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

Addanki Nagarjuna Chary
Roll No. 20131091

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

April, 2018

Supervisor: Dr. Ronnie Sebastian

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 Addanki Nagarjuna Chary at Indian institute of Technology, Bombay under the supervision of Dr. Ronnie Sebastian, Assistant Professor, Department of Mathematics, during the academic year 2017-2018.

Dr. Ronnie Sebastian

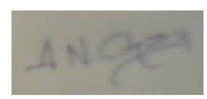
Committee:

Dr. Ronnie Sebastian

Dr. Manish Mishra

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, IIT Bombay, under the supervision of Dr. Ronnie Sebastian and the same has not been submitted elsewhere for any other degree.



Addanki Nagarjuna Chary

Abstract

Class Field Theory gives a one-one correspondence between the Galois groups of finite abelian extensions of a global field, k, and open subgroups of finite index in class group. This correspondence is captured by Reciprocity map and Existence theorem.
We first derive these theorems for local fields using Tate's theorem and Lubin-Tate Formal groups. From local case we go to global case using cohomology of Adeles and Ideles.

Contents

Introduction

In the first chapter we get introduced to the notion of valuation. This gives topological structure on a field. We read about the correspondence between the primes of $\mathbb{Q}$ and valuations on it. We study how these valuations extend to the extensions over $\mathbb{Q}$. In the second chapter we introduce Adeles and Ideles. We study the restricted topology on them and prove Dirichlet's theorem. In chapter 3 we read about the correspondence between the valuations in an extension to the primes in the extension. We also explicitly see how Galois group of the maximal unramified extension looks like.

In chapter 4 we study about Tate cohomology theory and profinite groups. These are basically tools we need to understand further chapters.

Chapter 5 and 6 are the most important part. Chapter 5 is Local class field theory, where we study the local reciprocity map and local existence theorem. We use Tate's theorem to prove the isomorphism but use Lubin-Tate Formal groups to explicitly give its description.

Chapter 6 is Global class field theory. We read about the cohomology of Ideles and prove two important inequalities. From these inequalities the reciprocity map and existence theorem follow.

Chapter 1

Valuations

1.1 Definitions

Definition 1.1. ***Valuation*** *on a field k is a map $||: k \to \mathbb{R}_{\geq 0}$ satisfying the conditions*

1. *$|a| = 0$ if and only if $a = 0$*
2. *$||: k^* \to \mathbb{R}_{>0}$ is a homomorphism*
3. *There exists constant C such that $|1 + a| \leq C$ for all $|a| \leq 1$*

We can define a topology k by taking open basic spheres $B_r(a) = \{x : |x - a| < r\}$. Two valuations are said to be equivalent if the topology induced by them is same.

Lemma 1.1. *Valuations $||_1$ and $||_2$ are equivalent if there exists a $c \in \mathbb{R}$ such that $|a|_1 = |a|_2^c$ for all $a \in k$.*

Proof. The statement boils down to proving that $|a|_1 < 1 \Leftrightarrow |a|_2 < 1$ if and only if there exists a $s \in \mathbb{R}$ such that $|a|_1 = |a|_2^s$. ($\Leftarrow$) case follows trivially.
Assume $|a|_1$ is non trivial and $|a|_1 < 1 \Leftrightarrow |a|_2 < 1$. Fix a $c \in k$ such that $|c|_1 > 1$. $|a|_1 = |c|_1^\alpha$ for some $\alpha \in \mathbb{R}$. Let $m/n \to \alpha^+$

$$|a|_1/|c|_1^{m/n} < |a|_1/|c|_1^\alpha = 1 \Rightarrow |a|_2/|c|_2^{m/n} < 1$$

Observe that the condition $|a|_1 < 1 \Leftrightarrow |a|_2 < 1$ can be restated as $|a|_1 > 1 \Leftrightarrow |a|_2 > 1$. This follows from the fact that $|a| < 1 \Rightarrow |a^{-1}| > 1$. Similarly if we consider $m/n \to \alpha^-$ we have

$|a|_2/|c|_2^{m/n} > 1$. Implying that $|a|_2/|c|_2^{\alpha} = 1$

$$log|a|_1/log|a|_2 = log_{|c|_2}|c|_1 \Leftrightarrow |a|_1 = |a|_2^{log_{|c|_2}|c|_1}$$

. □

Any valuation is equivalent to valuation where the constant in last inequality is 2. This can be seen by taking c in above lemma as $log_2 C$. Now from the fact $|1+a| \leq 2$ when $|a| \leq 1$ bi-implies $|a+b| \leq |a|+|b|$,refer pg43, [CF10]. We can replace the inequality in the definition by triangle inequality.

We define **Non archimedean** valuation by replacing the inequality with $|a+b| \leq max\{a,b\}$. This is equivalent to saying $n \leq 1$ for all $n \in k$. For a non archimedean valuation we define the set $\{x : |x| \leq 1\}$ as ring of integers denoted by $\mathfrak{o}$. Given $a, b \in \mathfrak{o}$ $|ab| = |a||b| \leq 1$ and $|a+b| \leq max\{|a|, |b|\}$. This shows that $\mathfrak{o}$ is a ring. The set $\mathfrak{p} = \{x : |x| < 1\}$ forms an ideal in $\mathfrak{o}$. $a \in \mathfrak{o}$ is unit if and only if $|a| = 1$. From this it implies that $\mathfrak{p}$ is set of all non units, hence maximal ideal. **Archimedean** valuation is defined to be valuation that is not non archimedean.
The valuation $||$ is called **discrete** if $log|a|$, for $a \neq 0$ forms a discrete additive subgroup of $\mathbb{R}$.

Lemma 1.2. *A non archimedean valuation is discrete if and only if the ideal* $\mathfrak{p}$ *is a principal ideal.*

Proof. Assume the valuation is discrete and $log|a|$ generates the additive subgroup. Then it is easy to observe that a generates the ideal. □

$(k, ||)$ is said to be complete if every cauchy sequence in k converges with respect to the metric induced by $||$. Let $\bar{k}$ denote a complete field. If $a \in \bar{k}$, $a = \lim a_n$ for $a \in k$. We define $|a| = \lim |a_n|$. Well definedness follows from the inequality

$$||a| - |b||_{\infty} \leq |a-b|$$

.

Lemma 1.3. *If* $\bar{k}$ *is completion of a discrete non archimedean valuation then the set of values* $||$ *taken on* k *and* $\bar{k}$ *are equal.*

Proof. Assume $a = \lim a_n$, from discreteness if $|a_n|$ are close enough there exists N such that for all $n, m \geq N$ $|a_n| = |a_m|$. □

1.2 Valuations on $\mathbb{Q}$

$|a|_\infty$ denotes the absolute value for $a \in \mathbb{Q}$. Given $x = a/b$ in $\mathbb{Q}$ for a prime p let $a/b = p^n a'/b'$ such that $p \not| a'b'$. We define p-adic valuation as $|a|_p = 1/p^n$. It is a trivial check to see that p-adic valuation is discrete and non archimedean.

Theorem 1.4 (Ostroswki's Theorem)**.** *Every valuation on $\mathbb{Q}$ is either equivalent to $||_\infty$ or $||_p$ for some prime p.*

Proof. Let $||$ be a non trivial valuation on $\mathbb{Q}$, we will prove separately in two cases

1. **Non archimedean**. $|n| \leq 1$ for all n. Since it is non trivial there exists a p such that $|p| < 1$. Define the set
$$A = \{a : |a| < 1\}$$
$p\mathbb{Z} \subset A$, since $p\mathbb{Z}$ is maximal $p\mathbb{Z} = A$. Any $a \in \mathbb{Q}$ takes the form $p^m b$, $p \not| b$ for some $m \in \mathbb{N}$.
$$|a| = |p|^m |b| = |p|^m = |a|_p^s, s = -mlog_p|p|$$

2. **Archimedean**. We know that given any two natural number m, n we have $|m|^{1/logm} = |n|^{1/logm}$. Let $|m|^{1/logm} = c$, then observe that $|x| = x^{lnc}$ for any $x > 0 \in \mathbb{Q}$

□

1.3 Finite Residue Fields

Let $||$ be a non archimedean discrete valuation and $\mathfrak{o}$, $\mathfrak{p}$ be its corresponding ring of integers and maximal ideal. We define residue field by $k_r = \mathfrak{o}/\mathfrak{p}$. In this section k_r is finite and $(k, ||)$ is complete. Let $\mathfrak{p} = (\pi)$. Every element $a \in k$ can be written uniquely as $u\pi^n$ for some unit u. Let a_i denote some fixed representatives of k_r throught this section.

