Class Field Theory

A Thesis

submitted to
Indian Institute of Science Education and Research Pune
in partial fulfillment of the requirements for the
BS-MS Dual Degree Programme

by

Siddharth Ramakrishnan

Indian Institute of Science Education and Research Pune
Dr. Homi Bhabha Road,
Pashan, Pune 411008, INDIA.

April, 2020

Supervisor: Dr. Dipendra Prasad
© Siddharth Ramakrishnan 2020

All rights reserved

Certificate

This is to certify that this dissertation entitled Class Field Theory towards the partial fulfilment of the BS-MS dual degree programme at the Indian Institute of Science Education and Research, Pune represents study/work carried out by Siddharth Ramakrishnan at Indian Institute of Science Education and Research under the supervision of Dr. Dipendra Prasad, Professor, Department of Mathematics , during the academic year 2019-2020.

Dr. Dipendra Prasad

Committee:

Dr. Dipendra Prasad

Dr. Chandrasheel Bhagwat 

This thesis is dedicated to everyone who believed in me, even at times when I didn't believe in myself

Declaration

I hereby declare that the matter embodied in the report entitled Class Field Theory are the results of the work carried out by me at the Department of Mathematics, Indian Institute of Technology, Bombay, under the supervision of Dr. Dipendra Prasad and the same has not been submitted elsewhere for any other degree.

Siddharth Ramakrishnan

Acknowledgments

First and foremost, I would like to thank my advisor, Prof. Dipendra Prasad, for his constant guidance and encouragement, and for helping me to get better as both a mathematics student and a person. I would also like to thank Dr. Chandrasheel Bhagwat, who always provided me with solutions and insights, in times of struggle. Also, no amount of words would be enough for my beloved teachers, who throughout these 5 years have constantly guided me towards the path of academia. Many thanks go to my family and friends for their unending support.

Abstract

The goal of the project is to study Class Field Theory. Class Field Theory studies the abelian extensions of local fields and global fields. There are different approaches for this and we focus on the cohomological approach envisaged by Hochschild and Nakayama. We give an exposition on how to prove certain theorems in Elementary Number Theory, using Class Field Theory. Also, we discuss the solution to a long-standing problem.

Contents

Introduction

Let K be an algebraic number field, and let O_K denote the ring of integers. Let $\rho \subset O_K$ be a prime ideal. Let L be a finite extension of K with degree n, and O_L be the corresponding ring of integers

$$\rho O_L = \prod_i q_i^{e_i}, \text{ where } q_i \text{ are prime ideals in } O_L.$$

Now, we have $n = \sum_i e_i f_i$, where $f_i = [O_L/q_i : O_K/\rho]$.
When L/K is Galois, e_is are independent of q_i and just depend on ρ. We say $e_i > 1$, then ρ is *ramified*, *unramified* other-wise. We say ρ is *totally split* if $e_i = f_i = 1 \ \forall$ i.
Frobenius proved that given any field K, the extensions of K, can be determined the set of primes totally split in K.
The aim of class field theory is to study the abelian extensions of K, based on arithmetic of K. Now let K=$\mathbb{Q}$. The quadratic extensions of $\mathbb{Q}$, can be determined using Gauss' Quadratic Reciprocity Law. Now consider the ideal group of K, $\mathbf{I}_K$. Now, we know the $\mathbf{I}_K/K^*$, the ideal class group of K. Now let $\mathcal{M}$, be a modulus, a product of prime ideals of K, and certain embeddings onto $\mathbb{R}$. $I^{S(\mathcal{M})}$, denote the ideal generated by primes not dividing $\mathcal{M}$. Now let $K_{\mathcal{M}}$ denote the set of $a \in K^*$ such that $\text{ord}_\rho(a-1) \geq ord_\rho(\mathcal{M})$.
Now define $C_{\mathcal{M}}$=$I^{S(\mathcal{M})}$/ $K_{\mathcal{M}}$, similar to the ideal class group. Now fix a subgroup H of $C_{\mathcal{M}}$, and consider the group $\bar{H} \subset I^{S(\mathcal{M})}$, containing $K_{\mathcal{M}}$. Let L be an abelian extension of K, and we call L a class field for $\mathcal{M}$, if prime ideals not dividing $\mathcal{M}$ that split in L, are the ones in $\bar{H}$.

Theorem 0.0.1. *For any finite abelian extension L of K, there exists a unique H a subgroup of $C_{\mathcal{M}}$, such that L is the class field for H. Also $Gal(L/K) \cong C_{\mathcal{M}}/H$.*

Takagi proved the theorem, and Artin gave an explicit map between the two groups,as

follows.

Theorem 0.0.2. *(Artin) Let L/K be a finite number field extension, which is Galois with Galois group G, which is abelian and S the set of prime ideals which are ramified in L. Now there is a homomomorphism $\Phi_{L/K} : I^S \to G$, such that Φ factors through $C_{\mathcal{M}}$. The map is called Artin map or the reciprocity map.*

The above theorem is one of the central theorems in Class Field Theory. This extended Class Field Theory for infinite extensions. By 1930, these theorems were proved using the technique of L-functions and analogous results for local fields were easily determined. But these was deemed unsatisfactory in the following aspects:
(1) The results are mainly algebraic, so the proofs also should be.
(2) Since local fields are simpler than global fields, proofs should be given first for local fields and then global fields not the other way around.
Chevalley proved these in 1930s, using Brauer groups. In 1950s Hoschild and Nakayama used cohomology to give an elegant reformulation of Class Field Theory.
This is the approach we follow in the project. We develop the machinery of Group Cohomology in Chapter 2. We learn Local Class Field Theory in Chapter 3 using these methods and get an explicit description using Lubin-Tate formal group laws. We use it to give a proof of Global Class Field Theory in Chapter 4. We give an exposition on how one can derive the reciprocity laws, remarked above, from Class Field Theory in Chapter 5. Also we discuss the solution to a longstanding problem in Class Field Theory in Chapter 6 . The exposition is mostly self-contained and assumes a basic understanding of algebraic number theory, roughly the first two chapters of [4]. The approach is following [1].

Chapter 1

Preliminaries

1.1 Topological Arithmetic

Definition 1.1.1. *Let K, be a field. A* valuation *on K is a map* $||: K \to \mathbb{R}_+$ *such that*

1. $| a |= 0 \iff a=0$.
2. $| a.b |=| a | . | b |$.
3. $| 1 + a | \leq C$, *a constant , whenever* $| a | \leq 1$

Definition 1.1.2. *Every field with a valuation has a metric topology, by defining* $d(a, b) =| a - b |$. *Two valuations are said to be equivalent, if the defined the same topology.*

Definition 1.1.3. $||$ *is a* non-archimedean valuation (discrete valuation)*, when* $C = 1$*, in 1.1.1(3) and* archimedean valuation*, when* $C = 2$.

It can be seen, that every non-archimedean valuation, is equivalent to a surjective homomorphism, v:$K^* \to \mathbb{Z}$.

$O_K : \{x \in K : v(x) \geq 0\}$ is called the valuation ring. Clearly O_K is a discrete valuation ring, and the maximal ideal is generated by π such that v(π)=1. We call π, a uniformizer of K. Now O_K/π is a field and we call it the residue class field of K.

Definition 1.1.4. *K is a local field, if K is a discrete valuation field with a finite residue class field. K is a global field if K is a finite separable extension of* $\mathbb{F}((t))$*, where* $\mathbb{F}$ *is a finite field.*

Theorem 1.1.1. (*Ostrowski*) *Any local field is isomorphic to a finite extension of* $\mathbb{Q}_p$ *or* $\mathbb{F}_p((t))$

Let L/K be a local field extension of degree n. Let π_L, π_K be the uniformizers of L and K. Let v_K be the valuation corresponding to K.

Definition 1.1.5. *1. L/K is called unramified if* $e = 1$.

2. L/K is called ramified if $e \geq 2$.

3. L/K is called totally ramified if $e = n$.

Definition 1.1.6. *Let K be a global field, and* $||_v$ *be a valuation. Now let* K_v*, denote the completion of K wrt this valuation.* O_v *and* U_v *denote the ring of integers and the unit group for the same.* Adele Ring A_K *of K, is the restricted direct product of* K_v *w.r.t* O_v*.* Idele Group I_K *of K, is the restricted direct product of* K_v^* *w.r.t* U_v*.*

Proposition 1.1.2. *Let K be a local field with residue class field with the residue class field k, and fix an algebraic closure of* $\bar{K}$*, with residue class field* $\bar{k}$*. Now for any finite, separable extension of l over k,* $\exists$ *a unique unramified extension of K, L contained in* $\bar{K}$*, with residue class field l.*

1.2 Kummer Theory

Let K be a field such that x^m -1 is separable over K. Now splitting field of this equation L, over K is a Galois extension. When K= $\mathbb{Q}$, the Galois group= $(\mathbb{Z}/m\mathbb{Z})^*$.

Proposition 1.2.1. *p is unramified in* $L/\mathbb{Q}$*, if* $p \equiv 1 (mod\ m)$*. p is ramified,* $\iff p \mid m$.

Lemma 1.2.2. *L/K has a cyclic Galois group* $\iff$ *L is the splitting field of* x^m *- b, for some* $b \in K$.

Proposition 1.2.3. *Let L/K be a splitting field of* x^m *- b, for some* $b \in K$.
p is unramified in L/K if p doesn't divide m and b.

Chapter 2

Group Cohomology

As denoted earlier, we try to take the cohomological approach to class field theory, and this chapter details some of the major concepts and theorems we are going to use.

2.1 G-modules

Let G be a group, $\mathbb{Z}$G denote the corresponding integral group ring and let,
$I_G = \{\Sigma\ a_g g\colon\ \Sigma\ a_g = 0\}$

Definition 2.1.1. *A* G-module *is an abelian group A with $\mathbb{Z}G$ action on A.*

Let R be a ring, D be a fixed R-module. We know that **Hom**(__, D) is a contravariant, left exact functor. Hence we can construct right derived functors of this functor, the **Ext** functor.

Similarly there is N $\otimes$__ is a right exact, covariant functor. Similar to the construction above, we can construct left derived functor of this functor, **Tor** functor.(For a general discussion of Ext and Tor functor, see [3])

Definition 2.1.2. *Let A be a G-module. A^G denote all elements of A fixed by G.*

Proposition 2.1.1. *Consider* $\mathbb{Z}$ *as a G-module with trivial G-action. Then,* $A^G = \boldsymbol{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A)$.

Proof. Any G-homomorphism from $\mathbb{Z}$ to A can be determined by it's value on 1.
Let a be the value of f taken at 1.
$f(g.1) = g.f(1)$
$f(1) = g.f(1)$
So, $\mathbf{Hom}_{\mathbb{Z}G}(\mathbb{Z},\mathrm{A})=A^G$ □

Definition 2.1.3. *1. nth Cohomology groups of G with coefficients in A is given by* $\boldsymbol{H}^n(G, A) = \boldsymbol{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, A)$

2. nth Homology groups of G with co-effecients in A is given by $\boldsymbol{H}_n(G, A) = \boldsymbol{Tor}^n_{\mathbb{Z}G}(\mathbb{Z}, A)$.

Theorem 2.1.2. *A short exact sequence*

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

leads to a long exact sequence,

$$....\mathbf{H}^{n-1}(G, C) \to \mathbf{H}^n(G, A) \to \mathbf{H}^n(G, B) \to \mathbf{H}^n(G, C) \to \mathbf{H}^{n+1}(G, A) \to \mathbf{H}^{n+1}(G, B).....$$

$$....\mathbf{H}^{n+1}(G, C) \to \mathbf{H}_n(G, A) \to \mathbf{H}_n(G, B) \to \mathbf{H}_n(G, C) \to \mathbf{H}_{n-1}(G, A) \to \mathbf{H}_{n-1}(G, B).....$$

Proof. Follows from the analogous long exact sequences for the Ext and Tor groups. □

Remark 2.1.1. *Since we have the long exact sequence, we can reduce a problem regarding the nth cohomology groups, to a problem regarding the lower level cohomology groups. This technique is called dimension-shifting.*

Definition 2.1.4. *Let X be an abelian group. A is co-induced, if* $A = \boldsymbol{Hom}_{\mathbb{Z}}(\mathbb{Z}G, X)$. *A is induced if* $A = \mathbb{Z}G \otimes X$.

