $Inf(\bar{\psi})$ for some $\bar{\psi} \in H^2(L/K)$ for some L galois over K. Now again consider the diagram :

$$\begin{array}{ccccccc} 0 & \longrightarrow & Ker(Res) & \xrightarrow{i} & H^2(K^{un}/K) & \xrightarrow{Res} & H^2(L^{un}/L) \\ & & \downarrow{\scriptstyle \eta} & & \downarrow{\scriptstyle Inf} & & \downarrow{\scriptstyle Inf} \\ 0 & \longrightarrow & H^2(L/K) & \xrightarrow{Inf} & H^2(K^{al}/K) & \xrightarrow{Res} & H^2(K^{al}/L) \end{array} \tag{3.26}$$

We have shown that η is an isomorphism. Thus $(\bar{\psi}) = \eta(\bar{\kappa})$ for some $\bar{\kappa} \in Ker(Res)$.

Hence $\bar{\phi} = Inf(\eta(\kappa)) = (Inf \circ i)(\bar{\kappa}) = Inf(i(\bar{\kappa}))$. This proves that the map $Inf : H^2(K^{un}/K) \to H^2(K^{al}/K)$ is surjective as well and is thus an isomorphism.

Recall that we have also proved the commutativity of the following diagram (Theorem 65) :

$$\begin{array}{ccc} H^2(K^{un}/K) & \xrightarrow{Res} & H^2(L^{un}/L) \\ \downarrow{\scriptstyle Inv_K} & & \downarrow{\scriptstyle Inv_L} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \end{array} \tag{3.27}$$

This in turn proves the commutativity of the following diagram :

$$\begin{array}{ccccccc} 0 & \longrightarrow & Ker(Res) & \longrightarrow & H^2(K^{un}/K) & \xrightarrow{Res} & H^2(L^{un}/L) \\ & & \downarrow & & \downarrow{\scriptstyle Inv_K} & & \downarrow{\scriptstyle Inv_L} \\ 0 & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \end{array} \tag{3.28}$$

All the vertical maps are isomorphisms.

We can combine the diagram 3.28 to the diagram 3.26 which means to compose diagram 3.28 with the inverse of diagram 3.26 to get the following commutative diagram :

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2(L/K) & \xrightarrow{Inf} & H^2(K^{al}/K) & \xrightarrow{Res} & H^2(K^{al}/L) \\ & & \downarrow{\scriptstyle inv_{L/K}} & & \downarrow{\scriptstyle inv_K} & & \downarrow{\scriptstyle inv_L} \\ 0 & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \end{array} \tag{3.29}$$

In particular, the $inv_K : H^2(K^{al}/K) \to \mathbb{Q}/\mathbb{Z}$ and $inv_L : H^2(K^{al}/L) \to \mathbb{Q}/\mathbb{Z}$ maps are also isomorphisms. Then we can say that for any finite Galois extension L of K, inv_K induces the isomorphism $inv_{L/K} = inv_K \circ Inf$. □

Remark 20. *Note that the diagram in the Theorem 66 commutes even if L/K is not Galois because to show that this diagram commutes, it suffices to show that the right square in the diagram 3.23 and the diagram 3.27 commute. The condition L/K is Galois is required only to prove that the left square in the diagram 3.23 commutes and hence is not required for the commutativity of the diagram in the Theorem 66.*

3.6 The Fundamental Class

Definition 30. *Let L be a finite Galois extension of K with Galois group G. By Section 3.5, there are isomorphisms*

$$Ker(Res) \xrightarrow{inv_K} \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

and

$$Ker(Res) \xrightarrow{\eta} H^2(L/K)$$

Composition of these isomorphisms gives us the isomorphism

$$H^2(L/K) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

This isomorphism is known as the invariant map $inv_{L/K}$.

Definition 31. *Let L be a finite Galois extension of K with Galois group G. We define the fundamental class $u_{L/K}$ of $H^2(L/K)$ such that*

$$inv_{L/K}(u_{L/K}) = \frac{1}{[L:K]} + \mathbb{Z} \tag{3.30}$$

Since diagram 3.29 commutes and the map $Inf : H^2(L/K) \to H^2(K^{al}/K)$ is injective, $u_{L/K}$ is also uniquely determined as :

$$inv_K(Inf(u_{L/K})) = \frac{1}{[L:K]} + \mathbb{Z} \tag{3.31}$$

Since the Inf map is injective, we may identify $Inf(u_{L/K})$ with $u_{L/K}$ and the above condition is written as

$$inv_K(u_{L/K}) = \frac{1}{[L:K]} + \mathbb{Z}$$

Theorem 67. *Let $L \supset E \supset K$ with L/K galois. Then*

$$\begin{aligned} Res(u_{L/K}) &= u_{L/E} \\ Cor(u_{L/E}) &= [E:K]u_{L/K} \end{aligned} \tag{3.32}$$

Moreover if E/K is Galois,

$$Inf(u_{E/K}) = [L:E]u_{L/K}$$

Proof. There is a commutative diagram by Theorem 66 :

$$\begin{array}{ccc} H^2(K^{al}/K) & \xrightarrow{Res} & H^2(K^{al}/E) \\ \downarrow{\scriptstyle inv_K} & & \downarrow{\scriptstyle inv_E} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{E:K} & \mathbb{Q}/\mathbb{Z} \end{array} \tag{3.33}$$

There is also a commutative diagram :

$$\begin{array}{ccc} H^2(K^{al}/E) & \xrightarrow{Res} & H^2(K^{al}/L) \\ \downarrow{\scriptstyle inv_K} & & \downarrow{\scriptstyle inv_E} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{L:E} & \mathbb{Q}/\mathbb{Z} \end{array} \tag{3.34}$$

Combining the two diagrams together, we get a commutative diagram :

$$\begin{array}{ccccc} H^2(K^{al}/K) & \xrightarrow{Res} & H^2(K^{al}/E) & \xrightarrow{Res} & H^2(K^{al}/L) \\ \downarrow{\scriptstyle inv_K} & & \downarrow{\scriptstyle inv_E} & & \downarrow{\scriptstyle inv_L} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{E:K} & \mathbb{Q}/\mathbb{Z} & \xrightarrow{L:E} & \mathbb{Q}/\mathbb{Z} \end{array} \tag{3.35}$$

Now we need a helping lemma which can be proved by direct verification.

Lemma 51. *If we have a commutative diagram such that the rows are exact*

$$\begin{array}{ccccc} A & \xrightarrow{f_1} & B & \xrightarrow{g_1} & C \\ \downarrow{\scriptstyle \eta_1} & & \downarrow{\scriptstyle \eta_2} & & \downarrow{\scriptstyle \eta_3} \\ D & \xrightarrow{f_2} & E & \xrightarrow{g_2} & F \end{array} \tag{3.36}$$

then the following diagram is also commutative with exact rows :

$$\begin{array}{ccccc} Ker(f_1) & \xrightarrow{incl.} & Ker(g_1 \circ f_1) & \xrightarrow{f_1} & Ker(g_1) \\ \downarrow{\scriptstyle \eta_1} & & \downarrow{\scriptstyle \eta_1} & & \downarrow{\scriptstyle \eta_2} \\ Ker(f_2) & \xrightarrow{incl.} & Ker(g_2 \circ f_2) & \xrightarrow{f_2} & Ker(g_2) \end{array} \tag{3.37}$$

where the map "incl." is the inclusion map.

Remark 21. *The fact that the rows are exact is a part of the Kernel - Cokernel lemma which comes from the Extended Snake Lemma.*

Now we will apply Lemma 51 to our diagram. In our situation, we have $f_1 = Res : H^2(K^{al}/K) \to H^2(K^{al}/E)$, $g_1 = Res : H^2(K^{al}/E) \to H^2(K^{al}/L))$ and $g_1 \circ f_1 = Res : H^2(K^{al}/K) \to H^2(K^{al}/L)$.