Lemma 1.5.
$$k = \{\sum_{i=n}^{\infty} a_i \pi^i : n \in \mathbb{Z}\}$$

Proof. Observe that the sequence $b_n = \sum_{i=n}^{\infty} a_i \pi^i$ is a cauchy sequence hence converges in k. Consider a unit $u \in \mathfrak{o}$. Say image of u in k_r is $a_0 \neq 0$. Then $u - a_0 \in \mathfrak{p}$, say $u - a_0 = \pi^n u_1$ where u_1 is a unit. $u_1 - a_1 \in \mathfrak{p}$ for some representative a_1 and $u = a_0 + \pi^n u_1$. Continuing like this we can write every unit u as $\sum_{i=n}^{\infty} a_i \pi^i$. The theorem follows from the fact that every element $a \in k$ can be represented as $\pi^n u$ for some unit u. □

Theorem 1.6. $\mathfrak{o}$ *is compact. Consequently* k *is locally compact.*

Proof. We have shown that every element $a \in \mathfrak{o}$ can be written as $\sum_{i=0}^{\infty} a_i \pi^i$. Assume that $\{\mathfrak{o}_i\}$ is an open cover of $\mathfrak{o}$ without a finite subcover.

$$\mathfrak{o} = \cup_i a_i \mathfrak{o}$$

hence one of $a_i\mathfrak{o}$ is covered by infinitely many $\mathfrak{o}_i$, say $a_0\mathfrak{o}$. Again $a_0\mathfrak{o} = \cup_i(a_0 + a_i\mathfrak{o})$ we get a_1 such that $a_0 + a_1\mathfrak{o}$ is covered by infinitely many $\mathfrak{o}_i$. Continuing like this we get an $\alpha = a_0 + a_1\pi + ... \in \mathfrak{o}$. WLOG assume $\alpha \in \mathfrak{o}_1$. Since $\mathfrak{o}_1$ is open, for some n, $a_0 + ... + a_n\pi^n\mathfrak{o} \subset \mathfrak{o}_1$. This contradicts the construction of α that $a_0 + ... + a_n\pi^n\mathfrak{o} \subset \mathfrak{o}_1$ is covered by infinitely many $\mathfrak{o}_i$. This proves $\mathfrak{o}$ is compact. Any element $a \in k$ has open set $a.\mathfrak{o}$ which is compact. This proves the theorem. □

1.4 Extensions of Valuation

Let l be a finite field extension of k. We call a valuation $||_1$ on l an extension to $||$ on k if $|a|_1 = |a|$ for all $a \in k$. If k is complete then the extended valuation is unique. If not there are only finitely many extension to a given valuation. We prove these two statements in this section.
Let V be a finite dimensional vector space over k. We define **norm**($\|\ \|$) on V as a function $\|\ \| : V \to \mathbb{R}$ satisfying the conditions

1. $\|a\| = 0$ if and only if $a = 0$
2. $\|a + b\| \leq \|a\| + \|b\|$
3. $\|ab\| = |a|\|b\|$ for all $a \in k$ and $b \in V$

Example: Let ω_i be basis for V. We define $\|v\|_0 = \|\sum_i a_i\omega_i\| = max\{|a_i|\}$. If k is complete then under this norm V is complete. V can be given topology by using basic open sets as spheres $B(r, a) = \{x : n(a - x) < r\}$. Observe that l can seen as a vector space over k and extended valuation as a norm. Since basic open spheres are same the topology induced as a norm and valuation are also same.

Definition 1.2 (Equivalent norms)**.** *If there exists positive real numbers* c_1 *and* c_2 *for norms* $\|\ \|_1$ *and* $\|\ \|_2$ *such that* $\|a\|_1 \leq c_1\|a\|_2$ *and* $\|a\|_1 \geq c_2\|a\|_2$ *for all* $a \in V$ *then* $\|\ \|_1$ *and* $\|\ \|_2$ *are said to be equivalent.*

Observe that equivalent norms produce same topology on the vector space.

Lemma 1.7. *For a finite dimensional vector space V over a complete field $(k, ||)$ any two norms are equivalent.*

Proof. Let V be of dimension n with basis ω_i. We show that every norm on V is equivalent to absolute norm $\| \|_0$. Let $\| \|$ be a norm on V.

$$\|v\| \leq \sum_i |a_i| \|\omega_i\| \leq \|v\|_0 \sum_i \|\omega_i\|$$

This proves $\|v\| \leq c\|v\|_0$ where $c = \sum_i \|\omega_i\|$. To prove the other way around we use induction. $n = 1$ is obvious with $c = max\{\|\omega_i\|\}$. Assume it is true for $n-1$. Let $V_i = k\omega_1 + ..k\omega_{i-1} + k\omega_{i+1} + .. + k\omega_n$. V_i by induction hypothesis is complete so is $V_i + \omega_i$. Hence $V_i + \omega_i$ is closed in V. $0 \notin V_i + \omega_i$. Hence there exists $c > 0$ such that $\|v_i + \omega_i\| \geq c$ for all $v_i \in V_i$, for all i. Take $v = \sum_i a_i \omega_i$ and $\|v\|_0 = |a_i|$. $a_i^{-1} v \in V_i + \omega_i$ hence $\|a_i^{-1} v\| \geq c$. Thus we have

$$\|v\| \geq c\|v\|_0$$

□

Theorem 1.8. *Let l be a field extension over complete field $(k, ||)$ of dimension $n \in \mathbb{N}$. Then the valuation $||$ can be uniquely extended to l given explicitly by the formula*

$$|a|_1 = |N_{l/k}(a)|^{1/n}$$

Proof. From the previous lemma considering l as a finite dimensional vector space every norm induces the same topology. Since a valuation can be considered as a norm we see that any two valuations induce the same topology. So any two valuations satisfy $|a|_1 = |a|_2^c$. But if we take $a \in k$ we see that $c = 1$. This proves uniqueness.

$$f : l \to \mathbb{R}$$

$$a \to |N_{l/k} a|^{1/n}$$

is a continous function. The only thing left to prove thet f is a valuation is the triangle inequality . On since the set $S = \{a \in l : \|a\|_0 = 1$ is compact. There exists $c_1, c_2 > 0$ such that $c_1 \leq f(a) \geq c_2$ for all $a \in S$. This implies $c_1 \leq f(a)/\|a\|_0 \leq c_2$. For all $f(a) \leq 1 \leq c_2(\|1 + a\|_0) \leq c_2(1 + c_1^{-1})$. This proves that f is a valuation. □

But in the case of an incomplete field we have

Theorem 1.9. *Let l be a finite separable extension over k of degree n. There can be atmost N number of extension of $| \; |$. Let l_i be the completion of l with respect to valuation $\| \|_i$, for $i \leq N$. Then we have*

$$\bar{k} \otimes_k l \cong \oplus_i l_i$$

.

Proof. Let us first see that $\bar{k} \otimes_k l$ is of the form mentioned. Let $l = k[a]$ and $f_a(x) \in k[x]$ is minimal polynomial of a then $\bar{k} \otimes_k l = \oplus_{j=0}^{n-1} a^j k$. Let $f_a(x) = \prod_i g_i(x)$ where $g_i(x)$ are irreducible polynomials in $\bar{k}[x]$. Take $l_i \cong \bar{k}[x]/g_i(x)$. Fix a $a_i \in l_i$ such that $g_i(a_i) = 0$. Define homomorphism

$$\theta_i : \bar{k} \otimes_k l \to l_i$$

$$a \to a_i$$

$$\sum_j b_j a^j \to b_j a_i^j$$

If $\theta_i(h(x)) = 0$ then $g_i(x)|h(x)$.

$$\theta : \bar{k} \otimes_k l \to \oplus_i l_i$$

$$x \to \oplus_i \theta_i(x)$$

This map is clearly a surjection. If $\theta(h(a)) = 0$ then $g_i(x)|h(x)$ for all i, hence $f_a(x)|h(x)$ implying $h(a) = 0$. This proves that the map is an isomorphism. Now consider an $b \in l$, $x = \sum_j b_j a^j$ where $b_j \in k$.

$$\theta_i(b) = 0 \Rightarrow \sum_j b_j a_i^j = 0$$

$h(x) \in k[x]$ and . This proves that $\bar{k}$ and l have an inclusion into l_i. l_i as an extension over $\bar{k}$ has a unique extension of $| \ |$, say $\| \ \|_i$. By the inclusion $\theta_i : l \to l_i$ define va;uation $| \ |_i$ on l by

$$|a|_i = \|\theta_i(a)\|_i$$

If $||_i$ is non zero on say l_i, then for all $b \in l_i, \neq 0$ we have $|a|_i = |b|_i |ab^{-1}|_i$. Hence $|b|_i \neq 0$. If $||_i$ is non zero on any two of l_i say l_1 and l_2 we have for $a_i \in l_i$

$$(a_1, 0, ..., 0).(0, a_2, 0...0) = (0, 0, ...0)$$

$$\Rightarrow |a_1|_i |a_2|_i = 0$$

This is a contradiction, since both are non zero. Hence $||_i$ can be non zero only on one l_i. ∎

Chapter 2

Number Fields

Finite extension over $\mathbb{Q}$ is known as **Number** field. In this entire section k represents a finite extension over $\mathbb{Q}$. Since $\bar{\mathbb{Q}}_{||_\infty} = \mathbb{R}$, the extensions of archimedean valuations lie in $\mathbb{R}$ or $\mathbb{C}$. In archimedean case if the field lies in $\mathbb{R}$ then valuation is normalized if it is absolute value. In case of $\mathbb{C}$, if it is square of the absolute value. In non archimedean case we call $||$ normalized if $|\pi| = 1/|k_r|$. It is well defined since k_r is finite extension of some $\mathbb{Z}/p\mathbb{Z}$.
If $(\mathbb{Q}, ||)$ is complete then normalized extension of $||$ is $|N_{k/\mathbb{Q}}|$, pg59 [CF10]. In the incomplete case, let $||_i$ be normalized extensions then $\prod_i |a|_i = N_{k/\mathbb{Q}}a|$. This follows from the fact that norm is the constant in characteristic polynomial and $f(x) = \prod_i g_i(x)$.
In this entire section v denotes a normalized valuation.

Lemma 2.1. *For any $a \in k$, $|a|_v = 1$ for all most all v.*

Proof. Given any $a \in \mathbb{Q}$ we know that there are only finitely many primes dividing it. There for all most all primes $|a|_p = 1$. Now consider $a \in k$, there exists $a_i \in \mathbb{Q}$ such that

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

For any discrete non archimedean valuation v we have

$$|a|_v^n \leq max\{|a|^i|a_i|_v\}$$

If $|a|_v \geq 1$

$$|a|_v^n \leq |a|^{n-1} max\{|a_i|_v\}$$

$$|a| \leq max\{|a_i|\}$$

Thus we have $|a|_v \leq 1$ and $|a^{-1}|_v \leq 1$ for almost all v. □

Lemma 2.2. *Let v run through all the normalized valuations of k then we have*

$$\prod_v |a|_v = 1 \forall a \in k$$

Proof. Let $v|p$ for some p. We have already shown that $|a|_v = N_{k_v/\mathbb{Q}_p} a$. Thus from the corollary of last section we have

$$\prod_v |a|_v = \prod_p (\prod_{v|p} |a|_v) = \prod_p (\prod_{v|p} N_{k_v/\mathbb{Q}_p} a) = \prod_p N_{k/\mathbb{Q}} a$$

Since $N_{k/\mathbb{Q}} a \in \mathbb{Q}$ it comes down to proving the statement for $\mathbb{Q}$. Consider a $b \in \mathbb{Q}$. $b = \pm \prod p_i^{n_i}$ for some finitely many primes p_i. We have $|b|_{p_i} = p^{-n_i}$ and $|b|_\infty = \prod p_i^{n_i}$. Hence the lemma follows. □

2.1 Adeles and Ideles

For a number field$k$ let $\mathfrak{m}_k$ denote the set of all normalized valuations. Adele ring V_k is subset of $\prod_{v \in \mathfrak{m}_k} k_v$ such that given $a = (a_v) \in V_k$ $a_v \in \mathfrak{o}_v$ for almost all v. This topology is known restricted topology of k_v with respect to $\mathfrak{o}_v$. We define topology on V_k by taking the basis elements as

$$\prod_v O_v$$

where O_v is open in k_v and $O_v = \mathfrak{o}_v$ for almost all v.