Definition 2.1.5. *A is cohomologically(homologically) trivial if* $\boldsymbol{H}^n(H, A)(\boldsymbol{H}_n(H, A))=0$ $\forall\ n \geq 1$, *and for all subgroups H of G.*

Proposition 2.1.3. *Co-induced modules are cohomologically trivial, induced modules are homologically trivial.*

We give a procedure of constructing the group cohomology functors, and the procedure *mutatis mutandis* holds for the group homology functor also. We can choose once and for all a projective resolution for $\mathbb{Z}$ as G-modules and calculate the Cohomology groups,

Remark 2.1.2. *P_i=$\mathbb{Z}[G^{i+1}]$, a free $\mathbb{Z}$ module with basis $G\times G...\times G$ (i+1 factors) and define the G-action as $g.(g_0,g_1,....g_i)=(g.g_0,g.g_1,....g.g_i)$ and extend it linearly. Now $\boldsymbol{Hom}_{\mathbb{Z}G}(P_i,A)$ can be identified as set of all maps from $G^i \to A$, with the boundary maps as $(df)(g_0,g_1,....g_i)=g_0.f((g_1,g_2,....g_i))+\sum_{i=1}^{n}$ $(-1)^j f(g_0,g_1,\ g_jg_{j+1}....g_i)+(-1)^{j+1}f(g_0,g_1,..g_i)$*

Definition 2.1.6. *f:G$\to$A such that $f(gh) = g.f(h) + f(g)$ is called a 1 co-cycle. f: G$\to$A is a co-boundary if $\exists$ a such that f(g)=g.a-a.*

$$\boldsymbol{H}^1(G, A)=\frac{\{\ 1-cocylces\}}{\{\ 1-coboundaries\}}$$

Proposition 2.1.4. *$\boldsymbol{H}_1(G, \mathbb{Z}) = G^{ab}$,where G^{ab} denotes the abelianization of G.*

Definition 2.1.7. *$Ind_H^G(A)$ = $\boldsymbol{Hom}_{\mathbb{Z}H}(\mathbb{Z}G,A)$*

Lemma 2.1.5. (*Shapiro's lemma*) *Let H be a subgroup of G and A be a H-module.* $\boldsymbol{H}^n(G,Ind_H^G(A))\cong \boldsymbol{H}^n(H,A)$.

Let A be a G-module and A' be a G'-module. f:G' $\to$G. Now A can be given a G' module structure as g'.a=f(g').a Let ϕ:A$\to$A' be a group homomorphism. We say ϕ is a compatible if it's a G'-module homomorphism as remarked above.

Now once we have a compatible homomorphism, we can get a map from n co-chains of standard complex P' to standard complex P. So we get a map from f*:$\mathbf{H}^n(G, A) \to \mathbf{H}^n(G', A')$.

Definition 2.1.8. *If H is a subgroup of G, and A'=A, we get a* restriction *map,*

$$Res:\boldsymbol{H}^n(G,A)\to\boldsymbol{H}^n(H,A).$$

Now H is a normal subgroup, there is a inflation *map,*

$$Inf:\boldsymbol{H}^n(G/H,A^H)\to\boldsymbol{H}^n(G,A).$$

Proposition 2.1.6. (*Restriction-Inflation Sequence*) *Let G be a group, H be a normal subgroup, A be a G-module then we get the following exact sequence,*

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

Moreover, suppose that $\boldsymbol{H}^i(H,A)=0$ $1 \leq i \leq q-1$.

$$0 \to \boldsymbol{H}^q(G/H,A^H) \xrightarrow{Inf} \boldsymbol{H}^q(G,A) \xrightarrow{Res} \boldsymbol{H}^q(H,A)$$

Theorem 2.1.7. (*Hilbert 90*) *For a L/K be a Galois extension with Galois group G,* $\mathbf{H}^1(G,L^*)=0$.

Definition 2.1.9. (*Profinite Group*) *A topological group is* profinite group*, if it is compact and totally disconnected.*

Proposition 2.1.8. *For a profinite group G,* $G \cong \varprojlim G/M$*, where M varies over open, normal subgroups of G.*

Definition 2.1.10. *Let G be a profinite group. A G-module A is said to be* discrete module*, if the stabilizer of each element is an open subgroup of G.*

Proposition 2.1.9. *Let G be a profinite group, A be a discrete G-module.* $\boldsymbol{H}^q(G,A)$ *is defined as* $\varinjlim \boldsymbol{H}^q(G/U,A^U)$*, where* A^U *denote the elements in A, fixed by all elements in U.*

2.2 Tate Groups

It was seen that, when G is a finite group, the nth homology groups and cohomology groups are connected to each other in a natural way. Tate groups are generalised cohomology groups which make this connection clear.

Assume that G is a finite group and N=$\sum_{g\in G}$ g, and the following submodule of $\mathbb{Z}$G. Multiplication by N gives an endomorphism ϕ of A.

It's easy to see that $\mathbf{H}_0(G,A) \subset$ Kernel(ϕ) and Image(ϕ) $\subset \mathbf{H}^0(G,A)$.

Definition 2.2.1. *Define a map ϕ^* induced by ϕ from $\boldsymbol{H}_0(G,A) \to \boldsymbol{H}^0(G,A)$ Define the tate groups as below*

$$\hat{\mathbf{H}}^n(G,A) = \left\{ \begin{array}{ll} \boldsymbol{H}^n(G,A), & \text{for } n \geq 1 \\ \boldsymbol{Coker}(\phi^*) & \text{for } n = 0 \\ \boldsymbol{Ker}(\phi^*), & \text{for } n = -1 \\ \boldsymbol{H}_{-n-1}(G,A), & \text{for } n \leq -2 \end{array} \right\}$$

Remark 2.2.1. *Consider the projective resolution for $\mathbb{Z}$ we constructed earlier. Now put P_{-n}=$\boldsymbol{Hom}(P,\mathbb{Z})$. Now since by construction as our projective G-modules were free $\mathbb{Z}$ modules, the dual sequence*
$0 \to \mathbb{Z} \to P_{-1} \to P_{-2} \to$..... is exact.
We can splice together two sequences and get an exact sequence, a complete resolution of $\mathbb{Z}$,
$\ldots. \to P_1 \to P_0 \to P_{-1} \to P_{-2} \to$.....
Now apply the functor $\boldsymbol{Hom}_{\mathbb{Z}G}(\_\_, A)$ for a G-module A, to this complete resolution. qth Tate group is the qth cohomology group of this derived sequence. It is clear that
$\boldsymbol{Hom}(\boldsymbol{Hom}(A,\mathbb{Z}),C) \cong A \otimes C$, whenever A is a finitely generated G-module.

Theorem 2.2.1. *A short exact sequence $0 \to A \to B \to C \to 0$ leads to a long exact sequence,*

$$\ldots. \to \hat{\mathbf{H}}^n(G,A) \to \hat{\mathbf{H}}^n(G,B) \to \hat{\mathbf{H}}^n(G,C) \to \hat{\mathbf{H}}^{n+1}(G,A) \to \ldots..$$

Proof. The positive and negative side of the exact sequence follows from Theorem 2.1.2. Now the part n=-2,-1,0 follows from the commutative diagram, applying snake's lemma.

$$\begin{array}{ccccccccc} \mathbf{H}_1(G,C) & \longrightarrow & \mathbf{H}_0(G,A) & \longrightarrow & \mathbf{H}_0(G,B) & \longrightarrow & \mathbf{H}_0(G,C) & \longrightarrow & 0 \\ \downarrow & & \downarrow{\scriptstyle \phi_A^*} & & \downarrow{\scriptstyle \phi_B^*} & & \downarrow{\scriptstyle \phi_C^*} & & \downarrow \\ 0 & \longrightarrow & \mathbf{H}^0(G,A) & \longrightarrow & \mathbf{H}^0(G,B) & \longrightarrow & \mathbf{H}^0(G,C) & \longrightarrow & \mathbf{H}^1(G,A) \end{array}$$

□

Restriction and Corestriction can be defined as above on the Tate Groups and they satisfy the following properties.

1. (G:H)=n Cor $\circ$ Res=n
2. If G has order n, all tate groups are annhilated by n.
3. If A is a finitely generated G-module, all tate groups are finite.
4. Let P be a p-Sylow subgroup of G, for some prime p.

   Res:$\hat{\mathbf{H}}^q(G,A) \to \hat{\mathbf{H}}^q(P,A)$ is injective on it's p-primary components.

Theorem 2.2.2. *Let G be a finite group, there exists a unique family of homomorphisms*

$$\hat{\mathbf{H}}^q(G,A) \otimes \hat{\mathbf{H}}^q(G,B) \to \hat{\mathbf{H}}^q(G,A\otimes B)\ (a\otimes b \to a.b)$$

such that:

1. *The homomorphisms are functorial in A and B.*
2. *For p=q=0, they are induced by the natural product $A^G \otimes B^G$*
3. *If*

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

   is exact and if

   $$0\to A\otimes M\to B\otimes M\to C\otimes M\to 0 \text{ is exact}$$

   , then for $c\in \hat{\mathbf{H}}^q(G,C)$ and $m\in\hat{\mathbf{H}}^q(G,M)$ $(\delta c).m=\delta(c.m)$
4. *If*

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

   is exact and if

   $$0\to M\otimes A\to M\otimes B\to M\otimes C\to 0$$

   is exact, then for $c\in \hat{\mathbf{H}}^q(G,C)$ and $m\in\hat{\mathbf{H}}^q(G,M)$ $m.(\delta c)=(-1)^q\delta(m.c)$

Proof. As we considered earlier, we have a complete resolution (P_n) of $\mathbb{Z}$.
Define ζ:$\mathrm{P}_0 \to \mathbb{Z}$ such that ζ(g)=1 $\forall$ g $\in$ G.
As for the existence of the family of homomorphisms,
$\Phi_{p,q}$:$\mathrm{P}_{p+q} \to \mathrm{P}_p \otimes \mathrm{P}_q$ satisfying
(i) $\Phi_{p,q} \circ d = d \otimes 1 + (-1)^p (1 \otimes d) \circ \Phi_{p,q+1}$ (ii)$(\zeta \otimes \zeta) \circ \Phi_{0,0} = \zeta$.

(i) tells us that the maps depends only on the class of the cocycles, so indeed we have a map from
$\hat{\mathbf{H}}^q(G, A) \otimes \hat{\mathbf{H}}^q(G, B) \to \hat{\mathbf{H}}^q(G, A \otimes B)$ defined by
f.g=(f$\otimes$g)$\circ\Phi_{p,q}$
Now (i) gives that f.g=(df).g+$(-1)^p$f.(dg)
The functoriality comes from the definition of the maps and (ii) yields (2).
Now for (3), consider the exact sequence
$0 \to \mathbf{Hom}_G(P_p, A) \to \mathbf{Hom}_G(P_p, B) \to \mathbf{Hom}_G(P_p, C) \to 0$.
Choose a cocycle in $\mathbf{Hom}_G(P_p, C)$, say c which represents the cohomology class γ. Now lift c to an element b $\in \mathbf{Hom}_G(P_p, B)$. db maps to 0 in $\mathbf{Hom}_G(P_{p+1}, C)$, so the exactness allows us to lift db to an element in $\mathbf{Hom}_G(P_{p+1}, A)$. Class of db in $\hat{\mathbf{H}}^{p+1}(G, A)$=$\delta(\gamma)$. If μ is a cocycle in $\mathbf{Hom}_G(P_q, M)$ representing m. d(μ)=0, and the discussion above gives $(\delta c).m = \delta(c.m)$. Similar proof works for (4). □

Definition 2.2.2. *Let H be a subgroup of G, and $g_1, g_2, ...g_n$ denote a set of representatives of G in H. We have a map $N_{G/H} : A^H \to A^G$ defined as $N_{G/H}(a) = \sum_i (g_i.a)$*
Using Proposition 2.1.6, we get a map

Cor: $\hat{\mathbf{H}}^q(H, A) \to \hat{\mathbf{H}}^q(G, A)$, the co-restriction map.

Proposition 2.2.3. *1. (a.b).c=a.(b.c)*

2. (a.b)=$(-1)^{dim(a).dim(b)}$(b.a)

3. Res(a.b)=Res(a).Res(b)

4. Cor(a.Res(b))=Cor(a).b

2.3 Cohomolgy of Cyclic Groups

Let G be a cyclic group of order n, generated by g and N=$\sum_{0\leq i<n}$ g^i. It's straightforward to see that the following sequence is a projective resolution for $\mathbb{Z}$.

$$.....\mathbb{Z}G\xrightarrow{g-1}\mathbb{Z}G\xrightarrow{N}\mathbb{Z}G\xrightarrow{g-1}\mathbb{Z}G\xrightarrow{\Sigma a_g g\to\Sigma a_g}\mathbb{Z}\to 0$$

This tells us that Tate groups for a cyclic group is periodic of period 2.

$$\hat{\mathbf{H}}^q(G,A)=\hat{\mathbf{H}}^{q+2}(G,A)\ \forall\ \mathrm{q}\in\mathbb{Z}$$

$\hat{\mathbf{H}}^{2q+1}(G,A)=\mathrm{A}_N/I_GA\ \forall\ \mathrm{q}\in\mathbb{Z}$, where A_N denote the kernel of multiplication by N.

$$\hat{\mathbf{H}}^{2q}(G,A)=\mathrm{A}^G/\mathrm{NA}\ \forall\ \mathrm{q}\in\mathbb{Z}$$

So, $\mathbf{H}^2(\mathrm{G},\mathbb{Z})=\mathbb{Z}/\mathrm{n}\mathbb{Z}$.