Then by exactness of the inflation-restriction sequence (Theorem 36), we get $Ker(f_1) = Inf_1(H^2(E/K))$, $Ker(g_1 \circ f_1) = Inf_2(H^2(L/K))$ and $Ker(g_1) = Inf_3(H^2(L/E))$ where Inf_1 is the inflation map $Inf : H^2(E/K) \to H^2(K^{al}/K)$, Inf_2 is the inflation map $Inf : H^2(L/K) \to H^2(K^{al}/K)$ and Inf_3 is the inflation map $Inf : H^3(L/E) \to H^2(K^{al}/E)$.

Moreover, the maps η_i are just the invariant maps. Thus by Lemma 51, we get the commutative diagram with exact rows :

$$\begin{array}{ccccc} Inf_1(H^2(E/K)) & \xrightarrow{i} & Inf_2(H^2(L/K)) & \xrightarrow{Res} & Inf_3(H^2(L/E)) \\ \downarrow{\scriptstyle inv_K} & & \downarrow{\scriptstyle inv_K} & & \downarrow{\scriptstyle inv_L} \\ \frac{1}{(E:K)}\mathbb{Z}/\mathbb{Z} & \xrightarrow{incl.} & \frac{1}{(L:K)}\mathbb{Z}/\mathbb{Z} & \xrightarrow{(E:K)} & \frac{1}{(L:E)}\mathbb{Z}/\mathbb{Z} \end{array} \tag{3.38}$$

It is easy to verify that the following diagram commutes :

$$\begin{array}{ccccc} H^2(E/K) & \xrightarrow{Inf} & H^2(L/K) & \xrightarrow{Res} & H^2(L/E) \\ \downarrow{\scriptstyle Inf_1} & & \downarrow{\scriptstyle Inf_2} & & \downarrow{\scriptstyle Inf_3} \\ Inf_1(H^2(E/K)) & \xrightarrow{i} & Inf_2(H^2(L/K)) & \xrightarrow{Res} & Inf_3(H^2(L/E)) \end{array} \tag{3.39}$$

Combining these two diagrams, we get the following commutative diagram :

$$\begin{array}{ccccc} H^2(E/K) & \xrightarrow{Inf} & H^2(L/K) & \xrightarrow{Res} & H^2(L/E) \\ \downarrow{\scriptstyle inv_K \circ Inf_1} & & \downarrow{\scriptstyle inv_K \circ Inf_2} & & \downarrow{\scriptstyle inv_L \circ Inf_3} \\ \frac{1}{(E:K)}\mathbb{Z}/\mathbb{Z} & \xrightarrow{incl.} & \frac{1}{(L:K)}\mathbb{Z}/\mathbb{Z} & \xrightarrow{(E:K)} & \frac{1}{(L:E)}\mathbb{Z}/\mathbb{Z} \end{array} \tag{3.40}$$

Now by the diagram 3.29, we know that $inv_K \circ Inf_2 = inv_{L/K}$, $inv_K \circ Inf_1 = inv_{E/K}$ and $inv_{L/E} = inv_L \circ Inf_3$. Hence we get the following commutative diagram :

$$\begin{array}{ccccc} H^2(E/K) & \xrightarrow{Inf} & H^2(L/K) & \xrightarrow{Res} & H^2(L/E) \\ \downarrow{\scriptstyle inv_{E/K}} & & \downarrow{\scriptstyle inv_{L/K}} & & \downarrow{\scriptstyle inv_{L/E}} \\ \frac{1}{(E:K)}\mathbb{Z}/\mathbb{Z} & \xrightarrow{incl.} & \frac{1}{(L:K)}\mathbb{Z}/\mathbb{Z} & \xrightarrow{(E:K)} & \frac{1}{(L:E)}\mathbb{Z}/\mathbb{Z} \end{array} \tag{3.41}$$

The commutativity of the second square shows that

$$inv_{L/E}(Res(u_{L/K})) = [E:K] \;\; inv_{L/K}(u_{L/K})$$

but we already know that

$$inv_{L/K}(u_{L/K}) = \frac{1}{[L:K]} + \mathbb{Z}$$

Thus we get

$$inv_{L/E}(Res(u_{L/K})) = [E:K]\left(\frac{1}{[L:K]} + \mathbb{Z}\right) = \left(\frac{1}{[L:E]} + \mathbb{Z}\right)$$

But also

$$inv_{L/E}(u_{L/E}) = \frac{1}{[L:E]} + \mathbb{Z}$$

Hence

$$inv_{L/E}(Res(u_{L/K})) = inv_{L/E}(u_{L/E})$$

Since $inv_{L/E}$ is an isomorphism, so

$$Res(u_{L/K}) = u_{L/E}$$

Thus

$$Cor(u_{L/E}) = Cor(Res(u_{L/K})) = [E:K]\ \ u_{L/K}$$

Similarly, the commutativity of the first square in diagram 3.41 shows that

$$inv_{L/K}(Inf(u_{E/K})) = inv_{E/K}(u_{E/K})$$

We know that

$$inv_{E/K}(u_{E/K}) = \frac{1}{[E:K]} + \mathbb{Z}$$

Thus

$$inv_{L/K}(Inf(u_{E/K})) = \frac{1}{[E:K]} + \mathbb{Z}$$

But

$$\frac{1}{[E:K]} + \mathbb{Z} = \ [L:E]\ \ \left(\frac{1}{[L:K]} + \mathbb{Z}\right) = [L:E]\ \ inv_{L/K}(u_{L/K}) = inv_{L/K}([L:E]\, u_{L/K})$$

Therefore,

$$inv_{L/K}(Inf(u_{E/K})) = inv_{L/K}([L:E]\, u_{L/K})$$

and so

$$Inf(u_{E/K}) = [L:E]\, u_{L/K}$$

since $inv_{L/K}$ is an isomorphism. □

3.7 The Local Artin Map

Remark 22. *Let L be a finite Galois extension of K with Galois group G. Let H be a subgroup of G and E be its fixed field. Then $H = Gal(L/E)$ and L is a Galois extension of E. Thus by Hilbert's Theorem* 90 *(Theorem* 20*), we have $H^1(H, L^*) = 0$. Also $H^2(H, L^*)$ is a cyclic group with order equal to $[L : E] = |H|$ because of Theorem* 66*. Thus hypothesis of Tate's theorem (Theorem* 45*) is satisfied.*

Definition 32. *By Tate's Theorem, for every finite Galois extension of local fields L/K with Galois group G and $r \in \mathbb{Z}$, the homomorphism*

$$H_T^r(G, \mathbb{Z}) \to H_T^{r+2}(G, L^*)$$

defined by $x \mapsto x \cup u_{L/K}$ is an isomorphism. When $r = -2$, this becomes an isomorphism

$$G^{ab} \cong K^*/Nm_{L/K}(L^*)$$

where $G^{ab} = G/G^c$ is the abelianization of G. The inverse isomorphism

$$\phi_{L/K} : K^*/Nm_{L/K}(L^*) \cong G^{ab}$$

is known as the Local Artin Map $\phi_{L/K}$.

Remark 23. *The Local Artin Map naturally induces the map*

$$K^* \to Gal(L/K)^{ab}$$

This is a surjective map with kernel $Nm_{L/K}(L^*)$. We will denote this map also by $\phi_{L/K}$. Though there is some ambiguity in this notation but the notation will be clear from the context.