Lemma 2.3. $V_k \cong V_{\mathbb{Q}} \otimes_{\mathbb{Q}} k$

Proof. This follows from $k \otimes_{\mathfrak{Q}} \mathfrak{Q}_p = \oplus_{v|p} k_v$ and $\oplus_i \omega_i \mathfrak{o} \cong \oplus_{v|p} \mathfrak{o}_v$ for almost all v, refer pg61 [CF10]. □

k can be seen as an element of V_k whose v^{th} component is k for all v. Thus we have an inclusion $k \to V_k$ and the images of k are known as principal adeles.

Lemma 2.4. *k^+ is discrete in V_k^+ and V_k^+/k^+ is compact.*

Proof. As seen earlier $V_k^+ \cong \oplus_i V_{\mathbb{Q}} \omega_i \cong \oplus_i V_{\mathbb{Q}}$. This implies $V_k^+/k^+ \cong \oplus V_{\mathbb{Q}}^+/\mathbb{Q}^+$. So it is enough to prove the statement for $\mathbb{Q}$.

For $\mathbb{Q}$ it is enough to show that we can find a neighborhood around 0 which is disjoint to $\mathbb{Q}$. By translation we can extend it to any neighborhood. Take the set $A = \big\{a \in V_{\mathbb{Q}} :$

$|a_\infty|_\infty < 1, |a_p|_p \leq 1$. A is open. If a rational number $q \in A$ since $|q_p|_p \leq 1$ for all p, $q \in \mathbb{Z}$. But $|q_\infty|_\infty < 1$ implies $q = 0$.

We construct a continous surjective map from a compact set to $V_{\mathbb{Q}}^+/\mathbb{Q}^+$. The continous image of compact set is compact, that proves the lemma. Consider a subset B of A where $|a_\infty|_\infty \leq 1$. Let $b \in V_{\mathbb{Q}}$, there are finitely many p such that $|b_p|_p > 1$. For such a p we have $b_p = s_p + r_p$ where $r_p \in \mathfrak{o}_p$. For all such p's the sum $s = \sum s_p \in \mathbb{Z}$. Thus we have $|b_p - s|_p \leq 1$ for all p. Now choose a r such that $|b_\infty - r - s|_\infty \leq 1/2$. Thus we have found $z = r + s \in \mathbb{Z}$ such that $b - z \in B$. We have constructed a surjective map from $B \to V_{\mathbb{Q}}^+/\mathbb{Q}^+$. □

As in the above proof we can similarly construct a compact set $W = \left\{\mathbf{a} \in V_k : |\mathbf{a}_v|_v \leq c_v\right\}$ for some constants c_v where $c_v = 1$ for almost all v. Satisfying the condition that every $\mathbf{a} \in V_k$ can be represented as $w + a$ where $w \in W$ and $a \in k$.

Theorem 2.5 (Weak approximation theorem)**.** *Let $|\ |_1, |\ |_2, \ldots |\ |_n$ be inequivalent valuations on k. Given $a_i \in k$ and $\epsilon > o$ there exists $a \in k$ such that*

$$|a - a_i|_i < \epsilon \quad \forall i$$

Proof. We use induction to construct x_i such that $|x_i|_i > 1$ and $|x_i|_j < 1$ for all $j \neq i$. For $n = 1$ say $|\ |_1$ and $|\ |_n$ are inequivalent. Then there exists a and b such that $|a|_1 < 1$, $|a|_n \geq 1$, $|b|_n < 1$ and $|b|_1 \geq 1$. $y = a/b$ satisfies the require condition that $|y|_1 < 1$ and $|y|_2 > 1$.
Now assume the statement is true for $n - 1$. So we have x such that $|x|_1 < 1$ and $|x|_j > 1$ for all $j \neq 1, n$.

1. If $|x|_n > 1$, take $t_m = x^m/1 + x^m$. Observe that $|t_m|_i \to 1$ for $i = 1, n$ and $|t_m|_i \to 0$ otherwise. Therefore for sufficiently large m we have $|t_m y| > 1$ and $|t_m y| < 1$ for all $i \neq 1$.

2. If $|x|_n < 1$ for sufficiently large m, $|x^m y|_1 < 1$ and $|x^m y|_i < 1$ for all $i \neq 1$.

Similarly we can construct x_i such that $|x_i|_i < 1$ and $|x_i|_j > 1$ for all $i \neq j$.

Let $z_{im} = x_i^m/1 + x_i^m$. Observe that

$$|z_{im} - 1|_i \to 0$$

$$|z_{im} - 0|_j \to 0,\ j \neq i$$

Let $z_m = \sum_i a_i z_{im}$

$$|z_m - a_i|_i \leq |a_i|_i |z_{im} - 1|_i + \sum_j |a_j|_i |z_{jm}|_i \to 0$$

Given ϵ we can find sufficiently large m and take a to be z_m to satisfy the required condition. □

Theorem 2.6 (Strong Approximation Theorem)**.** *Let w be a normalized valuation of k. S be a finite set of normalized valuations and $w \notin S$. Given $a_v \in k_v$ for all $v \in S$ and $\epsilon > 0$ there exists $a \in k$ such that $|a - a_v|_v < \epsilon$ for $v \in S$ and $|a|_v \leq 1$ for $v \notin S, \neq w$.*

Proof. Similar to the construction of B in the proof of compactness of V_k^+/k^+ we can construct a compact set $W = \{\mathbf{a} \in V - k : |a_v|_v \leq c_v\}$ for some constants $c_v = 1$ for almost all v such that every $\mathbf{a} \in V_k$ can be repersetned as $w + a$ where $w \in W$ and $a \in k$. We use the following lemma, pg66 [CF10],

Lemma 2.7. *For a number field k there is a corresponding constant $C > 0$ such that for $A \in V_k$ satisfying $\prod_{v \in \mathfrak{m}_k} |a_v|_v < C$. Thene there exists $b \in k$ such that $|b|_v \leq |a_v|_v$ for all v.*

Choose $a_v \in k_v$ such that $0 < |a_v|_v \leq c_v$ and $|a_v|_v = 1$ if $c_v = 1$. Choose $a_w \in k_w$ large enough that $\prod_{v \in \mathfrak{m}_k} |a_v|_v > C$.

So by above lemma there exists $b \in k$ such that

$$|b|_v \leq c_v^{-1}\epsilon, \ v \in S$$

$$|b|_v \leq c_v^{-1}, \ v \notin S, \neq w$$

Consider $\mathbf{a} \in V_k$ such that $\mathbf{a}_v = a_v, \ v \in S$ $\mathbf{a}_v = 0, \ v \notin S, \neq w$. There exists $b^{-1}\mathbf{a} = w + \beta$. $b\beta$ satisfies the required conditions.

□

The Idele group, J_k, is defined to be the set of all units of V_k. Define map

$$\tau : J_k \to V_k \times V_k$$

$$x \to (x, x^{-1})$$

J_k can be seen as a subset of $V_k \times V_k$ through this map. A subset O of J_k is said to be open if $\tau(O)$ is open in $\tau(J_k)$ with subset topology. It can be seen that this topology is equivalent to restricted product topology on k_v^* with respect to $\mathfrak{o}_v^*$.

$$J_k^1 := \left\{x \in J_k : \prod |x_v|_v = 1\right\}$$

Lemma 2.8. *Topology on J_k^1 as a subset of V_k is same as topology as a subset of J_k.*

Proof. Consider $\Gamma \subset J_k^{'}$ such that $\Gamma = O \cap J_k^{'}$ for an open set O in J_k and $1 \in \Gamma$. We want to find $U \subset V_k$ containing 1 such that $U \cap J_k^{'} \subset \Gamma$.

We may assume that if v is non archimedian then $\Gamma_v \subset \mathfrak{o}_v^*$. Further we may assume that if v is archimedean then $\Gamma_v = \{x \in k_v : |x-1| < \epsilon_v\}$. Choose a prime p such that for archimedean primes v we have

$$\prod_{v \in S_\infty} (1+\epsilon_v) < p$$

Take

$$U = \prod_{v \in S_\infty} \Gamma_v \times \prod_{v<p} \mathfrak{o}_p^* \times \prod_{v>p} \mathfrak{o}_v$$

If $(x_v) \in U \cap J_k^{'}$

$$\Rightarrow 1 = \prod_{v \in \mathfrak{m}_k} |x_v|_v = \prod_{v \in S_\infty} |x_v|. \prod_{v>p} |x_v|_v$$

$$\leq \prod_{v \in S_\infty} |x_v|_v/p \leq \prod_{v \in S_\infty} (1+\epsilon)/p < 1$$

This implies $x_v \in \mathfrak{o}_v^*$ for all $v > p$. Hence $U = \prod_{v \in S_\infty} \Gamma_v \times \prod_{v<p} \mathfrak{o}_p^* \times \prod_{v>p} \mathfrak{o}_v \subset \Gamma$

Now consider a subset W of $J_k^{'}$ open with respect to V_k topology. That is we have open set $\Gamma = \prod_{v \in S} \Gamma_v \times \prod_{v \notin S} \mathfrak{O}$ such that $W = \Gamma \cap J_k^{'}$. Γ contains open set $\Gamma^{'}$ of J_k given by $\prod_{v \in S} \Gamma_v \times \prod_{v \notin S} \mathfrak{o}_v^*$. Since $(x_v) \in W$ is a unit for all $v \notin S$, $W = \Gamma^{'} \cap J_k^{'}$. This proves the lemma. □

As a corollary we note

Corollary 2.9. *$J_k^{'}$ is closed in V_k.*

Proof. This follows from the fact that $J_k^{'}$ is kernel of the continous map

$$J_k \to \mathbb{R}$$

$$(x_v) \to \prod |x_v|_v$$

. □

Lemma 2.10. *J_k^1/k^* is compact*

Proof. We prove this by showing that J_k^1/k^* is continous image of a compact subset of $J_k^{'}$. Let $a \in V_k$ such that $\prod_{v \in \mathfrak{k}} |a_v|_v > C$ and $|a_v|_v = 1$ for almost all v. Consider the compact set $V = \{x \in V_k : |x_v|_v \leq |a_v|_v\}$.