Theorem 2.3.1. *Let $\mathbf{H}^2(G,\mathbb{Z})=\mathbb{Z}/n\mathbb{Z}$, be generated by σ. Then the map, $\mathbf{H}^q(G,A)\to\mathbf{H}^{q+2}(G,A)$, is an isomorphism, where the map is the cup product by σ.*

Proof. We have the following exact sequences

$$0\to\mathrm{I}_G\to\mathbb{Z}\mathrm{G}\to\mathbb{Z}\to 0 \text{ and}$$

$$0\to\ \mathbb{Z}\to\mathbb{Z}\mathrm{G}\to\mathrm{I}_G\to 0$$

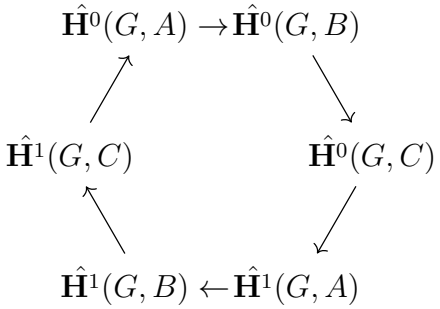
And hence we have
$\hat{\mathbf{H}}^0(\mathrm{G},\mathbb{Z})\cong\mathbf{H}^1(\mathrm{G},\mathrm{I}_G)\ \cong\mathbf{H}^2(\mathrm{G},\mathbb{Z})$
A generator of $\hat{\mathbf{H}}^0(\mathrm{G},\mathbb{Z})$ is a an integer prime to n, say a. We know that there exists $\mathrm{b}\in\mathbb{Z}/\mathrm{n}\mathbb{Z}$ such that $\mathrm{ab}\equiv 1(\mathrm{mod\ n})$. This gives us an inverse image to the cup product by a and hence an isomorphism, at the case q=0. Higher cases follow by dimension shifting.

□

Definition 2.3.1. (*Herbrand Quotient*) *For a cyclic group G and a G-module A. We define the Herbrand Quotient of A,* $h(A)=\frac{|\hat{\mathbf{H}}^0(G,A)|}{|\hat{\mathbf{H}}^1(G,A)|}$, *when both numerator and denominator are finite.*

Proposition 2.3.2. *Let* $0\to A\to B\to C\to 0$ *, be a short exact sequence. If two of the three Herbrand quotients are defined then, we have* $h(B) = h(A).h(C)$.

Proof. We get the following the exact hexagon,



from the periodicity of cohomology for cyclic groups. The proposition follows from calculating the sizes of the images and kernels in each component of the exact sequence. □

2.4 Some Theorems

Lemma 2.4.1. *Fix a prime number p, and G a p-group and A a G-module such that* $pA=0$. *Then the following are equivalent:*

1. $A = 0$.
2. $\boldsymbol{H}^0(G, A) = 0$.
3. $\boldsymbol{H}_0(G, A) = 0$.

Proof. (1) $\implies$ (2) and (1) $\implies$ (3) is trivial.
(2) $\implies$ (1): This proof follows from the orbit-stabilizer theorem for the group action. Each orbit has p-power order and since fixed points of A has at-least one element, the number of fixed points is divisible by p. So if A$\neq$0 $\implies \mathbf{H}^0(G, A) \neq 0$. Hence proved.

(3) $\implies$ (1):Consider $\bar{A}$=$\mathbf{Hom}$(A,$\mathbb{F}_p$). Since, $\mathbf{H}^0(G, \bar{A})$=$\mathbf{Hom}(\mathbf{H}_0(G, A), \mathbb{F}_p)$, we can use a similar argument to the above proof. □

Lemma 2.4.2. *Fix a prime number p, and G a p-group and A a G-module such that pA=0.Suppose* $\boldsymbol{H}_1(G, A)$*=0. Then A is a free module over* $\mathbb{F}_p[G]$*.*

Proof. Since the module is killed by p, so are the homology groups. Now consider an $\mathbb{F}_p$ basis $\bar{a_i}$s for $\mathbf{H}_0(G, A)$, and lift it to A to get a sub-module generated by the lifts a_is, say B. Set C=A/B. Then the exact sequence

$$0 \to \mathrm{B} \to \mathrm{A} \to \mathrm{C} \to 0,$$

yields

$$\mathbf{H}_0(G, B) \to \mathbf{H}_0(G, A) \to \mathbf{H}_0(G, C) \to 0$$

Now the construction of B tells us that $\mathbf{H}_0(G, B) \to \mathbf{H}_0(G, A)$ is an epimorphism, so $\mathbf{H}_0(G, C)$=0. Now by Lemma 2.4.1, C=0. So B=A,i.e a_i generate A as a G-module. So we have a surjective homomorphism θ onto A from a free $\mathbb{F}_p$[G] module F. So on the homology groups, we have
α:$\mathbf{H}_0(G, F) \to \mathbf{H}_0(G, A)$ an isomorphism, by construction.
$\mathbf{H}_1(G, A) \to \mathbf{H}_0(G, Ker(\theta)) \to \mathbf{H}_0(G, F) \xrightarrow{\alpha} \mathbf{H}_0(G, A) \to 0$.
$\mathbf{H}_1(G, A)$=0 and since α is an isomorphism $\mathbf{H}_0(G, Ker(\theta))$=0.
$\implies$ $Ker(\theta)$=0.
$\implies$ θ is an isomorphism.

□

Theorem 2.4.3. *Fix a prime number p, and G a p-group and A a G-module such that pA=0.Then the following are equivalent:*

1. *A is a free* $\mathbb{F}_p[G]$ *module.*
2. *A is an induced module.*
3. *A is cohomologically trivial.*
4. $\exists q \in \mathbb{Z}$ *such that* $\hat{\mathbf{H}}^q(G, A)$*=0.*

Proof. Clearly it suffices to prove (4) $\implies$ (1). Using dimension-shifting, we construct and consider another G-module A' with the property that $\hat{\mathbf{H}}^{q+r}(G,A) = \hat{\mathbf{H}}^{r-2}(G,A')$.
$\implies \hat{\mathbf{H}}^{-2}(G,A') = \hat{\mathbf{H}}^{q}(G,A) = 0.$
$\implies$ A' is a free $\mathbb{F}_p[G]$ module, hence cohomologically trivial(By Lemma 2.4.2).
$\implies \hat{\mathbf{H}}^{-2}$(G,A)=$\hat{\mathbf{H}}^{-q-4}$(G,A')=0.
$\implies$ A is free $\mathbb{F}_p$[G] module.

□

Theorem 2.4.4. *Fix a prime number p, and G a p-group and A a G-module such that A has no p-torsion. Then the following are equivalent:*

1. *A is cohomologically trivial.*
2. *$\exists q \in \mathbb{Z}$ such that $\hat{\mathbf{H}}^q(G,A)$=$\hat{\mathbf{H}}^{q+1}(G,A)$=0.*
3. *A/pA is a free $\mathbb{F}_p[G]$ module.*

Proof. (1) $\implies$ (2) is trivial.
(2) $\implies$ (3):

$$0 \to \mathrm{A} \xrightarrow{p} \mathrm{A} \to \mathrm{A/pA} \to 0.$$

Now

$$\hat{\mathbf{H}}^q(G,A) \to \hat{\mathbf{H}}^q(G,A/pA) \to \hat{\mathbf{H}}^{q+1}(G,A)$$

The assumption therefore says, $\hat{\mathbf{H}}^q$(G,A/pA)=0, and hence from Lemma 2.4.2, the assertion follows.
(3) $\implies$ (2) :
$\hat{\mathbf{H}}^q$(H,A) is a p-group.
The assumption yields, $\hat{\mathbf{H}}^q(H,A) \xrightarrow{p} \hat{\mathbf{H}}^q(H,A)$ is an isomorphism.
$\implies \hat{\mathbf{H}}^q(H,A)$=0.

□

Proposition 2.4.5. *Fix a prime number p, and G a p-group and A a G-module such that A has no p-torsion. A be a G-module which is a free $\mathbb{Z}$ module, and is cohomologically trivial. For a torsion free G-module B, the G-module N=Hom(A, B) is cohomologically trivial.*

Proof. The exact sequence

$$0 \to \mathrm{B} \xrightarrow{p} \mathrm{B} \to \mathrm{B/pB} \to 0 \ ,$$

gives rise to an exact sequence

$$0 \to \mathrm{N} \xrightarrow{p} \mathrm{N} \to \mathbf{Hom}(A, B/pB) \to 0$$

A/pA is a free $\mathbb{F}_p[G]$ module(Theorem 2.4.4), it's induced and hence it's the direct sum of s.A'(s $\in$G) where A' is a subgroup of A/pA. N/pN is therefore induced. Also from the exact sequence, N has no p-torsion. So by Theorem 2.4.4, N is cohomologically trivial. □

Theorem 2.4.6. *Consider a finite group G. Now fix a prime p and consider it's p-Sylow subgroup G_p. Let A be a $\mathbb{Z}$ free G-module. Then the following are equivalent:*

1. *For each prime G_p, A is a cohomologically trivial module.*
2. *A is a projective G-module*

Proof. (2) $\implies$ (1):
If A is cohomologically trivial as a G-module, it is cohomologically trivial as a G_p-module. Since projective modules are cohomologically trivial, the assertion follows.
(1) $\implies$ (2):
Choose an exact sequence

$$0 \to \mathrm{B} \to \mathrm{F} \to \mathrm{A} \to 0, \text{ where F is a free G-module.}$$

A is $\mathbb{Z}$-free, this gives an exact sequence

$$0 \to \mathbf{Hom}(A, Q) \to \mathbf{Hom}(A, F) \to \mathbf{Hom}(A, A) \to 0.$$

$\mathbf{Hom}(A, Q)$ satisfies the condtions of Prop 2.4.5 as a G_p module and is a cohomologically trivial G_p module. So, the derived map,
$\mathbf{Hom}_G(A, F) \to \mathbf{Hom}_G(A, A)$ is surjective since $\hat{\mathbf{H}}^1(\mathrm{G}, \mathbf{Hom}(A, Q)) = 0$.
So the identity map of A extends to a map A $\to$F.
$\Longrightarrow$ The exact sequence splits.
$\Longrightarrow$ A is a direct summand of F.
$\Longrightarrow$ A is projective. □

Theorem 2.4.7. *Let G be a finite group, and A be a G-module. The following are equivalent:*

1. *For each prime p,$\exists$ $q \in \mathbb{Z}$, such that $\hat{\mathbf{H}}^q(G_p, A)$=$\hat{\mathbf{H}}^{q+1}(G_p, A)$=0, for a p-Sylow subgroup G_p of G.*
2. *A is cohomologically trivial.*
3. *There is an exact sequence*

$$0 \to P_1 \to P_2 \to A \to 0$$

with P_1 and P_2 projective G-modules.

Proof. (3) $\Longrightarrow$ (2) $\Longrightarrow$ (1) is clear since projective modules are cohomologically trivial.
(1) $\Longrightarrow$ (3):
Let F be a free module with a surjective homomorphism onto A.
0$\to$B$\to$F$\to$A$\to$0.
$\hat{\mathbf{H}}^q(G_p, B) \cong \hat{\mathbf{H}}^{q-1}(G_p, F)$
$\hat{\mathbf{H}}^q(G_p, B) = \hat{\mathbf{H}}^{q+1}(G_p, B)$ for some q $\in \mathbb{Z}$.
Hence, we can apply Theorem 2.4.6, hence B is projective. □

Theorem 2.4.8. *Let G be a finite group, B and C be two G-modules, f:B$\to$C a G-homomorphism. For p a prime, consider the p-Sylow subgroup of G, G_p. Assume $\exists$ $n_p \in \mathbb{Z}$ such that f^*:$\hat{\mathbf{H}}^q(G_p, B) \to \hat{\mathbf{H}}^q(G_p, C)$ is an epimorphism when $q = n_p$, isomorphism when $q = n_p + 1$ and a monomorphism for $q = n_p + 2$. Then for all subgroups H of G and $\forall q \in \mathbb{Z}$ f^*:$\hat{\mathbf{H}}^q(H, B) \to \hat{\mathbf{H}}^q(H, C)$ is an isomorphism.*

Proof. We can always embed any G-module B inside a cohomologically trivial G-module, namely A=$\mathbf{Hom}(\mathbb{Z}G, B)$. We plan to use the theorems stated above regarding the cohomological triviality of G-modules. For that we consider the module A'=A $\bigoplus$ C, and it is clear

that $\hat{\mathbf{H}}^q(G_p, A') = \hat{\mathbf{H}}^q(G_p, C)$. Now we have the mapping $B \xrightarrow{b\to(i(b),f(b))} A'$. This is clearly injective and hence consider the short exact sequence $0\to B\to A'\to B'\to 0$.
Now the hypotheses tell that for all primes p, $\hat{\mathbf{H}}^q(G_p,B')=0$, for two consecutive values of q. From Theorem 4.9, this means that B' is cohomologically trivial. Hence the map, $f^*:\hat{\mathbf{H}}^q(H,B)\to\hat{\mathbf{H}}^q(H,C)$ is an isomorphism for all subgroups H of G. □

Theorem 2.4.9. *Let G be a finite group and A, B and C be three G-modules. Let* Φ*:*$A\otimes B \to C$ *a G-homomorphism. Fix a* $q \in \mathbb{Z}$ *and choose an element* $a \in \hat{\mathbf{H}}^q(G, A)$*. Consider the map from* $\hat{\mathbf{H}}^n(G_p, B) \to \hat{\mathbf{H}}^{n+q}(G_p, C)$ *induced by the cup product by* $Res_{G/G_p}(a)$*. For each prime p, assume that* $\exists$ n_p *such that this map is surjective for* $n=n_p\in\mathbb{Z}$*, bijective for* $n=n_p+1$ *and injetive for* $n=n_p+2$*. Then for all subgroups H of G and* $n \in \mathbb{Z}$*, the cup-product with* $Res_{G/H}(a)$ *is an isomorphism from* $\hat{\mathbf{H}}^q(H, B) \to \hat{\mathbf{H}}^{n+q}(H, C)$*.*