Lemma 52. *Let $L \supset E \supset K$ be a tower of local fields with L/K Galois. Then the following diagram commutes :*

$$\begin{array}{ccc} E^* & \xrightarrow{\phi_{L/E}} & Gal(L/E)^{ab} \\ \downarrow{\scriptstyle Nm_{E/K}} & & \downarrow{\scriptstyle i} \\ K^* & \xrightarrow{\phi_{L/K}} & Gal(L/K)^{ab} \end{array} \tag{3.42}$$

where the map i is the map induced by the inclusion map $Gal(L/E) \to Gal(L/K)$ and the map $\phi_{L/E}$ is induced by the Local Artin map $E^*/Nm_{L/E}(L^*) \to Gal(L/E)^{ab}$. Similarly $\phi_{L/K}$ is induced by the Local Artin map $K^*/Nm_{L/K}(L^*) \to Gal(L/K)^{ab}$.

Proof. By transitivity of the norm map, it is clear that the following diagram commutes :

$$\begin{array}{ccc} E^* & \longrightarrow & E^*/Nm_{L/E}(L^*) \\ \downarrow{\scriptstyle Nm_{E/K}} & & \downarrow{\scriptstyle Nm_{E/K}} \\ K^* & \longrightarrow & K^*/Nm_{E/K}(E^*) \end{array} \tag{3.43}$$

Thus it suffices to prove that the following diagram commutes :

$$\begin{array}{ccc} E^*/Nm_{L/E}(L^*) & \xrightarrow{\phi_{L/E}} & Gal(L/E)^{ab} \\ \Big\downarrow{\scriptstyle Nm_{E/K}} & & \Big\downarrow{\scriptstyle i} \\ K^*/Nm_{E/K}(E^*) & \xrightarrow{\phi_{L/K}} & Gal(L/K)^{ab} \end{array} \tag{3.44}$$

To prove

$$i \circ \phi_{L/E} = \phi_{L/K} \circ Nm_{E/K}$$

it suffices to show that

$$\phi_{L/K}^{-1} \circ \ i = Nm_{E/K} \circ \ \phi_{L/E}^{-1}$$

i.e. the following diagram commutes :

$$\begin{array}{ccc} Gal(L/E)^{ab} & \xrightarrow{\phi_{L/E}^{-1}} & E^*/Nm_{L/E}(L^*) \\ \Big\downarrow{\scriptstyle i} & & \Big\downarrow{\scriptstyle Nm_{E/K}} \\ Gal(L/K)^{ab} & \xrightarrow{\phi_{L/K}^{-1}} & K^*/Nm_{E/K}(E^*) \end{array} \tag{3.45}$$

We know that the map $\phi_{L/K}^{-1}$ is given by cup product with the local fundamental class $u_{L/K}$ and the map $\phi_{L/E}^{-1}$ is given by cup product with the local fundamental class $u_{L/E}$. Moreover, by Remark 7 and Theorem 38, the maps i and $Nm_{E/K}$ are nothing but the corestriction maps in dimension -2 and 0 respectively. Thus we are just required to show

$$Cor(x \cup u_{L/E}) = Cor(x) \cup u_{L/K}$$

But we know a standard property of cup products (Lemma 26)

$$Cor(a \cup Res(b)) = Cor(a) \cup b$$

which tells us that

$$Cor(x \cup (Res(u_{L/K})) = Cor(x) \cup u_{L/K}$$

But by Theorem 67, we know that $Res(u_{L/K}) = u_{L/E}$ and so we are done. □

Lemma 53. *For every $\kappa \in H^1(Gal(L/K), \mathbb{Q}/\mathbb{Z})$ and $a \in K^*$, we have*

$$\kappa(\phi_{L/K}(a)) = inv_K(a \cup \delta\kappa)$$

Proof. To ease notation, we set $\sigma_a = \phi_{L/K}(a)$ and $\overline{\sigma_a}$ the element of $H^{-2}(G, \mathbb{Z})$ which corresponds to $\phi_{L/K}(a)$ under the isomorphism $H^{-2}(G, \mathbb{Z}) \cong G^{ab}$. We denote by $\overline{a}$ the class of a in $H^0(G, L^*)$. Since $\phi_{L/K}^{-1} : H^{-2}(G, \mathbb{Z}) \to H^0(G, L^*)$ is given by cup product with the local fundamental class $u_{L/K}$, so we have

$$\overline{\sigma_a} \cup u_{L/K} = \overline{a}$$

Thus

$$\overline{a} = u_{L/K} \cup \overline{\sigma_a}$$

since we know that $b \cup a = (-1)^{pq}(a \cup b)$. Therefore,

$$\overline{a} \cup \delta\kappa = (u_{L/K} \cup \overline{\sigma_a}) \cup \delta\kappa = u_{L/K} \cup (\overline{\sigma_a} \cup \delta\kappa) = u_{L/K} \cup \delta(\overline{\sigma_a} \cup \kappa)$$

since $\delta(a \cup b) = (-1)^p(a \cup \delta(b))$. By Lemma 29, we have

$$\overline{\sigma_a} \cup \kappa = \overline{\kappa(\sigma_a)} = \frac{r}{n} + \mathbb{Z} \in \frac{1}{n}\mathbb{Z}/\mathbb{Z} = H^{-1}(G, \mathbb{Q}/\mathbb{Z})$$

for some r where $n = |G|$. Note that the last equality follows from the fact that G has trivial action on $\mathbb{Q}/\mathbb{Z}$ which means that the Kernel of norm map is $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ and $I_G(\mathbb{Q}/\mathbb{Z}) = 0$. Now we want to find $\delta(\overline{\kappa(\sigma_a)})$. We have to again use the description of the map $H^{-1}(G, \mathbb{Q}/\mathbb{Z}) \to H^0(G, \mathbb{Z})$ provided in Remark 11.

Firstly note that $\frac{r}{n}$ itself is a preimage of $\frac{r}{n} + \mathbb{Z}$ under the map $\mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$. Since G has trivial action on Q, so norm of $\frac{r}{n}$ is equal to $n(\frac{r}{n}) = r$. Again r itself is a preimage of r under the inclusion map $\mathbb{Z} \to \mathbb{Q}$. Thus we have

$$\delta(\overline{\sigma_a} \cup \kappa) = \delta(\overline{\kappa(\sigma_a)}) = \delta\left(\frac{r}{n} + \mathbb{Z}\right) = r + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z} = H^0(G, \mathbb{Z})$$

Therefore,

$$\overline{a} \cup \delta\kappa = u_{L/K} \cup (r + n\mathbb{Z})$$

Note that $u_{L/K} \cup (r + n\mathbb{Z})$ need to be calculated through the map

$$H^2(G, L^*) \to H^2(G, L^* \otimes \mathbb{Z}) \cong H^2(G, L^*)$$

where the last isomorphism is induced by the isomorphism

$$L^* \otimes \mathbb{Z} \to L^*$$

given by $x \otimes n \mapsto x^n$. Thus under this composite map, we have

$$u_{L/K} \mapsto u_{L/K} \otimes r \mapsto u_{L/K}^r$$

where the first step is because of Theorem 40. Hence

$$inv_K(u_{L/K} \cup (r+n\mathbb{Z})) = inv_K(u_{L/K}^r) = r\ inv_K(u_{L/K}) = r\left(\frac{1}{n} + \mathbb{Z}\right) = \frac{r}{n} + \mathbb{Z} = \kappa(\sigma_a) = \kappa(\phi_{L/K}(a))$$

□

Theorem 68. *Let $L \supset E \supset K$ be local fields with both L and E Galois over K. Then the following diagram commutes :*

$$\begin{array}{ccc} K^* & \xrightarrow{\phi_{L/K}} & Gal(L/K)^{ab} \\ \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \pi} \\ K^* & \xrightarrow{\phi_{E/K}} & Gal(E/K)^{ab} \end{array} \tag{3.46}$$

where the map π is induced by the surjective map $Gal(L/K) \to Gal(E/K)$ given by $\sigma \mapsto \sigma_E$.