Given a $x \in J_k^{'}$ there exists $b \in k$ such that $|b|_v \leq |x_v^{-1}.a_v|_v$ for all v. Thus we have $b.x \in V$. This defines a continous surjection

$$V \cap J_k^{'} \to J_k^{'}/k^*$$

$\square$

2.2 Dirichlet's Unit Theorem

Ideal class group, I_k, is defined to be set of formal sums of no archimedean valuations of k.

$$I_k \coloneqq \Big\{ \sum_v n_v v : v \in \mathfrak{m}_k \textit{ and non archimedean}, \ n_v \in \mathbb{Z} \Big\}$$

I_k is given discrete topology. There is natutal continous homomorphism $\upsilon : J_k \to I_k$

$$a = (a_v) \to \sum_{v \quad nonarch} v(a).v$$

The sum is finite since $a_v \in \mathfrak{o}_v^*$ for almost all v. $\upsilon(k^*)$ is known as group of principal ideals.

Lemma 2.11. *$I_k/\upsilon(k^*)$ is a finite group.*

Proof. $I_k/\upsilon(k^*)$ is continous image of the compact set J_k/k^*. Hence $I_k/\upsilon(k^*)$ is compact and discrete, so finite. $\square$

Theorem 2.12 (Dirichlet's Unit Theorem)**.** *For a finite set S of $\mathfrak{m}_k$ consisting of archimedean primes. The set $U_S \coloneqq \big\{ x \in k : |x|_v = 1 \ \forall \ v \notin S \big\}$ is direct sum of a finite cyclic group and free abelian group of rank $s-1$*

Proof. Define

$$J_{k,S} = \prod_{v \in S} k_v^* \times \prod_{v \notin S} \mathfrak{o}_v^*$$

$J_{k,S}^{'} \coloneqq J_{k,S} \cap J_k^{'}$. Since $J_{k,S}$ is an open subgroup of J_k, $J_{k,S}^{'}$ is an open subgroup of $J_k^{'}$. Hence $J_{k,S}^{'}/U_S = J_{k,S}^{'}/J_{k,S}^{'} \cap k^*$ is open subgroup of $J_k^{'}/k^*$. Hence is closed and compact. Consider the subset of $W \subset k^*$ defined by

$$c_1 \leq |x|_v \leq c_2, \ v \in S$$

$$|x|_v = 1, \ v \notin S$$

for some constants c_1 and c_2. This is the subset of compact subset of $V \subset J_k$ given by

$$c_1 \leq |x_v|_v \leq c_2,\ v \in S$$

$$|x_v|_v = 1,\ v \notin S$$

$V = W \cap k^*$, that is intersection of a compact set and a discrete set, hence is finite.

Take $c_1 = c_2 = 1$, these are elements in k^* which are units in every valuation. These contain the roots of unity. They also form a finite subgroup, hence are entirely roots of unity of some order.

Define

$$f : J_{k,S} \to \oplus_{i=1}^{s} \mathbb{R}^+$$

$$a \to \oplus_{i=1}^{s} log|a_i|_i$$

where $|\ |_i$ are valuations of S. This map is continous ans surjective. $f(J_{k,S}/ker(f))$ is subspace with $\sum_{i=1}^{s} x_i$ where $x_i \neq 0$. $f(J_{k,S}/ker(f))$ is $s-1$ dimensional subspace of $\oplus_{i=1}^{s}\mathbb{R}^+$. $f((J_{k,S}/ker(f))/(U_S/ker(f))) = f(J_{k,S}/U_S)$ is a compact subspace of this. Hence $f(U_S/ker(f))$ is free on $s-1$ element. Since $ker(f)$ restricted to U_S consists of x such that $|x|_v = 1$ for all v. We have U_S as direct sum of free abelian group generated by $s-1$ elements and a finite cyclic group consisting of roots of unity.

□

We note two important maps. l be a finite extension over k we define

1. Norm map.

$$N_{l/k} : V_l \to V_k$$

$$(N_{l/k}(a))_v = \prod_{w|v} N_{l_w/k_v} a_w,\ \forall\ a \in V_k$$

2. Conorm map.

$$Con_{l/k} : V_k \to V_k$$

$$(Con_{l/k}(a))_w = a_v,\ \forall\ w|v$$

If the context is clear we generally omit the l/k from the subscript.
Observe that $N_{l/k}U_l \subset U_k$ and $Con_{l/k}U_k \subset U_l$. Hence these definitions can be extended to J_k and I_k similarly. From the above definitions it follows that

$$N_{l/k} : I_l \to I_k$$

$$w \to e_{w/v} v$$

and

$$Con_{l/k} : I_k \to I_l$$

$$v \to f_{w/v} w$$

e is known as ramification index and f is extension degree of residue fields. These will be properly defined in the next chapter.

Chapter 3

Dedekind Domains

Throught this section R denotes an integral domain and K is the corresponding quotient field.

Definition 3.1 (Discrete additive valuation)**.** *A map $v : K \to \mathbb{Z} \cup \infty$ is a discrete valuation if,*

1. *v defines a surjective homomorphism $K^* \to \mathbb{Z}$*
2. *$v(0) = \infty$*
3. *$v(x + y) \geq inf\{v(x), v(y)\}$*

Observe that given $v(x)$ we can define a corresponding valuation $|x|_v := c^{v(x)}$ for some constant $c < 1$. This turns out be a discrete non archimedean valuation. we can choose c such that $||_v$ turns out to be a normalized valuation.

Definition 3.2. *Discrete valuation ring. Given a discrete valuation $v : K \to \mathbb{Z} \cup \infty$ discrete valuation ring is defined by the set $\{x \in K : v(x) \geq 0\}$*

This is same as $\mathfrak{o}$ of first chapter.

Theorem 3.1. *R is a discrete valuation ring if and only if it is noetherian, integrally closed and contains an unique prime ideal.*

Proof. ($\Leftarrow$) Let I be a non zero ideal of R, if $I/pI = 0$ by Nakayamma's lemma we have $I = 0$. Let $x \in I - pI$, since p is the only maximal ideal $Rad(x) = p$ and R is noetherian implies $\exists n$ s.t $Rad(x)^n = p^n \subset (x)$. Choose smallest n s.t

$$p^n I \subset p^n \subset (x) \subset I \subset p$$

take $a \in p^{n-1}I - (x)$ and define the map

$$\mu_{a/x} : p^n I \to p^n I$$

$$y \longmapsto ay/x$$

Observe $a/x(p^n I) \subset (1/x)p^n I p^{(n-1)} I$, if $1/xp^n I = R \Rightarrow p^n I = (x) \Rightarrow x \in pI$ hence $1/xp^n I \subset p$. Therefore this map satisfies an equation

$$\mu_{a/x}^n + a_1 \mu_{a/x}^{n-1} + ... + a_n = 0$$

$$\Rightarrow (a/x)^n + a_1(a/x)^{n-1} + ... + a_n) = 0 \Rightarrow a/x \in R$$

We have $a \in (x)$, contradiction, therefore $n = 0 \Rightarrow (x) = I$. We showed R is a PID hence a UFD, if $p = (\pi)$ since p is the only nonzero prime ideal every $x \in R$ admits a unique representaion $\pi^n u$ where $u \in R - p$ i.e, u is a unit in R. Define

$$v : R \to \mathbb{Z}_{\geq 0}$$

$$x = \pi^n u \longmapsto n$$

Now assume that R is a dvr corresponding to the discrete valuation v.

$$v(1) = v(1.1) = v(1) + v(1) \Rightarrow v(1) = 0$$

Take $u, v \in R$ s.t $uv = 1$

$$\Rightarrow v(xy) = v(x) + v(y) = 0 \Rightarrow v(x) = v(y) = 0$$

Since $v(x), v(y) \geq 0$. Observe that

$$v(u) = 0 \Rightarrow v(1/u) = 0 \Rightarrow (1/u) \in R$$

Therefore $u \in R$ is a unit iff $v(x) = 0$. Consider the set $\{x \in R : v(x) > 0\}$. The properties of valuation show that its an ideal and since its the set of all nonunits its the unique maximal ideal. Since R is a PID its noetherian and Integrally closed. □

A fractional ideal J of R is R submodule of K s.t $\exists a \in K$ s.t $aJ \subset R$. For a fractional ideal J we define $J^{-1} = \{x \in K : xJ \subset R\}$. Observe that J^{-1} is an R submodule and for any nonzero $a \in J$, $aJ^{-1} \subset R$ making J^{-1} a fractional ideal.