Proof. Now for the case q=0, we choose $a \in \hat{\mathbf{H}}^q(G, A)$ and $\alpha \in A^G$, which represents a. Now it's clear to see that α represents $\mathrm{Res}_{G/G_p}(a)$ $\forall$ p prime. Now we define the map f:B $\to$ C by $f(\beta)=\Phi(\alpha \otimes \beta)$. We will prove that $\forall$ b $\in$ B, $\Phi^*(Res_{G/H}(a).b) = f^*(b)$. For n=0, this follows from the property of cup products and the definition of f. Using dimension shifting, we prove the general case.
We know that, B and C can be seen as quotients of two cohomologically trivial modules B_* and C_*, with kernels B' and C'. Now f induces a map from B' to C', say f' and f_* from B_* to C_*.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & B' & \longrightarrow & B & \longrightarrow & B_* & \longrightarrow & 0 \\
\downarrow & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f_*} & & \downarrow \\
0 & \longrightarrow & C' & \longrightarrow & C & \longrightarrow & C_* & \longrightarrow & 0
\end{array}$$

Now since B_* and C_* are cohomologically trivial, we know the connecting homomorphisms are isomorphisms, and we get the diagram.

$$\begin{array}{ccc}
\hat{\mathbf{H}}^n(H, B) & \xrightarrow{\delta} & \hat{\mathbf{H}}^{n+1}(H, B') \\
\downarrow{\scriptstyle f^*} & & \downarrow{\scriptstyle f'^*} \\
\hat{\mathbf{H}}^n(H, C) & \xrightarrow{\delta} & \hat{\mathbf{H}}^{n+1}(H, C')
\end{array}$$

Now Φ induces a homomorphism $\Phi':A\otimes B'\to C'$.
And we have $\delta\circ f^*(b)=(f')^*\circ\delta(b)=(\Phi')^*(\mathrm{Res}_{G/H}(a).\delta(b))$
Using the commutativity of connecting homomorphisms, with cup products,
$\delta\circ f^*(b)=(\Phi')^*\circ\delta(\mathrm{Res}_{G/H}(a).b)=\delta\circ(\Phi')^*(\mathrm{Res}_{G/H}(a).b)$.

Now using the fact that the connecting homomorphisms are isomorphisms, $\Phi^*(\mathrm{Res}_{G/H}(a).b)=f^*(b)$ is clear. Now we can appeal to Theorem 2.4.8, and hence prove the theorem for q=0.
General case follows from dimension-shifting. □

Theorem 2.4.10. *(Tate) Let G be a group and let A be a G-module, $a \in \mathbf{H}^2(G, A)$. Let p be a prime in $\mathbb{Z}$ and G_p be a p-Sylow subgroup of G, and assume that*

1. $\mathbf{H}^1(G_p, A)=0$
2. $\mathbf{H}^2(G_p, A)$ *is generated by* $Res_{G/G_p}(a)$ *and has order equal to* $| G_p |$.

Then $\forall$ *H subgroup of G and* $n \in \mathbb{Z}$, *cup product with* $Res_{G/H}(a)$ *induces an isomorphism*

$$\hat{\mathbf{H}}^n(H, \mathbb{Z}) \xrightarrow{\sim} \hat{\mathbf{H}}^{n+2}(H, A).$$

Proof. This is Theorem 2.4.9 with B=$\mathbb{Z}$, C=A, q=2, n_p=-1. It is easily seen that these modules satisfy the hypotheses and hence the result follows. □

Remark 2.4.1. *This is the most crude version of the Class Field Theory. In our subsequent sections, we will try to show how when G is the Galois group of a field extension, and A a module associated with the extension satisfies, the assumptions of Tate's Theorem.*

Chapter 3

Local Class Field Theory

Let K be a *Local Field*, i.e a field complete w.r.t a discrete valuation, with a finite residue field. By Ostrowski's Theorem, K is either a finite extension of $\mathbb{Q}_p$ for some prime p $\in \mathbb{Z}$ or a Laurent series over a finite field, $\mathbb{F}_q((t))$ where q is a prime power. We can assume all the valuations for the field K are normalised, since any valuation is equivalent to one. Let K_s denote the separable closure of K and consider the Galois group of K_s over K, G(K_s/K). Using class field theory, we aim to describe the abelian extensions of K and the cohomological properties of extensions of K. Now using the discussion in Chapter-1, there is a maximal non-ramified extension of K inside K_s, we call it K_{nr}. Let L/K be an unramified extension of local fields of degree n, Gal(L/K) is cyclic of degree n. The generator of this group is called the Frob(L/K).

3.1 Cohomological Properties

Theorem 3.1.1. *Let L be an unramified extension of K of degree n, with residue field l and let G=G(L/K). Then the map induced by valuation v:* $\boldsymbol{H}^q(G, L^*) \to \boldsymbol{H}^q(G, \mathbb{Z})$ *is an isomorphism.*

Proof. Let U be the unit group of L. We have the following exact sequence

$$\mathbf{H}^q(\mathrm{G},\mathrm{U}) \to \mathbf{H}^q(\mathrm{G},\mathrm{L}^*) \to \mathbf{H}^q(\mathrm{G},\mathbb{Z}) \to \mathbf{H}^{q+1}(\mathrm{G},\mathrm{U})$$

We will show that $\mathbf{H}^q$(G,U)=0 $\forall$ q $\in \mathbb{Z}$. We need some following lemmas.

Lemma 3.1.2. *Let G be a finite group and let M be a G-module, M^i, $i \in \mathbb{Z}$ be a decreasing sequence of G-submodules, with M^0=M. If M=$\varprojlim M/M^i$ and if $\exists$ $q \in \mathbb{Z}$, such that $\boldsymbol{H}^q(G, M^i/M^{i+1})$=0, then $\boldsymbol{H}^q(G, M) = 0$.*

Proof. Consider a q co-cycle with values in M, say f. We need to show that there is some (q-1) co-chain g such that f=δg.
Since $\mathbf{H}^q(G, M/M^1) = 0$, f=$\delta g_1$+$f_1$, for f_1 some q co-cycle in M^1.
Now since $\mathbf{H}^q$(G,M^1/M^2)=0, f_1=δg_2+f_2, for f_2 some q co-cycle in M^2.
We can construct (f_n,g_n), inductively. Put g=$\sum g_n$.
Summing the f_n=δg_{n+1}+f_{n+1}, we have f=δg.
Hence we have proved what we wanted. □

Lemma 3.1.3. *Let K be a local field, U be a group of units of K, O be the ring of integers of K and k be the residue class field of K. Then $U/U^1 \cong k^*$ and $U^i/U^{i+1} \cong k$, when $i \geq 1$.*

Proof. For $\alpha \in U$ send $\alpha \to \bar{\alpha}$, the coset modulo the maximal ideal of O, in k*. Clearly it's seen that the kernel of this map is U^1. So first part is proved.
For $\beta \in U^i$, let β=1+$\pi^i\beta_1$. $\beta \to \bar{\beta_1}$, the coset modulo the maximal ideal of O, in k*. Clearly it's seen that the kernel of this map is U^{i+1}. So second part is proved. □

Lemma 3.1.4. *Let L and K be as in the theorem. Then $\boldsymbol{H}^q(G, U^i/U^{i+1}) = 0$.*

Proof. Now proving $\mathbf{H}^q$(G,l)=$\mathbf{H}^q$(G,l*)=0, proves the statement. Since L/K is unramified, G(L/K)$\cong$G(l/k) and hence G is cyclic. Now normal basis theorem tells $\mathbf{H}^q$(G,l)=0 $\forall$ q $\in \mathbb{Z}$. So applying Hilbert-90, $\mathbf{H}^1$(G,l*)=0. Now since G is cyclic and l* is finite, the Herbrand quotient is 1, hence $\mathbf{H}^2$(G,l*)=0, and since G is cyclic $\mathbf{H}^q$(G,l*)=0. □

Now Lemma 3.1.2 tells us that $\mathbf{H}^q$(G,U)=0. So we have proved what we wanted. □

We get an easy consequence of the above theorem.

Theorem 3.1.5. *The valuation map v: $K^*_{nr} \to \mathbb{Z}$ defines an isomorphism*

$$\boldsymbol{H}^2(\hat{\mathbb{Z}}, K^*_{nr}) \to \boldsymbol{H}^2(\hat{\mathbb{Z}}, \mathbb{Z}).$$

We give another interpretation of $\mathbf{H}^2(\hat{\mathbb{Z}}, K_{nr}^*)$. Consider the exact sequence $0\to\mathbb{Z}\to\mathbb{Q}\to\mathbb{Q}/\mathbb{Z}$, with each G-module has trivial action. Now since $\mathbb{Q}$ is an injective module, it's cohomologically trivial. So we have the boundary map δ: $\mathbf{H}^1(G, \mathbb{Q}/\mathbb{Z}) \to \mathbf{H}^2(G, \mathbb{Z})$ to be an isomorphism. Now since G acts trivially, $\mathbf{H}^1(G, \mathbb{Q}/\mathbb{Z})$=$\mathbf{Hom}(G, \mathbb{Q}/\mathbb{Z})$. When G=$\hat{\mathbb{Z}}$, we have an isomorphism $\gamma : \mathbf{Hom}(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}$ sending $\phi \to \phi(1)$. So we have isomorphims

$$\mathbf{H}^2(\hat{\mathbb{Z}}, K_{nr}^*) \xrightarrow{v} \mathbf{H}^2(\hat{\mathbb{Z}}, \mathbb{Z}) \xrightarrow{\delta^{-1}} \mathbf{Hom}(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\gamma} \mathbb{Q}/\mathbb{Z}.$$

So we have an isomorphism $\gamma \circ \delta^{-1} \circ v = inv_K$: $\mathbf{H}^2(\hat{\mathbb{Z}}, K_{nr}^*) \to \mathbb{Q}/\mathbb{Z}$.
Let L/K be a Galois extension, with Galois group G. Denote $\mathbf{H}^q(G, L^*)$ by $\mathbf{H}^q(L/K)$.

Theorem 3.1.6. *Let L/K be a finite extension of local fields, of degree n. We have the following commutative diagram.*

$$\begin{array}{ccc} \boldsymbol{H}^2(K_{nr}/K) & \xrightarrow{Res_{K/L}} & \boldsymbol{H}^2(L_{nr}/L) \\ \downarrow{\scriptstyle inv_K} & & \downarrow{\scriptstyle inv_L} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{\quad n \quad} & \mathbb{Q}/\mathbb{Z} \end{array}$$

Proof. Let G_K=G(K_{nr}/K) and G_L=G(L_{nr}/L) are cyclic groups and are generated by Frobenius of K, F_K and Frobenius of L, F_L, respectively. Now if f is the residue class degree L/K, then F_L= F_K^f. Let e denote the ramification index of L/K. Now we have the commutative diagram,

$$\begin{array}{ccccccc} \mathbf{H}^2(K_{nr}/K) & \xrightarrow{v_K} & \mathbf{H}^2(G_K, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & \mathbf{H}^2(G_K, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\gamma_K} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle Res} & & \downarrow{\scriptstyle e.Res} & & \downarrow{\scriptstyle e.Res} & & \downarrow{\scriptstyle n} \\ \mathbf{H}^2(L_{nr}/L) & \xrightarrow{v_L} & \mathbf{H}^2(G_L, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & \mathbf{H}^2(G_L, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\gamma_L} & \mathbb{Q}/\mathbb{Z} \end{array}$$

It's easy to see the commutativity of smaller squares, and the definition of inv maps proves the proposition. □

Corollary 3.1.7. $\mathbf{H}^2(L/K)$ *has order divsible by n.*

Proof. Clearly Ker($\mathrm{Res}_{K/L}$) $\subset \mathbf{H}^2(L/K)$.
But Theorem 3.1.6 tells us that Ker($\mathrm{Res}_{K/L}$) is generated by $u_{L/K}$, such that $\mathrm{inv}_K(u_{L/K})$=1/n.

Hence it's cyclic of order n, and a hence is a subgroup of order n. So the proposition is proved. □

Proposition 3.1.8. *Let L/K be an extension of local fields with Galois group G, there exists an open subgroup V of finite index in U_L, the unit group of L such that V has trivial cohomology.*

Proof. Let O_K, O_L be the ring of integers of K and L, and π_K and π_L be the uniformisers of K and L. By normal basis theorem ∃ a basis of L/K such that $\exists\alpha \in$ L $\sigma(\alpha)$ for $\sigma \in$G, is a K-basis for. Let A=$\sum_{\sigma\in G} O_K.\sigma(\alpha)$. Clearly A has trivial cohomology. We can choose α such that A$\subset O_L$ and clearly A is open in O_L, and ∃ N $\pi_K^N \subset O_L$. Set M=π_K^{N+1} . Choose V=1+M. We claim that V is a subgroup as stated in the proposition. We prove it using Lemma 8.2. So we will produce a decreasing filtration of V, V^i such that successive quotients are cohomologically trivial.
Set V^i=1+π_K^iM .
Proving $\mathbf{H}^q(G, V^i/V^{i+1})$=0 ∀ q ∈ $\mathbb{Z}$
The map taking 1+1+$\pi_K^i\beta \in V^i$ for $\beta \in$ M to it's image $\bar{\beta}$ in M/π_KM. Clearly the map is surjective and has V^{i+1} as it's kernel. But M/π_KM is a free G-module and hence is cohomologically trivial. □

Corollary 3.1.9. *If L/K is an unramified extension of local fields of degree n, h(U_L)=1, card($\boldsymbol{H}^2(L/K)$)=n.*

Proof. We have an exact sequence

$$0\to \mathrm{V}\to U_L\to \mathrm{U}_L/\mathrm{V}\to 0,$$

where V is as in the proposition.
h(V)=1, by construction and h(U/V)=1, since U/V is a finite module. Now h(U)=h(V).h(U/V)=1.
Now,

$$0\to \mathrm{U}_L\to \mathrm{L}\to \mathbb{Z}\to 0$$

h(L)=h(U_L).h($\mathbb{Z}$)
h(L)=1.n=n
By Hilbert-90, $\mathbf{H}^1(L/K)$=0, hence the proposition is proved. □

Proposition 3.1.10. *L/K be a finite extension of local fields of degree n with Galois group G.*

$$\boldsymbol{H}^2(L/K) \cong \mathbb{Z}/n\mathbb{Z}.$$

Proof. We begin the proof by proving a preparatory lemma.