Proof. As usual we denote $Gal(L/K)$ by G, $Gal(L/E)$ by H and then $G/H \cong Gal(E/K)$. For any character $\kappa \in H^1(G/H, \mathbb{Q}/\mathbb{Z})$, we have $inf(\kappa) \in H^1(G, \mathbb{Q}/\mathbb{Z})$. Then by definition of inflation map, for any $g \in G$, we have

$$(inf(\kappa))(g) = \kappa(gH) = \kappa(\pi(g))$$

Therefore,

$$\kappa(\pi(\phi_{L/K}(a)) = (inf(\kappa))(\phi_{L/K}(a)) = inv_{L/K}(\overline{a} \cup \delta(inf\kappa))$$

by Lemma 53. Since we know that inflation maps commute with the boundary map (Theorem 27), so

$$inv_{L/K}(\overline{a} \cup \delta(inf\kappa)) = inv_{L/K}(\overline{a} \cup \mathrm{inf}(\delta\kappa)) = inv_{L/K}(inf(\overline{a} \cup \delta\kappa)) = inv_{E/K}(\overline{a} \cup \delta\kappa)$$

because $inv_{E/K} = inv_{L/K} \circ inf$ by diagram 3.41. But

$$inv_{E/K}(\overline{a} \cup \delta\kappa) = \kappa(\phi_{E/K}(a)))$$

by Lemma 53. Hence for every $\kappa \in H^1(G/H, \mathbb{Q}/\mathbb{Z})$, we have

$$\kappa(\pi(\phi_{L/K}(a)) = \kappa(\phi_{E/K}(a))$$

which shows that

$$\pi(\phi_{L/K}(a)) = \phi_{E/K}(a)$$

□

Remark 24. *Theorem 68 immediately implies that if $L \supset E \supset K$ is a tower of finite abelian extensions of K, then $\forall\ a \in K^*$,*

$$\phi_{L/K}(a) \restriction_E = \phi_{E/K}(a)$$

Definition 33. *We define the Local Artin Map ϕ_K*

$$\phi_K : K^* \to Gal(K^{ab}/K)$$

to be the homomorphism such that for every finite abelian extension L/K,

$$\phi_K(a) \restriction_L = \phi_{L/K}(a)$$

Theorem 69. *For every local field K, there exists a homomorphism (local Artin map)*

$$\phi_K : K^* \to Gal(K^{ab}/K)$$

with the following properties :
(a) for every prime element π of K, $\phi_K(\pi) \restriction_{K^{un}} = Frob_K$;
(b) for every finite abelian extension L of K, $Nm_{L/K}(L^*)$ is contained in the kernel of $a \mapsto \phi_K(a) \restriction_L$, and ϕ_K induces an isomorphism

$$\phi_{L/K} : K^*/Nm_{L/K}(L^*) \to Gal(L/K)$$

Proof. (b) is clear from the diagram :

$$\begin{array}{ccc} K^* & \xrightarrow{\phi_K} & Gal(K^{ab}/K)^{ab} \\ \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \pi} \\ K^* & \xrightarrow{\phi_{L/K}} & Gal(L/K)^{ab} \end{array} \tag{3.47}$$

To prove (a), observe that for any finite unramified extension L of K (which is then cyclic and hence abelian), we have

$$\phi_K(\pi) \restriction_L = \phi_{L/K}(\pi) = Frob_{L/K}$$

and thus

$$\phi_K(\pi) \restriction_{K^{un}} = Frob_K$$

□

Theorem 70. *(Norm Limitation Theorem) Let L be a finite extension of K, and let E be the largest abelian extension of K contained in L; then*

$$Nm_{L/K}(L^*) = Nm_{E/K}(E^*)$$

Proof. Note that $L \supset E \supset K$. Thus we have the transitivity of the norm map (proved earlier),

$$Nm_{L/K} = Nm_{E/K} \circ Nm_{L/E}$$

which shows that

$$Nm_{L/K}(L^*) \subset Nm_{E/K}(E^*)$$

Therefore, we have a surjective map

$$\eta : \frac{K^*}{Nm_{L/K}(L^*)} \to \frac{K^*}{Nm_{E/K}(E^*)}$$

such that

$$x + Nm_{L/K}(L^*) \mapsto x + Nm_{E/K}(E^*)$$

Firstly suppose that L/K is Galois. We will prove that in this case,

$$Gal(E/K) = Gal(L/K)^{ab}$$

We know that for any galois extension F of K in L,

$$Gal(F/K) \cong \frac{Gal(L/K)}{Gal(L/F)}$$

We know from basic group theory that for a normal subgroup H of G,

$$G/H \text{ } is \text{ } abelian \iff H \supset G^c$$

where G^c denotes the commutator subgroup of G. Thus F is abelian if and only if $Gal(L/F) \supset Gal(L/K)^c$ and $Gal(L/F)$ is normal in $Gal(L/K)$.

Also, we know that for $F_1 \subset F_2$, we have $Gal(L/F_1) \supset Gal(L/F_2)$. Since E is the largest abelian extension of K in L, so $Gal(L/E)$ is the smallest normal subgroup of $Gal(L/K)$ containing $Gal(L/K)^c$ which is infact equal to $Gal(L/K)^c$. Let F_0 be the fixed field of $Gal(L/K)^c$. Then by the Fundamental Theorem of Galois Theory, we have $F_0 = E$. Thus

$$Gal(L/E) \cong (Gal(L/K)^c)$$

Hence we get that

$$Gal(E/K) \cong \frac{Gal(L/K)}{Gal(L/E)} = \frac{Gal(L/K)}{Gal(L/K)^c} = Gal(L/K)^{ab}$$

This shows that

$$\mid Gal(E/K) \mid = \mid Gal(L/K)^{ab} \mid$$

Now the isomorphism of local Artin map shows that

$$|Gal(L/K)^{ab}| = \left| \frac{K^*}{Nm_{L/K}(L^*)} \right|$$

and

$$|Gal(E/K)| = |Gal(E/K)^{ab}| = \left| \frac{K^*}{Nm_{E/K}(E^*)} \right|$$

All these equations can be combined to conclude that

$$\left| \frac{K^*}{Nm_{L/K}(L^*)} \right| = \left| \frac{K^*}{Nm_{E/K}(E^*)} \right|$$

Thus η is also an injection and we get $Ker(\eta)$ is trivial which means that

$$Nm_{E/K}(E^*) \subset Nm_{L/K}(L^*)$$

and so

$$Nm_{E/K}(E^*) = Nm_{L/K}(L^*)$$

Now consider the general case (L/K need not be Galois).

We are going to assume $char(K) = 0$. Let L' be a finite Galois extension of K containing L (Such an extension can be constructed by adjoining all the roots of minimal polynomials of a primitive element of L over K which is the splitting field of a seperable polynomial and hence Galois). Let $G = Gal(L'/K)$ and $H = Gal(L'/L)$.

For any Galois extension F of K inside L', we have

$$Gal(F/K) \cong \frac{Gal(L'/K)}{Gal(L'/F)}$$

Thus F is an abelian extension of K inside L' if and only if $Gal(L'/F) \supset G^c$ and $Gal(L'/F)$ is normal in $Gal(L'/K)$. Moreover F is contained in L if and only if $Gal(L'/F) \supset Gal(L'/L) = H$.

Hence F is an abelian extension of K inside L if and only if $Gal(L'/F) \supset G^c H$ and $Gal(L'/F)$ is normal in $Gal(L'/K)$.