If M is Rsubmodule of K then $M_{\mathfrak{p}} = MR_{\mathfrak{p}}$ is $R_{\mathfrak{p}}$-module and if M is finitely generated then $M_{\mathfrak{p}}$ is finitely generated over a PID. Consider M, N, free $R-$submodules of K of rank n. There exists a linear transormation l of K s.t $lM = N$. We define $[M : N]$ as fractional ideal $Rdet(l)$. If M, N are finitely generated, then $[M : N]$ is defined to be the unique ideal $[M : N]$ s.t

$$[M_{\mathfrak{p}} : N_{\mathfrak{p}}] = [M : N]R_{\mathfrak{p}} \forall \mathfrak{p}$$

This definition of $[M : N]$ is well defined only if $[M_{\mathfrak{p}} : N_{\mathfrak{p}}] = R_{\mathfrak{p}}$ for almost all $\mathfrak{p}$. Since M, N are finitely generated, we have $a, b \in K$ such that $aM \subset N \subset bM$. Since $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(b) = 0$ for almost all $\mathfrak{p}$, $M_{\mathfrak{p}} = N_{\mathfrak{p}}$ for almost all $\mathfrak{p}$. L be a seperable extension of K and S be the integral closure of R in L. Let $t_{L/K}$ denote the trace map on L, since L is seperable over K, $t_{L/K}$ defines a nondegenarate bilinear form on L. For any R submodule N of L we define $D_R(N) = \{x \in L : t_{L/K}(xN) \subset R\}$.

Lemma 3.2. *If N is a free R submodule of L then $D_R(N)$ is a free R submodule.*

Proof. Let $\{a_i\}$ be basis for N over R. Since $t_{L/K}$ is nondegenerate if $\{b_i\}$ is dual basis of $\{a_i\}$ then $D_R(N)$ is freely generated by $\{b_i\}$. □

Lemma 3.3. *If M is a free Rsubmodule of S with basis $\{u_i\}$ then $\mathfrak{d}(M)$ defined by $[D_R(M) : M]$ is generated by $det(t_{L/K}(u_iu_j))$*

Proof. Assume M is generated by $\{u_i\}$ and $D_R(M)$ by the dual basis $\{v_i\}$. Define

$$l : L \to L$$

$$v_i \longmapsto u_i$$

this takes $D_R(M)$ to M. Fix $\{v_i\}$ as basis for L then

$$l(v_i) = u_i = a_{i1}v_1 + ...a_{in}v_n$$

$t_{L/K}(u_iv_j) = 0$ if $i \neq j$ and $t_{L/K}(u_iv_j) = 1$ if $i = j$ hence

$$t_{L/K}(u_iu_j) = a_{ij}$$

Hence $[D_R(M) : M] = Rdet(t_{L/K}(u_iu_j))$ □

Theorem 3.4. *S is a finitely generated R module that spans L over K and is a dedekind domain.*

Proof. If $x \in L$ then $x = s/r$ for some $s \in S$ and $r \in R$. x satisfies a polynomial

$$x^n + a_{n-1}x^{n-1} + ... + a_0 = 0$$

if $a_i = b_i/c_i$ consider $r^n = (\prod a_i)^n$

$$(rx)^n + r^1a_{n-1}(rx)^{n-1} + ... + r^na_0 = 0, r^ia_{n-i} \in R$$

hence $rx \in S$, this implies $SK = L$. $x \in S$ if and only if $R[x]$ is finitely genererated R module, from this it follows that S is an R module.

S contains a free N module that spans L. From the definition of $D_R(N)$ it is easy to see that $S \subset D_R(S) \subset D_R(N)$. $D_R(N)$ is a free module over a noetherian ring(R), hence noetherian. Thus S as R submodule of $D_R(N)$ is noetherian. Since S is integrally closed, if α is inegral over S and satisfies $x^n + a_{n-1}x^{n-1} + .. + a_0$, $a_i \in S$ then α is finitely generated over $R[a_{n-1}, .., a_0]$. Thus α is finitely generated over R hence $\alpha \in S$. Let $\mathfrak{P}$ be a prime ideal in S and $\mathfrak{P} \cap R = \mathfrak{p}$. Consider an element $\alpha \in S - \mathfrak{P}$ that satisfies

$$x^n + a_{n-1}x^{n-1} + ... + a_0 = 0, a_i \in R$$

then $\overline{\alpha}$ satisfies

$$x^{n-i} + \overline{a}_{n-1}x^{n-i-1} + ... + \overline{a}_i = 0, \overline{a}_i \in R/\mathfrak{p}$$

for some $1 \leq j < n$. Rewriting it after substituting $\overline{\alpha}$ we have

$$\overline{\alpha}(\overline{\alpha}^{n-i-1} + \overline{a}_{n-1}\overline{\alpha}^{n-i-2} + ... + \overline{a}_{i+1})\overline{a}_i{}^{-1} = 1$$

. Thus we found an inverse for non zero element in $S/\mathfrak{P}$, making $\mathfrak{P}$ a maximal ideal. This completes the proof that S is a dedekind domain. □

It also follows from Hensel's lemma that $S = \{x \in L : N_{L/K}(x) \in R\}$. Since we have shown that $N_{L/K}$ is a normalized valuation, the maximal prime ideal of S corresponds to the normalized extension of the valuation corresponding to R.

$S/\mathfrak{p}S$ as a vectorspace over k is isomorphic to $S/\mathfrak{P} \oplus \mathfrak{P}^1/\mathfrak{P}^2 \oplus .... \oplus \mathfrak{P}^{e-1}/\mathfrak{P}^e$. We have $S/\mathfrak{P} \cong \mathfrak{P}/\mathfrak{P}^2$ by the map $s \longmapsto s\pi_L$, similarly $\mathfrak{P}^i/\mathfrak{P}^{i+1} \cong \mathfrak{P}^{i+1}/\mathfrak{P}^{i+2}$ for all $i \leq e-2$. If $\overline{x}_1, \overline{x}_2....\overline{x}_f$ is basis of $S/\mathfrak{P}$ over $R/\mathfrak{p}$ then $\pi^i\overline{x}_1, \pi^i\overline{x}_2....\pi^i\overline{x}_f$ is basis of $\mathfrak{P}^i/\mathfrak{P}^{i+1}$ over $R/\mathfrak{p}$, $\overline{x}_i \in k_L$. Consider $N = Rx_1 + ... + Rx_f + ... + Rx_1\pi^{e-1} + ... + Rx_f\pi^{e-1}$ then $S = \mathfrak{p}S + N$, by Nakayama's lemma, $S = N$. Hence $\{\pi^j x_i\}$ $1 \leq j \leq e-1, 1 \leq i \leq f$ forms a basis for L over K.

Consider a pair of dedekind domains R_1, R_2 with quotient fields K_1,K_2 respectively s.t $R_1 \subset R_2$. If $\mathfrak{p}_2$ is a prime ideal in R_2 and the prime ideal $\mathfrak{p}_1 = \mathfrak{p}_2 \cap R_1$ is also nonzero then we define residue class degree $f(\mathfrak{p}_2/\mathfrak{p}_1) = (k_2 : k_1)$, where $k_i = R_i/\mathfrak{p}_i$. The ramification index is defined by $e(\mathfrak{p}_2/\mathfrak{p}_1) = v_{\mathfrak{p}_2}(\mathfrak{p}_1 R_1)$. From here assume that R is d.v.r and K is complete. Let $\mathfrak{p}$ and $\mathfrak{P}$ denote the prime ideals of R and S respectively.We define residue class degree of $\mathfrak{P}, f$ as $k_L : k$ where $k_L = S/\mathfrak{P}$ and $k = R/\mathfrak{p}$.

Lemma 3.5. *$ef = [L : K]$*

Proof. $\mathfrak{P}^{i+1}$ is maximal ideal in $\mathfrak{P}^i$. We have $S/\mathfrak{P} \cong \mathfrak{P}/\mathfrak{P}^2$ by the map $s \longmapsto s\pi_L$. Similarly we have $\mathfrak{P}^i/\mathfrak{P}^{i+1} \cong \mathfrak{P}^{i+1}/\mathfrak{P}^{i+2}$ for all $i \leq e-2$. Since S is a free R moduke of rank $[L : K]$, dimension of $S/\mathfrak{p}S$ is $[L:K]$. lemma follows from the fact that $S/\mathfrak{p}S$ as a vectorspace over k is isomorphic to $S/\mathfrak{P} \oplus \mathfrak{P}^1/\mathfrak{P}^2 \oplus .... \oplus \mathfrak{P}^{e-1}/\mathfrak{P}^e$ □

Definition 3.3. *Finite seperable extension L over K is said to be **Unramified** if $e(L/K) = 1$ and k_L is seperable over k*

An *eisenstein polynomial* in $K[X]$ is a seperable polnoymial

$$E(x) = x^n + a_{m-1}x^{n-1} + ... + a_0$$

where $v_K(a_i) = 1$ for all $1 \leq i \leq n-1$ and $v_K(a_0) = 1$

Lemma 3.6. *$E(x)$ is an irreducible polynomial.*

Proof. Assume $E(x)$ is not irreducible amd $x^n + a_{n-1}x^{n-1} + ... + a_0 = (x^m + ... + b_0)(x^{n-m} + ... + c_0)$. Since $b_0c_0 \in \mathfrak{p}$ assume WLOG $b_0 \notin \mathfrak{p}$ and c_{n-i} be the smallest c_i s.t $c_i(mod\mathfrak{p}) \neq 0$

$$a_i = b_0c_{n-i} + ...b_{n-i}c_0$$

$$a_i - b_1c_{n-1-i} + ...b_{n-i}c_0 = b_0c_{n-i}$$

$\mathfrak{p}$ divides LHS above but not RHS, hence $E(x)$ is irresucible. □

We state a very useful lemma without proof.

Lemma 3.7 (Hensel's Lemma). *Let R is a complete local ring, $\mathfrak{p}$ be it's prime ideal and $k = R/\mathfrak{p}$. Let $f(x) \in R[x]$ be a monic polynomial and $f(x) \equiv \overline{f}(x)(mod\mathfrak{p})$. If $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ where $(\overline{g}(x), \overline{h}(x)) = 1$ then there exists unique $g(x), h(x) \in R[x]$ such that $f(x) = g(x)h(x)$, $h(x) \equiv \overline{h}(x)(mod\mathfrak{p})$ and $g(x) \equiv \overline{g}(x)(mod\mathfrak{p})$*

In the case of finite separable extension L over a local field K where S is integral closure of R in L. If $\overline{f}(x)$ were separable and $\overline{f}(\overline{\alpha}) = 0$ for some $\overline{\alpha} \in k_L$ then the lemma says that there exists a unique $\alpha \in S$ such that $f(\alpha) = 0$ and $\alpha \equiv \overline{\alpha}(mod(\mathfrak{P}))$.