Lemma 3.1.11. (*Ugly Lemma*) *Let G be a finite group and consider a G-module M, suppose $\rho, q \geq 0$ and ρ,$q \in \mathbb{Z}$. Let the following be true:*

1. *$\hat{\boldsymbol{H}}^i(H, M) = 0$, $0 < i < q$ for all subgroups H of G.*

2. *$H \trianglelefteq K \subset G$, with H and K subgroups of G, and K/H is cyclic of prime order, then the order of $\hat{\boldsymbol{H}}^i(H, M)$ divides (K:H)$^\rho$.*

Then order of $\hat{\boldsymbol{H}}^i(G, M)$ divides $\mid G \mid^\rho$.

Proof. Since the restriction map to the cohomology groups of p-Sylow subgroup is injective on the p-primary components, we infer that proving the theorem for p-groups will suffice. We prove the proposition using induction. We know that G has a normal subgroup of index p, say H. We apply the hypothesis to G/H. Now (2) tells me that $\hat{\mathbf{H}}^i(G/H, M^H)$ divides p^ρ and induction hypothesis for H tells me that $\hat{\mathbf{H}}^i(H, M)$ divides $\mid H \mid^\rho$.
Now the restriction-inflation sequence

$$0 \to \hat{\mathbf{H}}^i(G/H, M^H) \to \hat{\mathbf{H}}^i(G, M) \to \hat{\mathbf{H}}^i(H, M).$$

So $\hat{\mathbf{H}}^i(G, M)$ has order dividing $\mid H \mid^\rho .\mathrm{p}^\rho = \mid G \mid^\rho$.
Now q=0, is given by the following exact sequence,

$$\mathrm{M}^H/N_H M \xrightarrow{N_{G/H}} M^G/N_G M \to (M^H)^{G/H}/N_{G/H}(M^H)$$

using the definition of Tate groups. □

Take M=L*, ρ=1 and q=2 in the Ugly Lemma. It's easy to see that both (1) and (2) are satisfied. From corollary 8.7, we know that $\mathbf{H}^2(L/K)$ has a cyclic subgroup of order n. Now using the Ugly Lemma, $|\ \mathbf{H}^2(L/K)\ |$ has order dividing n. So the proposition is proved. □

Let L/K be a finite extension of local fields with Galois group, G. Recalling Tate's Theorem, we need to show that for a $\in \mathbf{H}^2(G, L^*)$:

1. $\mathbf{H}^1(G_p, L^*)$=0 and

2. $\mathbf{H}^2(G_p, L^*)$ is generated by $\mathrm{Res}_{G/G_p}(a)$, and $|\ \mathbf{H}^2(G_p, L^*)\ | = |\ G_p\ |$.

(1) follows by applying Hilbert-90, (2) follows from Theorem 3.1.6.

Theorem 3.1.12. *For $\forall q \in \mathbb{Z}$, there is an isomorphism*

$$\hat{\boldsymbol{H}}^q(G, \mathbb{Z}) \xrightarrow{\cdot u_{L/K}} \hat{\boldsymbol{H}}^{q+2}(G, L^*),$$

where $u_{L/K}$ generates $\boldsymbol{H}^2(L/K)$.

Proof. This is following Tate's Theorem. □

Proposition 3.1.13. *Let L/K be a local field extension with Galois Group G. For all $q \in \mathbb{Z}$ and H, a subgroup of G, and K' be a fixed field of H, we have the following two commutative diagrams.*

$$\begin{array}{ccc} \mathbf{H}^q(G,\mathbb{Z}) & \xrightarrow{\cdot u_{L/K}} & \mathbf{H}^{q+2}(G, L^*) \\ \downarrow Res & & \downarrow Res \\ \mathbf{H}^q(H,\mathbb{Z}) & \xrightarrow{\cdot u_{L/K'}} & \mathbf{H}^{q+2}(H, L^*) \end{array} \qquad \begin{array}{ccc} \mathbf{H}^q(G,\mathbb{Z}) & \xrightarrow{\cdot u_{L/K}} & \mathbf{H}^{q+2}(G, L^*) \\ Cor \uparrow & & Cor \uparrow \\ \mathbf{H}^q(H,\mathbb{Z}) & \xrightarrow{\cdot u_{L/K'}} & \mathbf{H}^{q+2}(H, L^*) \end{array}$$

Proof. This follows from the fact that $u_{L/K'} = Res(u_{L/K})$, and also the properties of cup-products following Proposition 2.2.3. □

3.2 Norm Groups and Existence Theorem

Definition 3.2.1. *$M \subset K^*$ is called a norm subgroup, if $\exists$ a finite extension L such that $M=N_{L/K}(L^*)$*

Proposition 3.2.1. *1. There exists an inclusion reversing, bijective correspondence between finite abelian extension of K and norm subgroups of K.*

2. Let L and L' be finite extensions of K, then $N_{LL'/K}((LL')^*)=N_{L/K}(L^*)\cap N_{L/K}(L'^*)$ and $N_{L\cap L'/K}((L\cap L')^*)=N_{L/K}(L^*).N_{L'/K}(L'^*)$

3. Any subgroup of K^* containing a norm subgroup is a norm subrgoup.

4. Let E be a finite extension and E^{ab} be the maximal sub-extension of E. Then $N_{E/K}(E^*) = N_{E^{ab}/K}((E^{ab})^*)$.

Proof. The proof (1),(2) and (3) follows from the properties of the Local Artin map. (4) follows from Proposition 3.1.13. □

Theorem 3.2.2. (*Local Existence Theorem*) *A subgroup of K^* is a norm subgroup if and only if it is an open subgroup of finite index.*

Proof. Necessity of the condition follows from the properties of the norm map, and the topology on the field. The sufficiency follows from construction in the next section. □

3.3 Lubin-Tate Theory

The results in this section is due to [**1**]. We already know that there is a map $\phi_{L/K} : K^* \to Gal(K^{ab}/K)$, the Local Artin map. We construct extensions of K, K_n such that $\mathrm{Nm}_{K_n/K}(K_n) = (1 + M^n)\pi^{\mathbb{Z}}$, where M $\subset$ K be the valuation ideal and π is the uniformiser of K, such that

1. $[K_n : K]$=q$^n - q^{n-1}$.

2. π is a norm from every K_n.

We set K_π=$\bigcup_n K_n$ and construct the maximal unramified extension of K, K_{un} by adjoining all m-th roots of unity, where m is co-prime to q. Now we get K^{ab}=$K_\pi.K_{un}$, and we get an explicit description of the Local Artin map.

Definition 3.3.1. (*Formal Group*) *Let A be commutative ring with 1, choose* $F \in A[[X,Y]]$ *such that*

1. $F(X,F(Y,Z)) = F(F(X,Y),Z)$.
2. $F(X,0)$=X *and* $F(0,Y)$=Y.
3. $\exists$ *a unique* $G(X) \in A[[X,Y]]$ *such that* $F(X,G(X)) = 0$.
4. $F(X,Y) = F(Y,X)$.
5. $F(X,Y)$=X+Y+(*higher terms of degree* ≥ 2).

Definition 3.3.2. *Define* $\mathcal{F}_\pi$, *as the set of formal power series in one variable such that*

1. $f(X) = \pi X +$ (*higher terms of degree* $\geq$ *2*)
2. $f(X) = X^q (mod \pi)$

Definition 3.3.3. *Let F and G be two formal group laws,* $f : F \to G$, *be a homomorphism, if* $f(F(X_1, X_2, X_3, ...X_n)) = G(f(X_1), f(X_2), f(X_3), ...f(X_n))$.

Proposition 3.3.1. *Let* $f,g \in \mathcal{F}_\pi$, *and let* $h(X_1, X_2, X_3, ...X_n)$, *be a linear form.* $\exists$ *a unique* $\phi \in A[[X_1, X_1, X_2, X_3, ...X_n]]$ *such that* $f(\phi(X_1, X_2, X_3, ...X_n))$=$\phi(g(X_1), g(X_2), g(X_3), ...g(X_n))$, *also* $\phi(X_1, X_2, X_3, ...X_n) = h(X_1, X_2, X_3, ...X_n)$+ (*higher terms of degree* $\geq$ *2*).

Proof. Clearly $h(X_1, X_2, X_3, ...X_n)$ satisfies the condition. Higher cases and uniqueness follows using induction. □

Corollary 3.3.2. *Let* $f \in \mathcal{F}_\pi$, *there exists a unique formal group law,* F_f, *which admits f as an endomorphism.*

Proposition 3.3.3. *Let* $f \in \mathcal{F}_\pi$, *and let* F_f *admits f as an endomorphism. Now* $\forall a \in A$, *there exists a unique* $[a]_f \in A[[X]]$, *such that*

1. $[a]_f$ *commutes with* f

2. $[a]_f = aX +$(*higher terms of degree* ≥ 2).

Corollary 3.3.4. *We get an injective homomorphism,* $A \to End(F_f)$. *Also let* $f,g \in F_f$, *then their corresponding group laws are isomorphic.*

Let K be a local field, π be the uniformiser of K, and let O_K, be it's ring of integers. Fix an algebraic closure of K, K^{al}. $A_f = \{\alpha \in K^{al} : \mid \alpha \mid < 1\}$. Define the action of O_K on A_f, as $a.\alpha = [a]_f(\alpha)$. Also define $A_n = \{\alpha \in A_f : [\pi]_f{}^n(\alpha) = 0\ \}$.

Theorem 3.3.5. *Let,* $K_n = K[A_n]$. *The following is true.*

1. K_n *is a totally ramified extension of degree* $q^n - q^{n-1}$.

2. $(A/\pi^n)^* \cong Gal(K_n/K)$.

3. $\forall\ n$, π *is a norm from* K_n.

Proof. Choose $f \in F_f$. Choose $\pi_1 \in O_K$ such that $f(\pi_1)=0$. Now choose π_2, such that $f(\pi_2)=\pi_1$. Inductively choose π_n, such that $f(\pi_n)=\pi_{n-1}$., We have the following tower of fields,

$$\begin{array}{c} K_n \\ | \\ K(\pi_n) \\ | \\ K(\pi_{n-1}) \\ \vdots \\ K(\pi_2) \\ | \\ K(\pi_1) \\ | \\ K \end{array}$$

Now, since O_K is a PID, $Gal(K_n/K) = End(A_n) = (A/\pi^n)^*$. Now since the minimal polynomials of each π_i, is eisenstein, we get $K(\pi_n)$ is totally ramified and of degree $q^n - q^{n-1}$. But $|(A/\pi^n)^*| = q^n - q^{n-1}$. Hence $K_n = K(\pi_n)$, so the (1),(2) of the propositon is proved. Now (3) follows from the minimal polynomial of π_n, has constant term π except q=2 and n=1. Now in this case K_n=K, and hence statement is trivially satisfied. □

Now we clearly have constructed the extension corresponding to $(1 + M^n)\pi^{\mathbb{Z}}$,and the Proposition 3.2.1 tells us that we have constructed enough extension to prove the theorem for all open subgroups of finite index. Now we state the following theorem without proof.

Theorem 3.3.6. *Let $\phi_K \to Gal(K^{ab}/K)$. Now we know we can write K^{ab}=K_π.K_{un}, by the above discussion. Let u be a unit of K, and π be the uniformiser of K. Now, $\phi(u)$ acts as trivial on K_{un} and as $[u^{-1}]_f$ on K_π. Also $\phi(\pi)$ acts $Frob_K$, the Frobenius automorphism on K_{un}, and 1 on K_π.*

Chapter 4

Global Class Field Theory

Let K be a *Global Field*, i.e either an algebraic number field or a Global function field. Using class field theory, we aim to learn about the abelian extensions of K and the cohomological properties of extensions of K. The results are similar to those of Chapter 3 and the proofs use most of those results.

4.1 Theorems

Theorem 4.1.1. *Let L/K be a number field extension, which is Galois with Galois group G, which is abelian and S be a finite set of primes in K, containing the ones which are ramified in L. Let I^S be the group of fractional ideals which are co-prime to the ones in S. Now for every such S, there is a homomomorphism $\Phi_{L/K} : I^S \to G$, and such that Φ factors through $C_{\mathcal{M}}$. Such a map is called the Global Artin Map.*

In order to attempt a purely algebraic proof of above, Chevalley reduced the statement about ideals, to one about ideles. He proved the equivalence between the theorem above and the following one

Theorem 4.1.2. *Let K be an algebraic number field. K^{ab}, denote the maximal abelian extension inside a fixed seperable closure of K. There exists a homomorphism $\phi : \mathbb{I}_K \to Gal(K^{ab}/K)$ such that the following are true*

1. $K^* \subset Ker(\phi)$

2. *For every finite extension L, of K, the map induces an isomorphism* $\mathbb{I}_K/K^*.Nm(\mathbb{I}_L) \cong Gal(L/K)$.