Also, we know that for $F_1 \subset F_2$, we have $Gal(L/F_1) \supset Gal(L/F_2)$. Since E is the largest abelian extension of K in L, so $Gal(L/E)$ is the smallest normal subgroup of $Gal(L/K)$ containing $G^c H$

which is infact equal to G^cH. Let F_0 be the fixed field of G^cH. Then by the Fundamental Theorem of Galois Theory, we have $F_0 = E$. Hence we know that

$$Gal(L'/E) \cong G^cH$$

and thus

$$Gal(E/K) \cong \frac{Gal(L'/K)}{Gal(L'/E)} = \frac{G}{G^cH}$$

Take any $a \in Nm_{E/K}(E^*)$. We have to show that $a \in Nm_{L/K}(L^*)$ (since we already know that $Nm_{L/K}(L^*) \subset Nm_{E/K}(E^*)$). Consider the commutative diagram obtained by combining the diagrams in Lemma 52 and Lemma 68 :

$$\begin{array}{ccc} L^* & \xrightarrow{\phi_{L'/L}} & H/H^c \\ \Big\downarrow{\scriptstyle Nm_{L/K}} & & \Big\downarrow{\scriptstyle incl.} \\ K^* & \xrightarrow{\phi_{L'/K}} & G/G^c \\ \Big\downarrow{\scriptstyle id} & & \Big\downarrow{\scriptstyle proj.} \\ K^* & \xrightarrow{\phi_{E/K}} & G/G^cH \end{array} \tag{3.48}$$

Note that the inclusion map $H/H^c \to G/G^c$ is induced by the inclusion map $H \to G$ (since $H \cap G^c = H^c$) and is given by $hH^c \mapsto hG^c$ and the projection map $G/G^c \to G/G^cH$ is given by $gG^c \mapsto gG^cH$.

Since $a \in Nm(E^*)$, so $\phi_{E/K}(a) = 1$. By the commutativity of the lower square, we get $\phi_{L'/K}(a) \mapsto 1$ under the projection map. We want to show that $\phi_{L/K}(a)$ is in the image of the inclusion map. It suffices to show that whenever an element of G/G^c maps to 1 under the projection map, then it is in the image of the inclusion map.

Let $gG^c \mapsto 1$ under the projection map. Then $g \in G^cH$ and so $g = g_1h$ for some $g_1 \in G^c$ and some $h \in H$. Thus

$$gG^c = g_1hG^c = hg_2G^c = hG^c = incl.(hH^c)$$

and so we are done. Note that we have used that $g_1h = hg_2$ for some $g_2 \in G^c$ since G^c is a normal subgroup of G. Hence $\phi_{L'/K}(a)$ is in the image of inclusion map, say $\phi_{L/K}(a) = incl.(hH^c)$. Since $\phi_{L'/L}$ is surjective, so $hH^c = \phi(L'/L)(b)$ for some $b \in L^*$). Thus $\phi_{L/K}(a) = \phi(L'/L)(incl.(b))$. The commutativity of the upper square then implies that

$$\phi_{L'/K}(a) = \phi_{L'/K}(Nm_{L/K}(b))$$

Thus

$$\frac{a}{Nm_{L/K}(b)} \in Ker(\phi_{L'/K}) = Nm_{L'/K}(L'^*)$$

and so

$$\frac{a}{Nm_{L/K}(b)} = Nm_{L'/K}(c)$$

for some $c \in L^*$. Again, transitivity of norms show that $Nm_{L'/K}(c) = Nm_{L/K}(Nm_{L'/L}(c))$ and thus

$$a = Nm_{L/K}(b)\, Nm_{L'/K}(c) = Nm_{L/K}(b)\ (Nm_{L/K}(Nm_{L'/L}(c))) = Nm_{L/K}(b\, Nm_{L'/L}(c))$$

Hence $a \in Nm_{L/K}(L^*)$ and we are done. □

3.8 The Hilbert Symbol

In order to prove the Existence Theorem, we need a result from the theory of Hilbert Symbol.

Theorem 71. *Let K be a local field containing a primitive n^{th} root of 1. Any element of K^* that is a norm from every cyclic extension of K of degree dividing n is an n^{th} power.*

Proof. We will require the following standard result in the theory of Hilbert Symbols.

Theorem 72. *The Hilbert Symbol has the following properties :*

(a). It is bi-multiplicative, i.e.

$$(aa', b) = (a, b)(a', b)$$
$$(a, bb') = (a, b)(a, b')$$

(b). It is skew symmetric, i.e.

$$(b, a) = (a, b)^{-1}$$

(c). It is non-degenerate, i.e.

$$(a, b) = 1 \ \text{ for all } b \in K^*/K^{*n} \quad \Longrightarrow \quad a \in K^{*n}$$
$$(a, b) = 1 \ \text{ for all } a \in K^*/K^{*n} \quad \Longrightarrow \quad b \in K^{*n}$$

(d). $(a, b) = 1$ if and only if b is a norm from $K[a^{1/n}]$.

Proof. See Theorem 4.4, page 112, [1]. □

Now we prove Theorem 71 with the help of Theorem 72. Let a be an element of K^* which is a norm from every cyclic extension of degree dividing n. By part (d) of Theorem 72, it follows that $(a, b) = 1$ for all $a \in K^*$ which means that $b \in K^{*n}$ by part (c) of Theorem 72 and thus b is an n^{th} power. □

3.9 The Existence Theorem

Let K be a local field.

Definition 34. *A subgroup N of K^* is known as a norm group if there is a finite abelian extension L/K such that $Nm_{L/K}(L^*) = N$*

If N is a norm subgroup, then $K^*/N \cong Gal(L/K)$, and so N is of finite index in K^*.

Lemma 54. *If L and L' are abelian extensions of K, then*

$$L \subset L' \;\Leftrightarrow\; Nm_{L/K}(L^*) \supset Nm_{L'/K}(L'^*)$$

and

$$Nm_{LL'/K}((LL')^*) = Nm_{L/K}(L^*) \cap Nm_{L'/K}(L'^*)$$

Proof. If $L \subset L'$, then transitivity of the norm map tells us that

$$Nm_{L/K}(L^*) \supset Nm_{L'/K}(L'^*)$$

Hence, in particular

$$Nm_{LL'/K}((LL')^*) \subset Nm_{L/K}(L^*)$$

and

$$Nm_{LL'/K}((LL')^*) \subset Nm_{L'/K}(L'^*)$$

since $L \subset LL'$ and $L' \subset LL'$. Therefore,

$$Nm_{LL'/K}((LL')^*) \subset Nm_{L/K}(L^*) \cap Nm_{L'/K}(L'^*)$$

Conversely, let $a \in Nm_{L/K}(L^*) \cap Nm_{L'/K}(L'^*)$, then

$$\phi_{L/K}(a) = 1 = \phi_{L'/K}(a)$$

But

$$\phi_{LL'/K}(a) \restriction_L = \phi_{L/K}(a) = 1$$

and

$$\phi_{LL'/K}(a) \restriction_L' = \phi_{L'/K}(a) = 1$$

by Lemma 68. Since the map

$$\sigma \mapsto (\sigma \restriction_L, \sigma \restriction_{L'}) \;\; : \;\; Gal(LL'/K) \to Gal(L/K) \times Gal(L'/K)$$

is injective, thus we get $\phi_{LL'/K}(a) = 1$ and so $a \in Nm_{LL'/K}((LL')^*)$. This completes the proof that

$$Nm_{LL'/K}((LL')^*) = Nm_{L/K}(L^*) \cap Nm_{L'/K}(L'^*)$$

Finally let $Nm_{L/K}(L^*) \supset Nm_{L'/K}(L'^*)$. Then by the above result, we have

$$Nm_{LL'/K}((LL')^*) = Nm_{L/K}(L^*) \cap Nm_{L'/K}(L'^*) = Nm_{L'/K}(L'^*)$$

But we also know by the local Artin map that

$$[K^* : Nm_{L'/K}(L'^*)] = [L' : K]$$

and

$$[K^* : Nm_{LL'/K}((LL')^*)] = [LL' : K]$$

Hence $[LL' : K] = [L' : K]$. Since $L' \subset LL'$, thus $L' = LL'$ which means $L \subset L'$ and so we are done. ☐