Proposition 3.8. *Suppose L is an unramified extension over K. Then there exists an element $x \in S$ with $k_L = k[\overline{x}]$. If x is such an element and $g(x)$ is it's minimal polynomial over K, then $S = R[x]$, $L = K[x]$ and $\overline{g}(x)$ is irreducible in $k[x]$ and separable.*

Proof. Since k_L is seperable over k, $k_L = k[\overline{\alpha}$ for some $\overline{\alpha} \in k_L$. Let $f(x)$ be minimal polynomial of $\overline{\alpha}$ in $k(x)$. $F(x) \in S[x]$ such that $F(x) = f(x)$. Since $f(x)$ is irreducible $F(x)$ is irreducible, otherwise going mod for the factorization of $F(x)$ gives us a factorization of

$f(x)$. Since $f(x)$ is separable we can apply Hensel's lemma to get a unique $\alpha \in S$ such that $\alpha = \overline{\alpha}$ and $F(\alpha) = 0$.

$$[L : K] \geq degree(F(x)) \geq degree(f(x)) = [k_L : k] = [L : K]$$

Thus we have degree$(F(x)) = [L : K]$, hence $L = K[\alpha]$. $k_L = k \oplus k\overline{\alpha} \oplus ... \oplus k\overline{\alpha}^{n-1}$, by Nakayama's lemma we can lift the basis to S and we get $S = R \oplus R\alpha \oplus ... \oplus R\alpha^{n-1}$. □

Proposition 3.9. *Suppose $g(x)$ is a monic polynomial in $R[x]$, such that $\overline{g}(x)$ is irreducible in $k[x]$ and separable. If x is a root of $g(x)$ then $L = K[x]$ is unramified over K and $k_L = k[x]$.*

Proof. Since $\overline{g}(x)$ is irreducible and separable degree$(g(x))$ = degree$(\overline{g}(x))$. Thus we have

$$[L : K] = degree(g(x)) = degree(\overline{g}(x)) \leq [k_L : k] \leq [k_l : k]$$

Hence $[L : K] = [k_l : k]$ and $k_L \cong k[x]/\overline{g}(x)$. If α is a root of $g(x)$ then $L = K[\alpha]$ and $k_L = k[\overline{\alpha}]$. □

Theorem 3.10. *given $\overline{k}$ a finite seperable extension of k there exists a finite seperable extension $L = L(\overline{k})$ over K, such that*

1. *$\overline{k} \cong k_L$*
2. *L is unramified over K*
3. *the canonical map is bijective*

$$Hom_K(L, K) \longrightarrow Hom_k(k_L, k)$$

Proof. $\overline{k} = k[\overline{\alpha}]$ for some $\alpha \in \overline{k}$. assume $\overline{\alpha}$ satisfies

$$\overline{g(x)} = x^n + \overline{a}_{n-1}x^{n-1} + ... + \overline{a}_0, \overline{a}_{n-i} \in k$$

consider $g(x) = x^n + a_{n-1}x^{n-1} + ... + a_0 \in K[X], a_i \equiv \overline{a}_i mod(\mathfrak{p})$ since $\overline{g(x)}$ is seperable and irreducible $g(x)$ is seperable and irreducible. Consider any L s.t $L \cong K[X]/g(x)$, by hensel's lemma there exists an unique $\alpha \in L$ s.t $\alpha \equiv \overline{\alpha} mod(\mathfrak{p})$ and $g(\alpha) = 0$. Hence we have $k_L \cong k[X]/\overline{g(x)} \cong \overline{k}$ and also $[L : K] = [k_L : k]$ since degree of $\overline{g(x)} = g(x)$ making L unramified extension.

we are left to prove the bijection of canonical map given

$$\overline{f} : k[\overline{\alpha}] \to k_{L'}$$

$$\overline{\alpha} \longmapsto \overline{\beta}$$

assume $\overline{\alpha}, \overline{\beta}$ satisfy $\overline{g(x)} = x^n + \overline{a}_{n-1}x^{n-1} + ... + \overline{a}_0$. If there exists β_1, β_2 s.t $g(\beta_1) = g(\beta_2) = 0$ where $g(x) = x^n + a_{n-1}x^{n-1} + ... + a_0$ and $\overline{\beta}_1 = \overline{\beta}_2 = \overline{\beta}$ then $\overline{g(x)}$ is not seperable. Hence there exists a unique $\beta \in L^{'}$ s.t $g(\beta) = 0$ and $\overline{g(\overline{\beta})} = 0$. This defines a unique homomorphism

$$f : L \to L^{'}$$

$$\alpha \longmapsto \beta$$

whose restriction to $k[\overline{\alpha}]$ defines $\overline{f}$ □

Theorem 3.11. *Composite of two unramified extensions is unramified*

Proof. Let $L_1 = K[\alpha], L_2 = K[\beta]$ be unramified extensions such that $k_{L_1} = k[\overline{\alpha}], k_{L_2} = k[\overline{\beta}]$. Assume $f(x) \in K[X]$ is minimal polynomial of α in $K[x]$ but it may split in $L_2[x]$. Say $f(x) = \prod h_i(x)$ where $h_i(x) \in L_2[X]$ are irreducible and $h_1(\alpha) = 0$. Since $\overline{f(x)}$ is seperable, $\overline{h_1(x)}$ is seperable in k_{L_2}. $\overline{h_1(x)}$ is also irreducible in k_{L_2}, if not assume $\overline{h_1(x)} = \overline{g(x)h(x)}$. Since $\overline{h_1(x)}$ is separable $(\overline{g(x)}, \overline{h(x)}) = 1$ by Hensel's lemma we can find $g(x), h(x)$ such that $h_1(x) = g(x)h(x)$ which gives us a contradiction. Thus by proposition3 $L_2[\alpha] \cong L_2[X]/h_1(x)$ is unramified over L_2, hence over K. Thus $L_1L_2 = L_2[\alpha]$ is unramified over K. □

Thus taking compositum of all umramified extensions we get a maximal unramified extension of K in its algebraic closure denoted by K_nr

Lemma 3.12. *If L is unramified extension and σ is an automorphism of L then σL is unramified extension*

Proof. Assume $L = K[\alpha]$, $\sigma(\alpha) = \beta$ and $g(x) \in K[X]$ be the minimal polynomial of α and β. BY theorem4 we have a unique homomorphism

$$\overline{\sigma} : k_L \to k_{\sigma L}$$

$$\overline{\alpha} \longmapsto \overline{\beta}$$

Since $\overline{\beta}$ is root of $\overline{g}(x)$ which is irreducible and seperable, $[k_{\sigma L} : k] \geq$ degree$\overline{g}(x)$. Hence $[\sigma L : K] \geq [k_{\sigma L} : k] \geq [k_L : k] = [L : K] = [\sigma L : K]$. This proves that σL is unramified. □

Given a seperable extension L over K let L_0 denote the composite of all unramified extensions over K in L. Since σL_0 is unramified, L_0 is normal. Consider $L^{'} = L(k^s)$ which is an unramified extension, hence $L^{'} \subset L_0$. Thus $k^s \subset k_{L_0}$, but k_{L_0} is seperable, hence $k^s = k_{L_0}$

Lemma 3.13. *Adjoining e^{th} roots of unity to K where $(e, p) = 1$ is an unramified extension.*

Proof. Let ζ_e denote the primitive e^{th} roots of unity with minimal polynomial $f(x)$ in $R[x]$. Since $x^e - 1$ is separable in k_{ζ_e}, $\overline{f}(x) \in k_{\zeta_e}$ is separable. Since it's separable and $f(x)$ is irreducible by Hensel's lemma we conclude that $\overline{f}(x)$ is irreducible.Applying proposition2 K_{ζ_e} is unramified over K. □

Theorem 3.14. *Every unramified extension of degree n is given by adjoining $q^n - 1th$ roots of unity where $q = \#k$*

Proof. Assume L is an unramified extension by theorem3 we have $Gal(L/K) \cong Gal(k_L/k)$. $x^{q^n} - x$ is seperable in k_L hence by Hensel's lemma L contains $(q^n - 1)$th roots of unity, ζ_{q^n-1}. By applying above lemma $L^{'} = K[\zeta_{q^n-1}]$ is unramified extension of degree n in over K and $L^{'} \subset L$, hence $L = L^{'}$. □

Chapter 4

Tate's Cohomology and Profinite Groups

4.1 Tate's Cohomology

Throught this section let G be a finite group. For $i > 0$, $Z_i \coloneqq \mathbb{G}^{i+1}$, $G^{i+1} = G \times G \times .... \times G$, $i+1$ times. For a G module A, $Hom(G, A)$ can be given module structure by $(g.f)(x) \coloneqq g.f(g^{-1}x)$. We denote $Hom(G, A)^G = \left\{ f \in Hom(G, A) : g.f = f \ \forall g \in G \right\}$ by $Hom_G(G, A)$. G always acts trivially on $\mathbb{Z}$.