Similar to the chapter on Local Class Field theory, we show the group $\mathrm{C}_K = \mathbb{I}_K/K^*$, satisfy the hypotheses for Tate's theorem and hence obtain the results.

4.2 Cohomology of Ideles

Proposition 4.2.1. *Let v be a prime of K, and w_0 be a prime of L over v. Now there is an isomorphism* $\mathbf{H}^r(G, \prod_{w|v} L_w^*) \cong \mathbf{H}^r(G_{w_0}, L_{w_0}^*)$

Proof. This follows from noting that $\prod_{w|v} L_w^* \cong \mathrm{Ind}_{G_{w_0}}^G(L_{w_0}^*)$. Similar statements hold $\mathbf{H}^r(G, \prod_{w|v} U_w) \cong \mathbf{H}^r(G_{w_0}, U_{w_0})$.

Proposition 4.2.2. $\mathbf{H}^r(G, \mathbb{I}_L) \cong \bigoplus_v \mathbf{H}^r(G^v, L^{v*})$

Proof. Applying the proposition 4.2.1, and from the definition of the idele group, we get the result. □

Corollary 4.2.3. 1. $\mathbf{H}^1(G, \mathbb{I}_L) = 0$

2. $\mathbf{H}^2(G, \mathbb{I}_L) = \bigoplus_v \mathbb{Z}/n_v\mathbb{Z}$

Let K be a number field and the idele group $\mathbb{I}_K$. Now, we define, the idele class group $\mathrm{C}_K = \mathbb{I}_K/K^*$. This group plays the role similar to that of the multiplicative group of a local field in Local Class Field Theory. Now it's easy to see that for any number field extension L/K with galois group G, $\mathbf{H}^0(G, C_L) = C_K$, and $\hat{\mathbf{H}}^0(G, C_L) = \mathbb{I}_K/K^*.Nm(\mathbb{I}_L)$

Proposition 4.2.4. (*1st Inequality*) *For any galois extension of global fields L/K, with Galois group G,* $| \mathbb{I}_K/K^*.Nm(\mathbb{I}_L) | \geq n$.

Proof. Consider S, a finite set of primes in K, such that

1. S contains the infinite primes
2. S contains all ramified primes
3. S has enough primes such that $\mathbb{I}_K = \mathbb{I}_{K,S}.K^*$.

Let T be the primes lying above S. Let U(T) denote the elements in L^*, which are units at all primes in T. Clearly, $C_L = \mathbb{I}_{L,T}/U(T)$. Now we compute the Herbrand Quotient of C_L. $h(C_L) = h(\mathbb{I}_{L,T})/h(U(T))$. Now $h(\mathbb{I}_{L,T})$ can be obtained by reducing it to the local case, as in Proposition 4.2.1, and similar proof works for U(T). It's easy to see that $h(\mathbb{I}_{L,T})/h(U(T))$=n. From this and the discussion above, the proposition follows. □

Proposition 4.2.5. (*2nd Inequality*) *Let the assumptions of the previous proposition hold. Then*

1. $|\ \hat{\mathbf{H}}^0(G, C_L)\ |$ *and* $|\ \mathbf{H}^2(G, C_L)\ |$ *divide n.*
2. $\mathbf{H}^1(G, C_L) = 0$.

Proof. The proof given below follows for number field extensions and function field extensions, with degree prime to characteristic.
It's clear to see that proving the result for a $\mathbb{Z}/p\mathbb{Z}$-extension, of a field containing nth root of unity is sufficient. But when G is cyclic, the computation on Herbrand Quotient above tells us that, proving $|\ \hat{\mathbf{H}}^0(G, C_L)\ |$ divides n is sufficient. We will prove the result for the extension L/K, with Galois group $(\mathbb{Z}/p\mathbb{Z})^r$.
Clearly, L=K$[a_1^{1/p}, ...a_r^{1/p}]$. Choose a set of finite primes S, such that

1. S contains the infinite primes
2. S contains the divisors of primes and the $a_i s$ are units.
3. S has enough primes such that $\mathbb{I}_K = \mathbb{I}_{K,S}.K^*$.

Now let s=$|\ S\ |$.
Clearly $\exists$ a finite set of primes T, such that
a$\in$U(S) is a p-th power $\iff$ a is a p-th power for all $K_v, \forall$ v$\in$ T.
Now let M = $\prod_{v\in S} K_v^{*p} \times \prod_{v\in T} K_v^* \times \prod_{v\notin S\bigcup T} U_v$.

From a purely group-theoretical calculation, $[\mathbb{I}_{\mathbb{K}} : K^*M] = \frac{[\mathbb{I}_{\mathbb{S}\cup\mathbb{T}}:M]}{[U(S\cup T):K^*\cap M]}$.
Now, clearly $[\mathbb{I}_{S\cup T} : M] = p^{2s}$, from the definition of M.
Also $K^* \cap M = U(S \cup T)^p$.
This shows $[U(S \cup T) : K^* \cap M] = p^{2s-r}$.
Hence we have showed $[\mathbb{I}_{\mathbb{K}} : K^*M] \mid p^r$.
Also M$\subset$ Nm$(\mathbb{I}_L) \implies [\mathbb{I}_{\mathbb{K}} : K^*.Nm(\mathbb{I}_L)] \mid p^r$.
Hence we have proved what we wanted. □

Let L/K be a finite Galois extension of global fields with Galois group G, $\mathbf{H}^n(G, C_L)$ is denoted as $\mathbf{H}^n(L/K, C_L)$ and similarly for other cohomology groups.

Proposition 4.2.6. *Let L/K, be a Galois extension of global fields, with $[L : K]$ finite. Then $\mathbf{H}^2(G, C_L)$ is cyclic of order $[L : K]$.*

Proof. Consider $\mathbb{I}_L$. Since by proposition 4.2.2, we have inv_v map for each valuation v. Define inv:$\mathbf{H}^2(G, \mathbb{I}_L) \to \mathbb{Q}/\mathbb{Z}$ as $\text{inv}((\alpha_v)_v) = \Sigma_v inv_v(\alpha_v)$.
The map induces a map inv: $\mathbf{H}^2(G, C_L) \to \mathbb{Q}/\mathbb{Z}$. Using the local information about the map, we get that map is a surjection onto $\mathbb{Z}/n\mathbb{Z}$. Now $\mathbf{H}^2(G, C_L)$ has order dividing n, by Proposition 4.2.5. So it's an isomorphism. □

We get that $\mathbf{H}^2(G, C_L)$ is generated by an element $u_{L/K}$, such that inv($u_{L/K}$)=1. Now it's clear to see that G-module C_L, satisfies the hypothesis of the Tate's theorem. Hence we have the following.

Theorem 4.2.7. *For $\forall q \in \mathbb{Z}$, there is an isomorphism*

$$\hat{\mathbf{H}}^{q-2}(G, \mathbb{Z}) \xrightarrow{.u_{L/K}} \hat{\mathbf{H}}^q(G, C_L),$$

where $u_{L/K}$ generates $\boldsymbol{H}^2(L/K, C_L)$.

From the interpretation of the cohomology groups, we have obtained our contention.

Proposition 4.2.8. *Let L/K be a global field extension with Galois Group G. For all $q \in \mathbb{Z}$ and H, a subgroup of G, and K' be a fixed field of H, we have the following two commutative diagrams.*

$$\begin{array}{ccc} \hat{\mathbf{H}}^q(G,\mathbb{Z}) & \xrightarrow{.u_{L/K}} & \hat{\mathbf{H}}^{q+2}(G,C_L) \\ \downarrow Res & & \downarrow Res \\ \hat{\mathbf{H}}^q(H,\mathbb{Z}) & \xrightarrow{.u_{L/K'}} & \hat{\mathbf{H}}^{q+2}(H,C_L) \end{array} \qquad \begin{array}{ccc} \hat{\mathbf{H}}^q(G,\mathbb{Z}) & \xrightarrow{.u_{L/K}} & \hat{\mathbf{H}}^{q+2}(G,C_L) \\ Cor \uparrow & & Cor \uparrow \\ \hat{\mathbf{H}}^q(H,\mathbb{Z}) & \xrightarrow{.u_{L/K'}} & \hat{\mathbf{H}}^{q+2}(H,C_L) \end{array}$$

4.3 Norm Groups and Existence Theorem

Definition 4.3.1. *A subgroup H of C_K is said to be normic if $\exists$ L with H=$Nm(C_L)$.*

Proposition 4.3.1.

1. *Any subgroup of C_K containing a norm subgroup is a norm subgroup.*
2. *Let E be a finite extension and E^{ab} be the maximal sub-extension of E. Then $N_{E/K}(C_E) = N_{E^{ab}/K}(C_{(E^{ab})})$.*

Theorem 4.3.2. *Let K be a global field. Let H be an open subgroup of finite index in C_K. Then H is normic.*

Chapter 5

Applications

As noted in the introduction, Class Field Theory was inspired by law of quadratic reciprocity. We try to give an exposition on how one can derive quadratic, cubic and bi-quadratic reciprocity laws, from statements of Class Field Theory.

5.1 Norm Residue Symbol

Let K be a number field, and let K contains m-th roots of unity. Let S denote the set of primes in K, which contains the archimedean ones and the ones dividing m. Now S$(a_1, a_2, ..., a_r)$ be the set of primes in S and the ones which divide at-least one a_i. Let a, b $\in$ K*, and for an arbitrary prime v of K, let Φ_v be the local artin map, for the field K_v*, for the extension K($\sqrt[m]{a}$)/K. We define

$$(a, b)_v = \frac{\Phi_v(b)(\sqrt[m]{a})}{(\sqrt[m]{a})} .$$

Clearly, $(a, b)_v$ is a m-th root of unity. Also the properties of local artin map gives us $(a, b)_v.(a, b')_v=(a, bb')_v$, and also $(a, b)_v.(a', b)_v=(aa', b)_v$. The above two statements, says that $(a, b)_v$=1 if a or b is an mth power in K_v*. This gives us a bi-linear map $K_v^m \times K_v^m$. Using Local Class Field Theory, $(a, b)_v$=1 $\iff$ b is a norm from the extension $K_v(\sqrt[m]{a})/K_v$.

Lemma 5.1.1. *Let F be a field containing the mth roots of unity, and choose $a \in F^*$.*
$\forall\ x \in F$, x^m-a is a norm from F($\sqrt[m]{a}$).

Proof. We have an isomorphism from Galois Group G, to a subgroup of μ_m, μ_d. Now choose a set of representatives of cosets of μ_d in μ_m, (ζ_i). Let $\alpha = \sqrt[m]{a}$. Now,

$$x^m\text{-a}=\prod_{\zeta\in\mu_m}\ (\text{x-}\zeta\alpha)=\text{N}_{F(\ \sqrt[m]{a})/F}(\prod_{i=1}^{m/d}(x-\zeta_i\alpha))$$

□

By Lemma 5.1.1, we have $(a,b)_v$=1 if a+b is a m-th power in K_v. We get,
$(a,-a)_v = (a,1-a)_v$=0. Also we get $(a,b)_v = (b,a)_v^{-1}$. Now using the interpretation of Global Artin map, as a product of local artin maps, $\forall a,b \in$ K*, $\prod_{\forall v}(a,b)_v$=1.
We put

$$\left(\frac{a}{b}\right) = \prod_{v\notin S(a)}(a,b)_v.$$

Proposition 5.1.2. *Let $v \notin S(a)$ and ρ_v denote the prime ideal corresponding to v, the following are equivalent,*

1. $\left(\frac{a}{v}\right) = 1$.
2. $x^m \equiv a (mod\ \rho_v)$
3. x^m=*a is solvable with $x \in K_v$*

Proposition 5.1.3. (*General power reciprocity Law*)

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1}=\prod_{v\in S(a)\cap S(b)}(b,a)_v$$

Proof. This is a straightforward calculation following (5.1). □

5.2 Quadratic Reciprocity Law

We try to give a method of proof of Quadratic Reciprocity Law, one of the most celebrated theorems in Mathematics, not only Number Theory. This is a theorem, which gives conditions of solvability of a quadratic equation, modulo primes. This was conjectured by Euler in 1600's, and was formulated in the present form by Legendre. Gauss proved the theorem in 1801, and he was so captivated by the theorem that, he called it *aureum theorema*(Golden Theorem). He gave 5 other proofs for the theorem, before anyone else found a proof. He denotes to theorem as "Fundamental Theorem" and in his *Disquisitiones Arithmeticae*, he writes

> "The fundamental theorem must certainly be regarded as one of the most elegant of its type."

There are around 250 published proofs of the statement. Generalisation of quadratic reciprocity law has yielded great achievements in number theory and algebraic geometry.