Lemma 55. *Every subgroup of K^* containing a norm group is itself a norm group.*

Proof. Let N be a norm group i.e. $N = Nm_{L/K}(L^*)$ for some abelian extension L/K and let $I \supset N$. Then $\phi_{L/K}(I)$ is a subgroup of $Gal(L/K)$ and let M be its fixed field. Thus $Gal(L/M) = \phi_{L/K}(I)$ by Galois Theory and $\phi_{L/K}$ maps I onto $Gal(L/M)$. Consider the commutative diagram :

$$\begin{array}{ccc} K^* & \xrightarrow{\phi_{L/K}} & Gal(L/K) \\ \Big\downarrow{\scriptstyle id} & & \Big\downarrow{\scriptstyle \pi} \\ K^* & \xrightarrow{\phi_{M/K}} & Gal(M/K) \end{array} \tag{3.49}$$

The kernel of $\phi_{M/K}$ is $Nm_{M/K}(M^*)$. On the other hand, the kernel of

$$K^* \to Gal(L/K) \to Gal(M/K)$$

is given as

$$\phi_{L/K}^{-1}(Gal(L/M)) = \phi_{L/K}^{-1}(\phi_{L/K}(I)) = I$$

To see the last equality, let $x \in \phi_{L/K}^{-1}(\phi_{L/K}(I))$, so $\phi_{L/K}(x) = \phi_{L/K}(i)$ for some $i \in I$. Thus $\frac{x}{i} \in Ker(\phi_{L/K}) = Nm_{L/K}(L^*) = N \subset I$ and so $x \in I$ and we are done. □

Lemma 56. *Let L be a field extension of K. Then $Nm_{L/K}(L^*)$ is an open subgroup of finite index in K^*.*

Proof. It suffices to show that $Nm_{L/K}(U_L)$ is an open subgroup of K^* since we know that if a subgroup of a topological group contains an open subgroup, then it is itself open (because it is a union of open cosets). The group U_L is compact. Since the norm map is continuous, $Nm_{L/K}(U_L)$ is a compact subset of K^*. In particular, $Nm_{L/K}(U_L)$ is a closed subset of K^*. We know that

$$Nm_{L/K}(U_L) \subset Nm_{L/K}(L^*) \cap U_K$$

Let $x \in Nm_{L/K}(L^*) \cap U_K$. Then $x = Nm_{L/K}(y)$ for some $y \in L^*$ and $x \in U_K$ i.e. $|x| = 1$. Since $|x| = |y|^n$, so $|y| = 1$ as well i.e. $y \in U_L$ and so $x \in Nm(U_L)$. Therefore we have shown

$$Nm_{L/K}(L^*) \cap U_K \subset Nm_{L/K}(U_L)$$

Combining these relations together, we get

$$Nm_{L/K}(U_L) = Nm_{L/K}(L^*) \cap U_K$$

Thus we get an injective map

$$i : U_K/Nm_{L/K}(U_L) \to K^*/Nm_{L/K}(L^*)$$

which shows that $Nm_{L/K}(U_L)$ has finite index in U_K. Since $Nm_{L/K}(U_L)$ is closed in K^*, so it is closed in U_K as well. Therefore, $Nm_{L/K}(U_L)$ is a closed subgroup of finite index in U_K. Since the complement of $Nm_{L/K}(U_L)$ (w.r.t. U_K) is given by union of finitely many cosets, each of which is closed, so $Nm_{L/K}(U_L)$ is open in U_K. Since

$$U_K = \left\{x \in K^* :\ |x| < \frac{1}{|\pi_K|}\right\} \cap \{x \in K^* :\ |x| > |\pi_K|\}$$

so U_K is open in K^* and thus $Nm_{L/K}(U_L)$ is open in K^*. □

We also need to recall a basic result in topology.

Recall that a collection A of subsets of a set X is said to have the finite intersection property (FIP) if the intersection over any finite subcollection of A is nonempty.

Lemma 57. *If X is a compact topological, then a collection of closed sets of X having the finite intersection property has non-empty intersection.*

Theorem 73. *(Existence Theorem) Every open subgroup of finite index in K^* is a norm group.*

Proof. We will need a few helping lemmas.

Lemma 58. *For any finite L/K, the norm map $L^* \to K^*$ has closed image and compact kernel.*

Proof. Since the image $Nm(L^*)$ has finite index (i.e. $K^*/Nm(L^*)$ is finite), so it is open by Lemma 56 and thus closed. Since a singleton set is closed in every metric space and the norm map is continuous, so kernel of the norm map is closed. Moreover, we have

$$ord_L(Nm(a)) = [L : K]\, ord_L(a)$$

since all conjugates have the same order. Thus if $a \in Ker(Nm)$, then $ord_L(a) = 0$ and so $a \in U_L$. Hence we have shown that $Ker(Nm)$ is a closed subset of U_L. Since U_L is compact, so $Ker(Nm)$ is also compact. □

Let $D_K = \cap_L Nm_{L/K}(L^*)$ where L runs over the finite extensions of K. Note that by Theorem 70 (Norm Limitation Theorem), we get $D_K = \cap_L Nm_{L/K}(L^*)$ where L runs over the finite abelian extensions of K.

Lemma 59. *For each finite extension K'/K, $Nm_{K'/K} D_{K'} = D_K$.*

Proof. Let $a \in D_{K'}$, and let L be a finite extension of K'. Then $a \in Nm_{L/K'}(L^*)$, say $a = Nm_{L/K'}(b)$ for some $b \in L^*$. Then $Nm_{K'/K}(a) = Nm_{K'/K}(Nm_{L/K'}(b)) = Nm_{L/K}(b)$ by the transitivity of norms. Thus we have shown that $a \in Nm_{L/K}(L^*)$ for any finite extension L/K'. Now let L be any finite extension of K. Then by what we have shown $a \in Nm_{LK'/K}((LK')^*)$ but by Lemma 54, we know that $Nm_{LK'/K}((LK')^*) \subset Nm_{L/K}(L^*)$ and so $a \in Nm_{L/K}(L^*)$ for any finite extension L/K. Hence we have shown that

$$Nm_{K'/K} D_{K'} \subset D_K$$

Conversely let $a \in D_K$, and consider the sets

$$Nm_{L/K'}(L^*) \cap Nm^{-1}_{K'/K}(a), \quad L/K' finite$$

Firstly we will show that all these sets are nonempty. Since $a \in D_K$, so or any finite extension L/K', $a = Nm_{L/K}(b)$ for some $b \in L^*$. Thus $a = Nm_{K'/K}(Nm_{L/K'}(b))$ and so $Nm_{L/K'}(b) \in Nm^{-1}_{K'/K}(a)$. Since we have $Nm_{L/K'}(b) \in Nm_{L/K'}(L^*)$, so $Nm_{L/K'}(b) \in Nm_{L/K'}(L^*) \cap Nm^{-1}_{K'/K}(a)$ and thus we are done.