$$d_{i-1} : Z_i \to Z_{i-1}$$

$$(g_0, g_1, ..., g_i) \to \sum_{j=0}^{i} (-1)^j (g_0, g_1, ..., g_i)$$

This is a G module homomorphism. $Z_{-i} = Hom(Z_{i-1}, \mathbb{Z})$

$$d_{-i} : Z_{-i} \to Z_{-i-1}$$

Take $f \in Hom(\mathbb{Z}[G^i], \mathbb{Z})$ we define

$$d_{-i}.f(g_0, g_1, ..., g_i) = f(d_{i-1}(g_0, g_1, ..., g_i))$$

By the above definitions we have the exact sequence

$$\to Z_1 \xrightarrow{d_0} Z_0 \xrightarrow{\epsilon} Z_{-1} \xrightarrow{d_{-1}} Z_{-2} \to$$

$$\epsilon : Z_0 \to Z_{-1}$$

$$\sum a_i g_i \to \sum a_i . \sum g_i$$

This exact sequence is known as a standard complex. This induces a chain

$$\xrightarrow{d_{-2}} Hom_G(Z_{-2}, A) \xrightarrow{d_{-1}} Hom_G(Z_{-1}, A) \xrightarrow{\epsilon} Hom_G(Z_0, A) \xrightarrow{d_1} Hom_G(Z_1, A) \xrightarrow{d_2}$$

$$d_q : Hom_G(Z_{q-1}, A) \to Hom_G(Z_q, A)$$

$$d_q.f(g_0, g_1, ..., g_q) = f(d_q g_0, g_1, ..., g_q)$$

These are G module homomorphisms. For a G module A Tate's groups are defined as

$$\hat{H}^q(G, A) = ker(d_q)/img(d_{q-1}) \; \forall q \in \mathbb{Z}$$

Elements of $ker(d_q)$ are known as q-cocycles and of $img(d_{q-1})$ are know as $q-1$ cochains. Let $H^q(G, A)$ denote the q^{th} cohomology groups and $H_q(G, A)$ denote the q^{th} homology groups. $N : A \to A$, $a \to \sum g.a$ induces $N : H_0(G, A) \to H^0(G, A)$. We define $\hat{H}_0(G, A) = ker(N)$. It can be seen that

$$\hat{H}^q(G, A) = \hat{H}^q(G, A), \; q \geq 1$$

$$\hat{H}^{-1}(G, A) = \hat{H}_0(G, A)$$

$$\hat{H}^{-q} = H_{q-1}(G, A)$$

For an exact sequence of G modules

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

we have the exact sequence

$$\to \hat{H}^q(G, A) \to \hat{H}^q(G, B) \to \hat{H}^q(G, C) \xrightarrow{\delta} \hat{H}^{q+1}(G, A) \to$$

δ above is known as connecting homomorphism.

Let H be a subgroup of G then we have embedding $f : H \to G$. This induces map known as restriction homomorphism

$$Res : \hat{H}^q(G, A) \to \hat{H}^q(G, A)$$

If H is a normal subgroup then A^H is a G/H module. $G \to G/H$ induces $\hat{H}^q(G/H, A^H) \to \hat{H}^q(G, A^H)$. $A^H \to A$ induces $\hat{H}^q(G, A^H) \to \hat{H}^q(G, A)$. Thus we have the inflation map

$$Inf : \hat{H}^q(G/H, A^H) \to \hat{H}^q(G, A)$$

For Homology groups we can also define corestriction map induced by $H \to G$

$$cor : H_q(H, A) \to H_q(G, A)$$

This can be extended to all Tate's groups by dimension shifting, pg104 [CF10]. We note an important lemma, pg101 [CF10]

Lemma 4.1. *If $\hat{H}^i(G, A) = 0$ for all $1 \le i \le q-1$ for some $q > 1$ then the following sequence is exact*

$$0 \to \hat{H}^q(G/H, A^H) \xrightarrow{inf} \hat{H}^q(G, A) \xrightarrow{res} \hat{H}^q(H, A)$$

Lemma 4.2 (**Shapiro's lemma**)**.** *Let B be a H module, then*

$$\hat{H}^q(G, Hom_H(\mathbb{Z}[G], B)) = \hat{H}^q(H, B)$$

Proof. Define

$$f : Hom_G(Z, Hom_H(\mathbb{Z}[G], B)) \to Hom_H(Z, B)$$

For $\psi \in Hom_G(Z, Hom_H(\mathbb{Z}[G], B))$, $f(\psi)(g) := \psi(g)(1)$. The lemma follows from the fact that it is an isomorphism. □

Definition 4.1 (Cup product)**.** *There exists a unique family of homomorphisms in $\hat{H}^{p+q}(G, A \otimes B)$ denoted by $a.b$ for $a \in \hat{H}^p(G, A)$ and $b \in \hat{H}^q(G, B)$ written as*

$$\hat{H}^p(G, A) \otimes \hat{H}^q(G, B) \to \hat{H}^{p+q}(G, A \otimes B), \ \forall \, p, q \in \mathbb{Z}$$

satisfying

1. *These homomorphisms are funcorial in A and B.*
2. *For $p = q = 0$ they are induced by $A^G \otimes B^G \to (A \otimes B)^G$.*
3. *If $0 \to A_1 \to A_2 \to A_3 \to 0$ and $0 \to A_1 \otimes B \to A_2 \otimes B \to A_3 \otimes B \to 0$ then for $a_3 \in \hat{H}^p(G, A_3)$ and $b \in \hat{H}^q(G, B)$ we have $(\delta(a_3)).b = \delta(a_3.b)$*
4. *If $0 \to B_1 \to B_2 \to B_3 \to 0$ and $0 \to A \otimes B_1 \to A \otimes B_2 \to A \otimes B_3 \to 0$ then for $a \in \hat{H}^p(G, A)$ and $b_3 \in \hat{H}^q(G, B_3)$ we have $a.(\delta.b_3) = (-1)^p \delta(a.b_3)$*

From pg108 of [CF10] we note the lemma

Lemma 4.3. *1. $Res(a.b) = Res(a).Res(b)$*

2. $Cor(a.Res(b)) = Cor(a).b$

For a finite cyclic group G we have the theorem

Theorem 4.4. *$\hat{H}^2(G,\mathbb{Z})$ is cyclic and the cup product with the generator induces an isomorphism*

$$\hat{H}^q(G,A) \to \hat{H}^{q+2}(G,A)$$

For a finite cyclic group G if $\hat{H}^0(G,A)$ and $\hat{H}^1(G,A)$ are finite then we define Herbrand Quotient, $h(G,A)$, by $[\hat{H}^0(G,A)]/[\hat{H}^1(G,A)]$.

4.2 Profinite Groups

Let I be a set with a relation $\leq$ which is reflexive and transitive. Inverse system over I is $\{G_i\}$ indexed over I with continous homomorphism $\theta_i^j : G_j \to G_i$ for all $i \leq j$ satisfying $\pi_i^i = 1$ and $\pi_i^j \circ \pi_j^k = \pi_i^k$.

Let G_i be finite sets with discrete topology. $G \coloneqq \{(a_i) \in \prod_{i\in I} G_i : \pi_i^j(a_j) = a_i\}$. G is closed in $\prod G_i$(product topology). We denote $G = \varprojlim G_i$ and call it a profinite group(G_i are finite).

Theorem 4.5. *A topological group is profinite if and only if it is compact and totally disconnected.*

Proof. Consider $G = \varprojlim G_i$. G_i are finite and discrete hence compact, so is $\prod G_i$. Since G is closed, it is compact. To prove it is totally disconnected it is enough to show that intersection of all compact subgroups is 1. Let $G_i^{'}$ denote the subset of $\prod G_i$ containg 1 at G_i component. $\cap G_i^{'} = 1$, hence $\prod G_i$ is totally disconnected which follows to G.

Let G be a compact and totally disconnected set. Let G_i be collection of open normal subgroups. The natural maps $G/G_j \to G/G_i$ for $G_j \subset G_i$ make it an inverse system. Let

$$\mu : G \to \varprojlim G/G_i$$

$$x \to xG_i$$

Injectivity follows from the fact that every neighborhood of 1 contains a normal subgroup. If $a = (a_iG_i)$ then $\cap a_iG_i$ is non empty. This shows surjectivity. Restriction to G/G_i is continous, hence θ is continous. Thus we have shown that if G is a profinite group and G_i are open normal subgroups then $G = \varprojlim G/G_i$ □

Thus from above theorem it follows that if l/k is a Galois extension and l_i are intermediate fields $G(l/k) = \varprojlim G(l_i/k)$. From theorem 3.14 $Gal(k_{ur}/k) = \varprojlim \mathbb{Z}/n\mathbb{Z}$. It is denoted by $\hat{\mathbb{Z}}$.

Direct system is set abelian groups $\{A_i\}$ indexed over I with maps $\mu_i^j : A_i \to A_j$ such that $\mu_j^k \circ \mu_i^j = \mu_i^k$. Let $A' = \sqcup A_i$, we can define an equivalence relation $x - y \Leftrightarrow \mu_i^k x = \mu_j^k y$ for some k. $A = \varinjlim A_i$ is set of equivalence classes. This can be made an abelian group by defining $x + y$ as equivalence class of $\mu_i^k x + \mu_j^k y$ for any $k \geq i, j$

If $G = \varprojlim G/U_i$ and A is a G module then $A = \varinjlim A^{U_i}$. We have direct system $(I, \hat{H}^q(G/U_i, A^{U_i}); \theta_i^j)$ where

$$\theta_i^j : \hat{H}^q(G/U_i, A^{U_i}) \to \hat{H}^q(G/U_j, A^{U_j}) \to \hat{H}^q(G/U_j, A^{U_j})$$

This gives us $\hat{H}^q(G, A) \varinjlim \hat{H}^q(G/U_i, A^{U_i}$. Thus if E is Galois extension over K, we have $\hat{H}^q(G, E) = \varinjlim \hat{H}^q(G(K_i/K), K_i)$ for finite intermediate extensions K_i. Similarly we have $\hat{H}^q(G, E^*) = \varinjlim \hat{H}^q(G(K_i/K), K_i^*)$

Lemma 4.6. *Galois extension E has trivial cohomology.*

Proof. If E is a finite extension then by normal basis theorem E is induced, hence has trivial cohomology. □

Lemma 4.7. $\hat{H}^1(G, E^*) = 1$

Proof. Consider E to be finite extension. Let $\tau \in G$ and f be a 1 cocycle. By independence of characters we have a non zero $b = \sum_{\sigma \in G} f(\sigma).\sigma(c)$ for some c. Then $\tau(b) = f^{-1}(\tau)b$. Hence f is a cochain. □