Theorem 5.2.1. *Let p,q be two odd primes in $\mathbb{Z}$. The reciprocity law states that*

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

The following statements are called supplements to the reciprocity law,

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

Proof. We set K=$\mathbb{Q}$, and m=2. Now clearly S=$\{2,\infty\}$. Now the interpretation of $(a,b)_v$ as the norm of an extension, gives us $(x,p)_\infty$=1. The statements are equivalent to evaluating, $(a,b)_v$, for certain cases. Now $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$=$(p,q)_2.(p,q)_\infty$. We know that, numbers$\equiv$1(mod 8) are 2-adic squares.
This gives, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ if p$\equiv$q(mod $8a_0$), where a=$2^v.a_0$, where a_0 is odd.
By the discussion above, $(p,q)_\infty$=1. Now let p,q be odd primes, such that p$\equiv$q(mod8), then

$\left(\frac{p}{q}\right).\left(\frac{q}{p}\right)=\left(\frac{-1}{q}\right)$. Now fixing r, varying p, keeping (p,q)=1, we get $\left(\frac{p}{q}\right).\left(\frac{q}{p}\right)$ depends on Q(mod 8). Calculating $\left(\frac{p}{q}\right).\left(\frac{q}{p}\right)$ for the first few primes, gives the result. Similar procedure, for the cases -1 and 2, yields the supplementary laws. □

In the subsequent sections, we will prove higher reciprocity laws, namely cubic and bi-quadratic reciprocity laws. Both these reciprocity laws were proved originally by Jacobi sums, but these didn't yield much progress for higher reciprocity laws in 1844. Much work on higher reciprocity laws, were proved after Artin Reciprocity Laws.

5.3 Cubic Reciprocity Law

Let ζ_3, be the cubic root of unity. Let $\alpha \in \mathbb{Z}[\zeta_3]$, such that α is co-prime to 3 i.e $\alpha \equiv \pm 1 \bmod (1-\zeta_3)^2$. Then α is called 3-primary. We will prove the following theorem.

Theorem 5.3.1. (*Cubic Reciprocity Law*) α, $\beta \in \mathbb{Z}[\zeta_3]$, *where both are 3-primary, then*

$$\left(\frac{\alpha}{\beta}\right)_3=\left(\frac{\beta}{\alpha}\right)_3.$$

Proof. Let K=$\mathbb{Q}(\zeta_3)$, then 3 is totally ramified in K, and the unique ideal above 3 is generated by $\lambda = 1-\zeta_3$, and is denoted by v. U_i=$\{$u$\in$ K$^*_v$:u$\equiv$1(mod λ^i)$\}$. U_i/U_{i+1} is cyclic of order p, and is generated by the image of η_i=1-λ^i. Then we have the following:

1. $(\eta_i, \eta_j)_v$=$(\eta_i,\eta_{i+j})_v$.$(\eta_{i+j},\eta_j)_v$.$(\eta_i,\lambda)_v{}^{-1}$

2. If i+j $\geq$ p+1, then (a,b)$_v$=1, a $\in U_i$, b $\in U_j$.

3. $$(\eta_i, \lambda)_v = \left\{ \begin{array}{ll} 1 & \text{for } 1 \leq i \leq p-1 \\ \lambda & \text{for } i = p \end{array} \right\}$$

4. (a,b)$_v$ is the unique skew-symmetric pairing K$_v$* $\times$ K$_v$* $\to \mu_3$, satisfying (1) and (3).

Now, let K_v=$\mathbb{Q}_3(\zeta_3)$. Since α, β are 3-primary, $\alpha, \beta \in U_2$, the statement is to prove that the bi-linear pairing denoted as above is trivial on $U_2 \times U_2$. This follows from the fact that $U_3 = U_4$. Also the general fact that the nth norm residue pairing is trivial on $U_i \times U_j$ whenever $U_{i+j} \subset U_n$. So this proves the cubic reciprocity law. Now similar to the proof of the cubic reciprocity law, we use the triviality of norm pairing. Clearly $U^4 = U^3$. □

5.4 Biquadratic Reciprocity Law

Let $\alpha \in \mathbb{Z}[\iota]$, such that $\alpha \equiv 1 \bmod (1+\iota)^3$. Then α is called primary. Clearly every element in $\mathbb{Z}[\iota]$ is primary, after a suitable multiplication by a power of ι. We will prove the following theorem.

Theorem 5.4.1. (*Biquadratic Reciprocity Law*) α, $\beta \in \mathbb{Z}[\iota]$, *where both are primary, then*

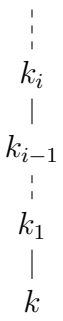
$$\left(\frac{\alpha}{\beta}\right)_4 \left(\frac{\beta}{\alpha}\right)_4^{-1} = (-1)^{\frac{N\alpha-1}{4}\frac{N\beta-1}{4}},$$ *where* $N{:}\mathbb{Z}[\iota] \to \mathbb{Z}$ *is such that* $N(a+ib)=a^2+b^2$.

Proof. The theorem amounts to computing, the power residue symbol $(\alpha, \beta)_{1+i}$, for m=4, K=$\mathbb{Q}$, using the power reciprocity law. Let K_v=$\mathbb{Q}_2(\iota)$. Now the ring of integers of K_v, is $\mathbb{Z}_2(\iota)$, and π be the uniformizer. If $\alpha \in U^3$, $\alpha \in U^4 \iff N(\alpha) \in 1+ 8\mathbb{Z}$. The theorem reduces to determine the norm residue pairing for F^*. Clearly F^*/F^{*4}=$(\pi)\times$ U/U^4. Now U_k/U_{k+1} is generated by 1-π^k. So F^*/F^{*4}=$(\pi)\times$(1-π)$\times$(1-π^2)$\times$ (1-π^3). We get π=1-i. Now the bi-linearity of the pairing reduces to evaluating $(a,b)_{1+i}$, for a,b $\in$ {1-i,i,3+2i,5}. This yields us bi-quadratic reciprocity law. □

Chapter 6

Class Field Towers

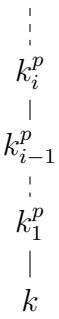
Let k be a number field and k_1 be it's Hilbert class field, i.e the Class field for the trivial modulus($\mathcal{M} = 1$). Clearly all prime ideals in k are unramified in k_1. Hilbert conjectured that ideals in k, become principal in k_1. Artin reduced it to a problem concerning finite abelian groups, and Furtwängler solved the problem, hence gave a positive answer to Hilbert's conjecture. However, it doesn't say that all ideals in k_1 are principal, since there might be ideals in k_1, which are not coming from k. So we can construct the class field of k_1, k_2 and go on by constructing consecutive class fields. So we have the following tower,



The question posed was whether this extension is finite, i.e whether exists some i such that k_i was a principal ideal domain. Similar to the discussion regarding Principle Ideal Theorem, we reduce it to a purely group theoretic question and answer that.

Definition 6.0.1. *Let p be a prime number, the* Hilbert p-Class Field*, is the maximal p-extension of k, contained in k_1 and is denoted by k_1^p.*

We can construct a similar tower of Hilbert p-class fields,Hilbert p-class field tower,



Denote $\mathrm{k}^p = \bigcup k_i^p$. Now if this extension is infinite, we know that the Hilbert Class field tower is infinite. We give criterion regarding the finiteness of Hilbert p-class field tower.

Definition 6.0.2. *For any group G, G/p denote the maximal abelian factor group of exponent p and $d^p(G)$.*

Let r_k denote the infinite primes of an algebraic number field.

6.1 Theorem due to Golod-Safarevic

Theorem 6.1.1. *(Golod-Safarevic) Let k be an algebraic number field of degree n, such that the Hilbert p-class field tower is finite. Then there exists a function such that* $d^p(G) < 2 + 2\sqrt{(r_k + \delta_k^p)}$.

Proof. Cl_k:Ideal Class Group,
C_k:Idele Class Group,
U_k:Idele Unit group
E_k:Groups of units in k
μ_k:Group of unity in k
G=Galois group(k^p/k)
$d^p(E_k)$=(r_k-1)+δ_k^p where δ_k^p=1 if k contains the pth roots of unity and 0 otherwise.
Let K, be the Hilbert Class Field of k.

Clearly, $\mathrm{d}^p(G) = d^p(Cl_k)$, and we will show that $\frac{1}{4}(d^p(G))^2 - d^p(G) < d^p(E_k)$.
Now we have the exact sequences

$$1 \to E_K \to U_K \to U_K/E_K \to 0$$

$$1 \to U_K/E_K \to C_K \to Cl_K \to 0$$

Since K is the Hilbert Class Field , U_K is a cohomologically trivial G-module. Applying that along with Tate's theorem for (G,C_K), we get
$\hat{\mathbf{H}}^0(G, E_K) \cong \hat{\mathbf{H}}^{-1}(G, U_K/E_K) \cong \hat{\mathbf{H}}^{-1}(G, C_K) \cong \hat{\mathbf{H}}^{-3}(G, \mathbb{Z})$
Now define $\mathrm{d}_i^p(G) = dim(\mathbf{H}_i(G, \mathbb{Z}/p))$

Lemma 6.1.2. *$d_i^p(G) = d^p(G)$, and $d_2^p(G) - d_1^p(G) = d^p(\mathbf{H}_2(G, \mathbb{Z}))$.*

Proof. This follows from using the derived homology sequence for
$0 \to \mathbb{Z} \xrightarrow{p} \mathbb{Z} \to \mathbb{Z}/p \to 0$, namely $0 \to \mathbf{H}_i(G, \mathbb{Z})/p \to \mathbf{H}_i(G, \mathbb{Z}/p) \to \mathbf{H}_{i-1}(G, \mathbb{Z})_p \to 0$.
where A_p and A/p denote the kernel and co-kernel of the endomorphism of A, by multiplication with p. The lemma follows by comparing $\mathbb{F}_p$ dimensions of each components. □

Proposition 6.1.3. *$d_2^p(G) > \frac{1}{4}(d_1^p(G))^2$*

Proof.

Lemma 6.1.4. *Let G be a finite p-group and A be a G-module with pA=0. Then the minimal number of generators of A as a G-module=dim($\mathbf{H}_0(G, A)$).*

Proof. We generate a sub-module B of A using the pre-images of the generators of $\mathbf{H}_0$(G,A). Now $\mathbf{H}_0$(G,A/B)=0 and appealing to Lemma 2.4.1, we get A/B=0. This proves the lemma. □

Lemma 6.1.5. *Let G be a finite group, such that pA=0. Then there exists a resolution with the following properties*

$$\ldots \to Y_2 \to Y_1 \to Y_0 \to A \to 0,$$

such that

1. *Each Y_n is free over $\mathbb{Z}G/p$.*

2. *The number of generators of each Y_n over $\mathbb{Z}G/p$=dim $\mathbf{H}_n(G, A)$*

3. *Image $(Y_{n+1}) \subset Y_n$*

Proof. The existence of Y_0 comes from Lemma 5.1.4. This gives an exact sequence

$$0 \to B \to Y_0 \to A \to 0$$

, and we get $\mathbf{H}_1(G, A) = \mathbf{H}_0(G, B)$ and can apply Lemma 5.0.4 to get Y_1. Now repeatedly applying Lemma 5.0.4 yields the exact sequence. □

E be a free $\mathbb{Z}G/\mathrm{p}$ module with 1 generator. D=E^d and R=E^r, and by Lemma 6.1.4, we have an exact sequence

$$\mathrm{R} \to D \to I.E \to 0.$$

Let A be a finite module and consider the polynomial,

$$\mathrm{p}_A(t) = \textstyle\sum_{n \geq 0} \dim(I^n \mathrm{A}/\mathrm{I}^{n+1}\mathrm{A})\mathrm{t}^n.$$

Now since dim(E/IE)=1, $P_E(t) = 1 + t.P_{IE}(t)$. Now $P_D(t) = d.P_E(\mathrm{t})$ and $P_R(t) = r.P_E(\mathrm{t})$. Now $0< t <1$ be a real variable, then

$$\tfrac{P_A(t)}{1-t} = \textstyle\sum_{n \geq 0} dim(A/I^{n+1}A)t^n.$$

Now we have an epimorphism $\mathrm{I}^{n+1}D \to I^{n+2}E$, and let R_{n+1} be the preimage of $\mathrm{I}^{n+1}D$ in R and hence we have an exact sequence $0 \to R/R_{n+1} \to D/I^{n+1}D \to E/I^{n+2}E \to 0$. Now $\dim(\mathrm{R}/\mathrm{R}_{n+1}) \leq dim(R/I^nR)$. So $\dim(\mathrm{D}/\mathrm{I}^n\mathrm{D}) \leq \dim(\mathrm{R}/\mathrm{I}^n\mathrm{R}) + \dim(\mathrm{IE}/\mathrm{I}^{n+1}\mathrm{E})/$. Hence 5.1 term by term, we get

$$\tfrac{P_D(t)}{1-t} \leq \tfrac{P_{IE}(t)}{1-t} + \tfrac{P_R(t)}{1-t}$$

$$\implies d.P_E(t) \leq \tfrac{P_E(t)-1}{t} + r.t.P_E(t)$$

$$\implies 1 \leq P_E(\mathrm{t})(\mathrm{r}t^2\text{-dt+1}) \text{ if } 0 < t < 1$$

Now $\mathrm{P}_E(\mathrm{t})$ has positive coefficients, we get
$0 < \mathrm{r}t^2\text{-dt+1}$ if $0 < t < 1$
We know from Lemma 6.1.2 that $\mathrm{d} \leq \mathrm{r} \leq 2\mathrm{r}$. Substituting $\mathrm{t}=\frac{d}{2r}$, we get $\mathrm{r} > \frac{d^2}{4}$
Hence the proposition is proved. □

Now, using Proposition 6.1.3 and the discussion above,

$$\tfrac{1}{4}(d^p(G))^2 - d^p(G) < d^p(\hat{\mathbf{H}}^0(G, E_k)) < d^p(E_k).$$

Hence we have proved the theorem. □

6.2 Theorem due to Brumer

We give a theorem which sets a lower limit for $d^p(Cl_k)$, and combining with the result of Golod and Safarevic, we get number fields where the Hilbert p-class field tower is infinite.