Let $[K'/K] = n$. Note that $Nm^{-1}_{K'/K}(a)$ is a closed subset of K'^* since the norm map is continuous. Since $Nm^{-1}_{K'/K}(a)$ is nonempty, we can choose an x_0 in $Nm^{-1}_{K'/K}(a)$. Observe that

$$Nm^{-1}_{K'/K}(a) = \{x \in (K')^* : Nm_{K'/K}(x) = Nm_{K'/K}(x_0)\} \subset \{x \in (K')^* : |x| = |x_0|\} = x_0 U_{K'}$$

which is compact and so $Nm_{L/K'}(L^*) \cap Nm^{-1}_{K'/K}(a)$ is contained in a compact set for all finite extensions L/K. We know that the norm group $Nm_{L/K'}(L^*)$ is closed in K'^*. $Nm^{-1}_{K'/K}(a)$ is also a closed subset of K'^* since the norm map is continuous. Thus, $Nm_{L/K'}(L^*) \cap Nm^{-1}_{K'/K}(a)$ is also a closed subset of K'^* which is contained in the compact set $x_0 U_{K'}$. Moreover for any two finite extensions L_1, L_2 of K, we know by Lemma 54 that $Nm_{LL'/K}((LL')^*) = Nm_{L/K}(L^*) \cap Nm_{L'/K}(L'^*)$ and thus the intersection of any two sets of the collection $Nm_{L/K'}(L^*) \cap Nm^{-1}_{K'/K}(a)$ is another set in the collection. This shows that this collection has the finite intersection property. Hence by Lemma 57, the collection

$$Nm_{L/K'}(L^*) \cap Nm^{-1}_{K'/K}(a), \quad L/K' finite$$

has nonempty intersection. Let b be an element in this intersection. Then b lies in $\cap_L Nm_{L/K'}(L^*) = D_{K'}$ and has norm a since it is also in $Nm^{-1}_{K'/K}(a)$. Thus $a = Nm_{K'/K}(b) \in Nm_{K'/K} D_{K'}$ and we are done. □

Lemma 60. *The group D_K is divisible.*

Proof. Let $n > 1$ be an integer. We have to show that $D_K^n = D_K$ (since D_K is a multiplicative group). Let $a \in D_K$. For each finite extension L of K containing a primitive n^{th} root of 1, define the set

$$E(L) = \{b \in K^* : b^n = a,\ b \in Nm_{L/K}(L^*)\}$$

Firstly we will show that $E(L)$ is nonempty for all L. We have $a \in D_K$ and so by Lemma 59, we have $a = Nm_{L/K}(a')$ for some $a' \in D_L$. But $a' \in D_L$ means that a' is a norm from all finite extensions of L and hence in particular a' is a norm from all cyclic extensions of order dividing n. Thus by Theorem 71, a' is an n^{th} power i.e. $a' \in (L^*)^n$ which means $a' = c^n$ for some $c \in L^*$. Therefore,

$$a = Nm_{L/K}(a') = Nm_{L/K}(c^n) = (Nm_{L/K}(c))^n$$

Thus $Nm_{L/K}(c) \in E(L)$ and so $E(L)$ is nonempty. For each finite L/K,

$$E(L) \subset \{b \in K^* : b^n = a\}$$

Note that $\{b \in K^* : b^n = a\}$ is a finite subset of K^* and thus compact. Each $E(L)$ is a finite subset of K^* and thus closed (since it is a union of singletons) and so each $E(L)$ is a non-empty closed subset of a compact set. Moreover, for any finite extensions L, L' of K containing a primitive n^{th} root of 1, we have $Nm((LL')^*) \subset Nm(L^*) \cap Nm(L'^*)$ and so

$$E(LL') \subset E(L) \cap E(L')$$

This shows that the collection $E(L)$ where L is a finite extension of K containing a primitive n^{th} root of 1 satisfies the finite intersection property. Hence by Lemma 57, this collection has a nonempty intersection. Let b_0 be an element in the intersection. Then $b_0^n = a$ and $b_0 \in Nm_{L/K}(L^*)$ for every finite extension L of K containing a primitive n^{th} root of 1. Now let L' be any finite extension of K. Then consider the smallest extension L'' of L' containing a primitive n^{th} root of 1. Clearly L'' is finite over L' and hence also over K. Then we have $b_0 \in Nm_{L''/K}((L'')^*)$. But by Lemma 54, we get

$$Nm_{L''/K}((L'')^*) \subset Nm_{L'/K}((L')^*)$$

and so $b_0 \in Nm_{L'/K}((L')^*)$ for any finite extension L'/K. Thus $b_0 \in D_K$. Since $a = b_0^n$, so $a \in D_K^n$ and we are done. □

Lemma 61. *Every subgroup I of finite index in K^* that contains U_K is a norm subgroup.*

Proof. Consider the map

$$ord_K : K^* \to \mathbb{Z}$$

We know that ord_K is a homomorphism, thus $ord_K(I)$ is a subgroup of $\mathbb{Z}$, so $ord_K(I) = n\mathbb{Z}$ for some $n \in \mathbb{N}$. Thus $ord_K^{-1}(n\mathbb{Z}) = ord_K^{-1}(ord_K(I)) \supset I$. Now let $x \in ord_K^{-1}(n\mathbb{Z})$ and so $ord_K(x) \in n\mathbb{Z}$ which implies $ord_K(x) = ord_K(i)$ for some $i \in I$. Thus $ord_K(x/i) = 0$ which means $x/i \in U_K$. Since $I \supset U_K$, so $x/i \in I$ and thus $x \in I$.

Thus we have shown that if I is a subgroup of K^* that contains U_K, then $I = ord_K^{-1}(n\mathbb{Z})$ for some $n \in \mathbb{N}$ where n is determined by the equation $ord_K(I) = n\mathbb{Z}$.

Let K_n be the unramified extension of degree n over K. Then $Nm_{K_n/K}(K_n^*)$ is a subgroup of K^* which contains U_K by Theorem 60 and $ord_K(Nm_{K_n/K}(K_n^*)) = n\mathbb{Z}$ because $ord_K(Nm_{K_n/K}(x)) = [K_n : K]\, ord_{K_n}(x) = n\, ord_{K_n}(x)$ and the map $ord_{K_n} : K_n^* \to \mathbb{Z}$ is surjective. Thus by the remark in the above paragraph, we get $I = Nm_{K_n/K}(K_n^*)$ and so we are done. □

Lemma 62. *Let $\{U_i : i \in I\}$ be a family of finite sets such that the following conditions are satisfied*

1. $\bigcap_{i \in I} U_i = \{1\}$
2. *For each $i, j \in I$, there exists some $k \in I$ such that $U_i \cap U_j = U_k$.*

Then there is some $i \in I$ such that $U_i = \{1\}$.

Proof. Let $U_1 = \{1, x_1, x_2, ..., x_{n_0}\}$ for some $n_0 \in \mathbb{N}$. By condition 1 in the hypothesis, there exists $i_1 \in I$ such that $x_1 \notin U_{i_1}$. Then by condition 2, there exists some $j_1 \in I$ such that $U_1 \cap U_{i_1} \supset U_{j_1}$. Then $U_{j_1} \subset \{1, x_2, ..., x_{n_0}\}$. We can iterate this process to get some $j_{n_0} \in I$ such that $U_{j_{n_0}} = \{1\}$. □

We now complete the proof of Theorem 73. Let U be the set of norm groups in K^*, so that $D_K = \bigcap_{N \in U} N$. Let I be a subgroup of K^* of finite index. Then $I \supset (K^*)^n$ where $n = [K^* : I]$. Since $D_K \subset K^*$, so $I \supset D_K^n$. Moreover, since D_K is divisible, so $I \supset D_K$. Therefore,

$$\bigcap_{N \in U} (N \cap U_K) \subset D_K \subset I$$

By Lemma 58, we know that N is closed in K^*. Therefore $N \cap U_K$ is closed subgroup of U_K which is compact. Hence each group $N \cap U_K$ is compact. Consider the projection map $\pi : K^* \to K^*/I$. Take the family

$$\{\pi(N \cap U_K) : N \in U\}$$

Clearly this is a family of finite sets (since K^*/I is finite). The condition

$$\bigcap_{N \in U} (N \cap U_K) \subset I$$

shows that

$$\pi\left(\bigcap_{N \in U} (N \cap U_K)\right) = \{1\}$$

which precisely means that the intersection of all the sets of this family is $\{1\}$. Moreover since intersection of two norm groups is a norm group, so the hypothesis of Lemma 62 is satisfied and we get $\pi(N \cap U_K) = \{1\}$ for some $N \in U$. Thus we have shown that there is a norm group N such that $N \cap U_K \subset I$. We want to strengthen this condition to say

$$N \cap (U_K(N \cap I)) \subset I$$

Let $y \in N \cap (U_K(N \cap I))$. Thus $y = y_1 y_2$ where $y_1 \in U_K$, $y_2 \in N \cap I$. Moreover $y \in N$. Since $y, y_2 \in N$, so $y_1 \in N$. Thus $y_1 \in N \cap U_K \subset I$. Thus $y_1 \in I$. Therefore, $y = y_1 y_2 \in I$ and we are done. Hence $N \cap (U_K(N \cap I)) \subset I$. Since N is a norm group, so K^*/N is finite by the local reciprocity law. Moreover, I is given to be a subgroup of finite index in K^* so K^*/I is also finite. Now consider the natural injection

$$K^*/(N \cap I) \to K^*/N \times K^*/I$$

given by $x + (N \cap I) \mapsto (x + N, x + I)$. Thus $K^*/(N \cap I)$ is also finite. Furthermore, consider the natural surjection

$$K^*/(N \cap I) \to K^*/(U_K(N \cap I))$$

given by $x + N \cap I \mapsto x + U_K(N \cap I)$. Thus $K^*/(U_K(N \cap I))$ is also finite which means that $U_K(N \cap I)$ is a subgroup of finite index in K^* that contains U_K and so is a norm group by Lemma 61. Now $N \cap U_K(N \cap I)$ being an intersection of two norm groups is also a norm group. Therefore I contains a norm group and so is itself a norm group by Lemma 55. □

Theorem 74. *Let I be a subgroup of K^*, then the following conditions are equivalent :*

(1). *I is a norm group.*
(2). *I is an open subgroup of finite index.*
(3). *I is a closed subgroup of finite index.*
(4). *I is of finite index in K^*.*

Proof. We have (1) implies (2) by Lemma 56. (2) is clearly equivalent to (3). Moreover, by Theorem 73, we have (2) implies (1). Hence we only need to show that (3) implies (4). We know that if I is of finite index m in K^*, then $I \supset K^{*m}$, but since K^{*m} is open (see Corollary 3.6, page 81, [2]), so I is open in K^{*m} and we are done. □

Corollary 9. $D_K = \{1\}$.

Proof. Choose a prime element π of K. Let $V_{m,n} = U_K^{(m)} \times \pi^{n\mathbb{Z}}$. Then $V_{m,n}$ is a subgroup of K^* of finite index which means that it is also open by Theorem 74. But by Theorem 73, $V_{m,n}$ is also a norm group. Thus $D_K \subset V_{m,n}$ for all m and n. Since $\cap_{m,n} V_{m,n} = \{1\}$, so $D_K = \{1\}$. □

Remark 25. *Theorem* 73 *is known as the Existence Theorem because its crucial assertion is that given an open subgroup I of finite index in K^*, there exists an abelian extension L/K whose norm group $Nm_{L/K}(L^*) = I$. This field L is uniquely determined (because of Lemma* 54*) and is called the class field associated with I.*

The Existence Theorem provides a topological characterization of norm groups, but there is also an arithmetic description of these groups :

Remark 26. *The norm groups of K^* are precisely the groups containing*

$$U_K^{(n)} \times (\pi)^f$$

for some $n \geq 0$ and some $f \geq 1$. Here $U_K^0 = U_K$, π is a prime element of K, and $(\pi)^f$ is the subgroup generated by π^f. (see Theorem (6.4), Page 97, [2] for proof.)

Remark 27. *$K^*/Nm_{L/K}(L^*)$ form an inverse system as L runs through the finite abelian extensions of K via the natural transition maps*

$$\phi_{i,j} : K^*/Nm_{L_1/K}(L_1)^* \to K^*/Nm_{L_2/K}(L_2)^*$$

for any $L_2 \subset L_1$. Also, $Gal(L/K)$ form an inverse system as L runs through the finite abelian extensions of K, ordered by restriction. Moreover, we have a family of homomorphisms (infact isomorphisms)

$$\phi_{L/K} : K^*/Nm_{L/K}(L^*) \to Gal(L/K)$$

between these inverse systems such that for any $L_2 \subset L_1$, the following diagram commutes (by Theorem 68) :

$$\begin{array}{ccc} K^*/Nm_{L_1/K}(L_1^*) & \xrightarrow{\phi_{L_1/K}} & Gal(L_1/K) \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ K^*/Nm_{L_2/K}(L_2^*) & \xrightarrow{\phi_{L_2/K}} & Gal(L_2/K) \end{array} \tag{3.50}$$

Therefore we get the map

$$\widehat{\phi}_K : \varprojlim_{N \in U} K^*/Nm_{L/K}(L^*) \to \varprojlim_{N \in U} Gal(L/K)$$

Since the inverse limit functor is left exact (see Proposition 10.3, page 164, [11]), the map $\widehat{\phi}_K$ is injective. Note that

$$\varprojlim_{N \in U} Gal(L/K) \cong Gal(K^{ab}/K)$$

Since intersection of any two norm groups is a norm group, so they become a local base for a topology i.e. there is a topology for which the norm groups form a fundamental system of neighborhoods of 1. This topology on K^* is called the norm topology. Let $\widehat{K^*}$ denote the completion of K^* with respect to this topology. Then we know that

$$\widehat{K^*} \cong \varprojlim_{N \in U} K^*/Nm_{L/K}(L^*)$$

(see page 103, [12]). Hence we get an injective map

$$\widehat{\phi}_K : \widehat{K^*} \to Gal(K^{ab}/K)$$

But since the maps $\phi_{L/K}$ are isomorphisms, so we can work with $\phi_{L/K}^{-1}$ instead of $\phi_{L/K}$ and repeat the above procedure to get the inverse of the map $\widehat{\phi}_K$.

Therefore, $\widehat{\phi}_K$ is infact an isomorphism of topological groups.

Remark 28. *Since intersection of the norm groups is trivial by Corollary 9, so K^* embeds into $\widehat{K^*}$ i.e. the natural map $K^* \to \widehat{K^*}$ is injective. Moreover, the image of K^* under this map is dense.*

Bibliography

[1] J.S. Milne, *Class Field Theory*, http://www.jmilne.org/math, 2013.

[2] J. Neukirch, *Class Field Theory*, -The Bonn Lectures- Edited by Alexander Schmidt, Springer, 2013.

[3] J.S. Milne, *Algebraic Number Theory*, http://www.jmilne.org/math, 2017.

[4] J. Neukirch, *Algebraic Number Theory*, Springer, 2013.

[5] J.S. Milne, *Field Theory*, http://www.jmilne.org/math, 2013.

[6] R.Sharifi *Group Cohomology*, http://www.math.ucla.edu/ sharifi/groupcoh.pdf

[7] D.S.Dummit and Richard M.Foote, *Abstract Algebra*, *Wiley Student Edition*, 2004

[8] J.P. Serre, Local Fields, Springer, 1979

[9] Dr. T. Dokchitser, *Local Fields*, www.pancratz.org/notes/Local.pdf, 2007

[10] D. Eisenbud, *Commutative algebra with a view towards algebraic geometry*, Springer,1999

[11] S. Lang, *Algebra*, *Revised Third Edition*, Springer,2002

[12] M.F. Atiyah and I.G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, 1969