Definition 6.2.1. *Define $e_k(q)$=gcd $e(\sigma)$, where $\sigma|q$. q is completely ramified if $e_k(q) > 1$.*

Theorem 6.2.1. *(Brumer) Let k, be an algebraic number field, which is Galois over $\mathbb{Q}$. There exists a function such that*

$$d^p(Cl_k) \geq t_k^p \text{ - } (\tfrac{r_k-1}{p-1} + v_p(n).\delta_k^p), \text{ where } t_k^p \text{ is the number of completely ramified primes, such that } p \text{ divides } e_k(q).$$

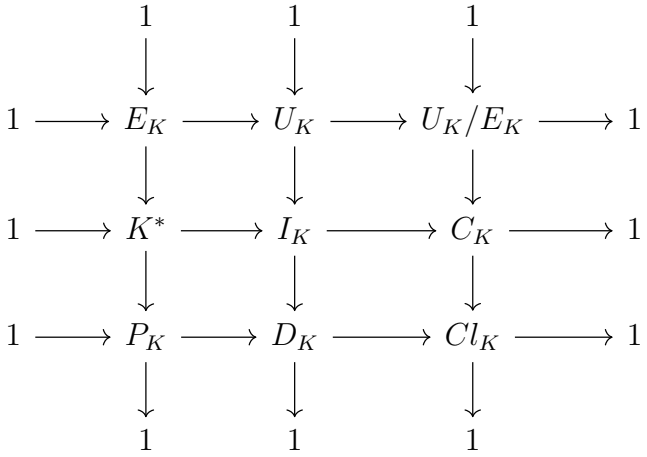
Proof. Let K be the Hilbert Class Field of k. G be the Galois group of K/k, G^* be the Galois group of K/$\mathbb{Q}$ and g be the be the Galois group of k/$\mathbb{Q}$. The restriction-inflation sequence yield

$$d^p(\mathbf{H}^1(G^*, E_K)) < d^p(\mathbf{H}^1(G, E_K)) + d^p(\mathbf{H}^1(g, E_k)).$$

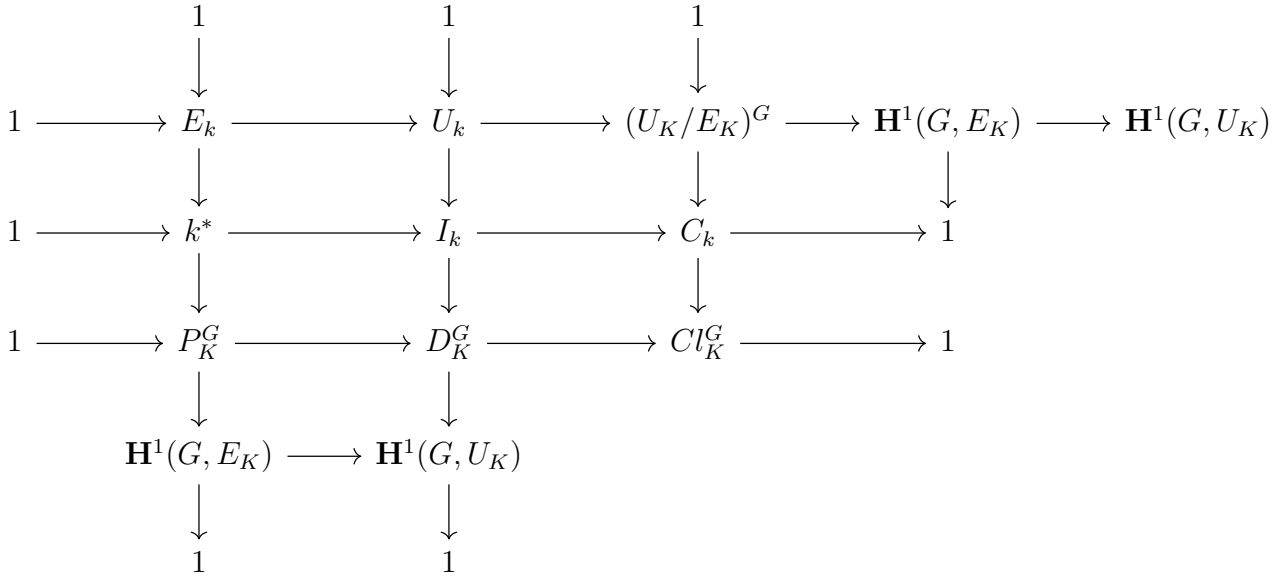
Now we will prove,
1.$\mathbf{H}^1(G, E_K) = Cl_k$

2.$d^p(\mathbf{H}^1(G^*, E_K))=\mathrm{t}_k^p$
3.$d^p(\mathbf{H}^1(g, E_k))=\frac{r_k-1}{p-1} + \mathrm{v}_p(\mathrm{n}).\delta_k^p$

Now for any algebraic number field of finite degree over $\mathbb{Q}$ with Galois group G. We have the following commutative diagram,



Applying the long-exact cohomology sequence, for this diagram,



We use the following:

Lemma 6.2.2. *Let K/k be a Galois extension of algebraic number fields, with Galois group G. Let $D_K^G \subset P_K$. Then we have the following exact sequence.*

$$1 \to Cl_k \to \mathbf{H}^1(G, E_K) \to \mathbf{H}^1(G, U_K) \to 1$$

Proof. The assumption tells that P_K^G=D_K^G, hence the map between them is an isomorphism. This tells us that the map is surjective. Similarly working on the upper right hand corner on the diagram tells about the kernel of the map. □

Now it's clear to see that it's true for the extension K/$\mathbb{Q}$ and K/k. Now for K/k, $\mathbf{H}^1(G, U_K) \implies \mathbf{H}^1(G, E_K) = Cl_k$. Now $\mathrm{Cl}_{\mathbb{Q}}$=1 $\implies \mathbf{H}^1(G^*, E_K) = \mathbf{H}^1(G^*, U_K)$.
Now reducing to the local case implies $\mathbf{H}^1(G^*, U_K)$= $\prod_q \mathbb{Z}/e_k(q)$. The discussion on p-rank, yields $d^p(\mathbf{H}^1(G^*, E_K))$=$\mathrm{t}_k^p$. □

In-order to prove (3), we prove a general statement.

Lemma 6.2.3. *Let G be a finite group of order, and A be a finitely generated G-module. Let Tor(A) denote the torsion group of A and let $\rho(A)$ denote the no.of generators of A/Tor(A) as an abelian group. For any prime number p, we have*

$$d^p(\mathbf{H}^1(G, A))=\tfrac{\rho(A)}{p-1} + v_p(n).d^p(Tor(A))$$

Proof. We will prove , $d^p(\mathbf{H}^1(G, A/Tor(A))) \leq \frac{\rho(A)}{p-1}$ and $d^p(\mathbf{H}^1(G, Tor(A)) \leq \mathrm{v}_p(\mathrm{n}).d^p(Tor(A))$.
Similarly we will prove the following theorem, in a generality. We will show the theorem when A is a torsion module and A is a free module separately.
Let A be a torsion module. Clearly $d^p(G) \leq \mathrm{v}_p(\mathrm{n})$. Since, $\mathbf{H}^1(G, A)$ is a quotient group of crossed homomorphisms from G to A. It's clear to see that the map just depends on the generators. So the set of crossed homomorphisms is an injection to A^d, where d is the no.of generators. Now Burnside basis yields, $d^p(G)$=d. Now the discussion tells us $d^p(\mathbf{H}^1(G, A)) \leq d^p(G).d^p(A)$. Hence the torsion case is proved. Now when A is a free module, we have the following lemma due to Chevalley. □

Lemma 6.2.4. *Let G=$\mathbb{Z}/p\mathbb{Z}$. Let A be a finitely generated A-module, then*

$$d^p(\mathbf{H}^1(G,A)) - d^p(\mathbf{H}^2(G,A)) = \frac{\rho(A)-p.\rho(A^G)}{p-1}.$$

Proof. It's clear that the LHS is an additive version of the Herbrand quotient hence, most of the properties about the Herbrand quotient can be used in the additive sense.
Proposition 2.3.2 tells us the additivity of the function on exact sequences. Similarly if A$\otimes_{\mathbb{Z}}\mathbb{Q}$ and B$\otimes_{\mathbb{Z}}\mathbb{Q}$ are isomorphic as $\mathbb{Q}$[G] modules, LHS takes the same value on A and B(LHS is a function of rational equivalent classes). A similar analysis tells us that, RHS too is a function of rational equivalence classes, additive on exact sequences. Now, A$\otimes_{\mathbb{Z}}\mathbb{Q}$ is a representation space of G. The theorem amounts to finding all the irreducible ones and verifying the proposition for those. A basic exercise in representation theory tells us that there are only two of those, a 1-dimensional trivial representation and a $p-1$ dimensional one. Hence the lemma amounts to verifying the result for $\mathbb{Z}$ and I_G, which follows from the exact sequence

$$0\to\mathbb{Z}\to\mathbb{Z}\mathrm{G}\to\mathrm{I}_G\to 0$$

and the properties for the Herbrand quotient of $\mathbb{Z}$ and $\mathbb{Z}G$. □

Lemma 6.2.5. *Let G be a finite p-group and A be a finitely generated G-module, which is torsion free. Then,*

$$d^p(\mathbf{H}^1(G,A)) \leq \frac{\rho(A)-\rho(A^G)}{p-1}.$$

Proof. The proof is by induction. When G=$\mathbb{Z}$/p$\mathbb{Z}$, Lemma 6.2.4 and the torsion-free property yields the result. The higher cases follow from the fact that for every p-group, we have a normal subgroup of index p and the corresponding restriction inflation sequence. □

Now, we know that restriction map from a group to it's p-Sylow subgroup is injective on it's p-primary components. So the theorem is proven if we have proved the same for p-groups. But using Lemma 6.2.5, we have obtained our contention. □

6.3 Some examples

As remarked in the introduction of the chapter we are seeking the question whether all class field towers are finite. Clearly from the above results we can see that, the class field tower is infinite if $\mathrm{t}_k^p \geq \frac{r_k-1}{p-1} + \mathrm{v}_p(\mathrm{n}).\delta_k^p + 2 + 2\sqrt{(r_k + \delta_k^p)}$.

Now let p=2, n=2. Now, δ_k^p=1. Also completely ramified is the same as being ramified. Let K be a quadratic number field. K has infinite-class field tower when the

$$\text{number of ramified primes is} \geq 2 + r_k + 2\sqrt{r_k + 1}.$$

Now if K is real, then r_k=2, hence the field should have at-least **8** ramified primes.
Now when K is imaginary, then r_k=1, hence the field should have at-least **6** ramified primes.
So the following examples have infinite class field towers.

Example 1. $\mathbb{Q}(2.3.5.7.11.13.15.17)$

Example 2. $\mathbb{Q}(-2.3.5.7.11.13)$

Chapter 7

Conclusion

Class field theory is one of the most profound achievements of algebraic number theory in the recent past. As remarked in the thesis, it took around 50 years, where mathematicians across the world were able to provide a systematic and elegant framework to understand and study the theory. We denote some the recent developments related to this, in this chapter.

Non-abelian Class Field Theory: It was suggested by Takagi at ICM 1920, regarding the possibility of extending the theory to facilitate non-abelian extensions of the base field. After decades of inactivity in this regard, the area had a lot of activity since Langlands proposed his seminal Langlands program, often remarked as one of the Grand Unifying Theories of Mathematics. He conjectured the correspondence between finite dimensional representations of the Galois group and automorphic cuspidal representations of the General linear group of the Adele group. This gives non-abelian class field theory as a special case.

Explicit Class Field Theory: One striking difference from 3.3 and the rest of this thesis is that, the particular section tries to give an explicit description of the maps involved in Class Field Theory, where other chapters are more abstract. There is a lot of research in this regard, in relation with finding the explicit maps in different cases.

Hilbert's twelfth problem or Kronecker's Jugendtraum: We have a full description on the nature of abelian extensions of $\mathbb{Q}$. Hilbert, in his famous 1900 ICM address, posed if it is possible to determine the abelian extensions of any number field. Kronecker has remarked this as one of his most cherished dreams of youth and hence the name. The answer to some specific cases is known, but the general result is still unsolved. *Stark Conjectures*, a series of conjectures of given by Harold Stark in the 20th century is another topic in this regard.

Bibliography

[1] Cassels, J. W. S., and Fröhlich, A. , Algebraic number theory, Academic Press, 1967.

[2] Serre, Jean-Pierre. Local Fields, Springer-Verlag, 1979

[3] Weibel, Charles A., An introduction to homological algebra, Cambridge University Press, 1994.

[4] Neukirch, Jürgen.,Algebraic Number Theory, Berlin: Springer-Verlag, 1999.

[5] Dummit, David S., and Foote, Richard M. ,Abstract Algebra, Wiley, 2011.

[6] Milne, J.S.,Class Field Theory, Online notes on Class Field Theory.