Chapter 5

Local Class Field Theory

5.1 Brauer Group

Throught this section k denotes complete field with respect to a non archimedean valuation v and a finite residue field k_r of order q. Brauer group of k denoted by $Br(k)$ is defined as $\varinjlim G(m/k)$ where m runs through finite extensions of k. $\mathfrak{o}$ denotes the ring of integers and $\mathfrak{p}$ the maximal ideal. Let l denote a finite Galois extension of degree n. Let k_{ur} be the maximal unramified extension of k with Galois group $\hat{\mathbb{Z}}$. In this section we prove that $Br(k) = \hat{H}^2(\hat{\mathbb{Z}}, k_{ur}^*)$.
From the exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$, we have

$$\hat{H}^1(G, \mathbb{Q}) \to \hat{H}^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} \hat{H}^2(G, \mathbb{Z}) \to \hat{H}^2(G, \mathbb{Q}/\mathbb{Z})$$

Since Q has trivial cohomology δ becomes an isomorphism. $\hat{H}^1(G, \mathbb{Q}/\mathbb{Z}) \cong Hom(G, \mathbb{Q}/\mathbb{Z}) \cong \hat{H}^2(G, \mathbb{Z})$. The map $\gamma : Hom(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}$ defined by $\phi \to \phi(1)$ is an ismorphism. The valuation map $v : k_{nr}^* \to \hat{\mathbb{Z}}$ defines a homomorphism $v : \hat{H}^2(\hat{\mathbb{Z}}, {k^*}_{nr}) \to \hat{H}^2(\hat{\mathbb{Z}}, \mathbb{Z})$. We define invariant map, $inv_k : \hat{H}^2(\hat{\mathbb{Z}}, k_{nr}^*) \to \mathbb{Q}/\mathbb{Z}$ as

$$inv_k = \gamma \circ \delta^{-1} \circ v$$

Claim is that this is an isomorphism. Which will be proved by showing that v is an ismorphism.

Proposition 5.1. *Let k_n be the degree n unramified extension of k with Galois group G then $\hat{H}^q(G, U_{k_n}) = 1$ for all $q \in \mathbb{Z}$.*

Proof. Define $U_n^i = 1 + \pi^n \mathfrak{o}_n$, then $U_n = \varprojlim U_n/U_n^i$. Let k_{n_r} denote the residue field of k_n.

We have a G module homomorphism

$$U_n \to k_{n_r}^*$$

$$a_0 + a_1\pi + ... \to a_0$$

The kernel is U_1, hence $U/U_1 \cong k_n^*$. Similarly the G module homorphism

$$U_n^i \to k_{n_r}^+$$

$$1 + \pi^n.a \to \bar{a}$$

has kernel U_n^{i+1}. Hence $U_n^i/U_n^{i+1} \cong k_n^+$. Since they are G module isomorphisms we have $\hat{H}^q(G, U/U_1) = \hat{H}^q(G, k_{n_r}^*)$ and $\hat{H}^q(G, U_n^i/U_n^{i+1}) = \hat{H}^q(G, k_{n_r}^+)$. From lemma 4.5 and 4.6, $k_{n_r}^+$ has trivial cohomology and $\hat{H}^1(G, k_{n_r}^*) = 1$. Since G is cyclic, we have $\hat{H}^{2q}(G, k_{n_r}^*) = 1$ and $\hat{H}^{2q+1}(G, k_{n_r}^*) = h(k_{n_r}^*).\hat{H}^{2q}(G, k_{n_r}^*)$. Since $k_{n_r}^*$ is finite $h(k_{n_r}^*) = 1$, refer pg109 [CF10]. This implies $\hat{H}^{2q+1}(G, k_{n_r}^*) = 1$.

$$1 \to U_1 \to U \to U/U_1 \to 1$$

$$\Rightarrow \hat{H}^{q-1}(G, U/U_1) \xrightarrow{\delta} \hat{H}^q(G, U_1) \to \hat{H}^q(G, U) \to 1$$

By above exact sequences given a q-cocycle $f \in \hat{H}^q(G, U)$ we have g_1, $(q-1)$-cochain in $\hat{H}^{q-1}(G, U)$ and f_1, q-cocycle in $\hat{H}^q(G, U_1)$ such that $f = \delta.g_1 + f_1$. Similarly we can construct $f_n = \delta.g_{n+1} + f_{n+1}$ where f_n is q-cocycle of $\hat{H}^q(G, U_n)$ and g_{n+1} is $(q-1)$-cochain of $\hat{H}^{q-1}(G, U_n)$. Now adding all $f_n = \delta.g_{n+1} + f_{n+1}$ we have $f = \delta(\sum g_i)$. The sum converges since $U_n = \varprojlim U/U_n$ and is a cochain. Since f is image of cochain we have $f = 0$. □

From the exact sequence $0 \to U_{k_n} \to k_n^* \xrightarrow{v} \mathbb{Z} \to 0$ we have the sequence

$$\hat{H}^q(G, U_{k_n}) \to \hat{H}^q(G, k_n^*) \xrightarrow{v} \hat{H}^q(G, \mathbb{Z}) \to \hat{H}^{q+1}(G, U_{k_n})$$

the isomorphism of v follows from the above proposition.
Let Γ_k denote the Galois group of k_{nr}^* then $\Gamma_k \cong Gal(\bar{k}_r/k_r)$. Since $l_r \subset \bar{k}_r$ we have an inclusion $Gal(\bar{l}_r/l_r) \to Gal(\bar{k}_r/k_r)$. This inclusion $\Gamma_l \to \Gamma_k$ gives us the map $Res : \hat{H}^2(\Gamma_k, k_{nr}^*) \to \hat{H}^2(\Gamma_l, l_{nr}^*)$

Proposition 5.2. *$inv_l \circ Res = n.inv_k$*

$$\begin{array}{ccc} \hat{H}^2(\Gamma_k, k_{nr}^*) & \xrightarrow{res} & \hat{H}^2(\Gamma_l, l_{nr}^*) \\ inv_k \uparrow & & \downarrow inv_l \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \end{array}$$

Proof. Let σ_k be the frobenius element of Γ_k. Let e be the ramification index and $f = [l_r : k_r]$. β_k is defined as $\beta_k(\chi) = \chi(\sigma_k)$. For $x \in k^*_{ur}$, $v_l(x) = ev_k(x)$. Hence we have the left most commutative diagram. $Gal(l_r/k_r)$ is a cyclic group of order f, hence we have $\sigma_l = \sigma_k^f$. The third commutative diagram follows as

$$\beta_l(e.res(\chi) = e\beta_l(res(\chi)) = e\chi(\sigma_k^f) = ef(\chi(\sigma_k)) = n\beta_l(\chi)$$

.

$$\begin{array}{ccccccc} \hat{H}^2(\Gamma_k, k^*_{nr}) & \xrightarrow{v_k} & \hat{H}^2(\Gamma_k, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & Hom(\Gamma_k, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\beta_k} & \mathbb{Q}/\mathbb{Z} \\ \downarrow res & & \downarrow e.res & & \downarrow e.res & & \downarrow n \\ \hat{H}^2(\Gamma_l, l^*_{nr}) & \xrightarrow{v_l} & \hat{H}^2(\Gamma_l, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & Hom(\Gamma_k, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\beta_l} & \mathbb{Q}/\mathbb{Z} \end{array}$$

This proves the theorem. □

5.2 Fundamental Class of $\hat{H}^2(G(l/k), l^*)$

Let x be an element of kernel of Res. Then from the previous proposition we have

$$inv_l(Res(x)) = 0 \Leftrightarrow n.inv_k(x) = 0 \Leftrightarrow inv_k(x) = 1/n$$

Hence the kernel is generated by an element $u_{l/k} \in \hat{H}^2(\Gamma_k, k^*_{nr})$ such that $inv_k(u_{l/k}) = 1/n$. Since $ker(res) \subset \hat{H}^2(G, l^*)$ we conclude that $\hat{H}^2(G, l^*)$ contains a cyclic group of order n. In fact we can show that $\hat{H}^2(G, l^*)$ is generated by $u_{l/k}$. First let us look at cyclic case.

Lemma 5.3. *For a cyclic extension l/k of degree n, $\hat{H}^2(G, l^*)$ is cyclic of order n.*

Proof. Let U be an open subgroup of U_l with trivial cohomology, refer pg134 [CF10].

$$1 \to U \to U_l \to U_l/U \to 1$$

From this we have $h(U_l) = h(U).h(U_l/U) = 1$, refer pg109 [CF10].

$$1 \to U_l \to l^* \xrightarrow{\text{v}} \mathbb{Z} \to 0$$

This gives $h(l^*) = h(\mathbb{Z}).h(U_l)$. $h(\mathbb{Z}) = [\hat{H}^0(G, \mathbb{Z})]/[\hat{H}^1(G, \mathbb{Z})]$. $G = \mathbb{Z}/n\mathbb{Z}$ acts trivially on $\mathbb{Z}$. $\hat{H}^0(G, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$ and $\hat{H}^1(G, \mathbb{Z}) = Hom(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = 0$. Hence $h(\mathbb{Z}) = n$. Therefore

$h(l^*) = 1$. Using the definition $h(l^*) = [\hat{H}^2(G, l^*)]/[\hat{H}^1(G, l^*)]$ and the fact that $\hat{H}^1(G, l^*) = 1$ we have $[\hat{H}^2(G, l^*)] = n$. □

We need the following lemma to go from cyclic case to a general case, refer pg135 [CF10].

Lemma 5.4. ***Ugly lemma:*** *Let $p, q \geq 0$ be integers. A be a G module. Assume*

1. *$\hat{H}^1(H, l^*) = 0$ for all subgroups H of G.*
2. *For $H \subset K \subset G$ such that H is normal in K and K/H cyclic of prime order. Then $[\hat{H}^q(H, A)] | [K : H]^p$.*

Proposition 5.5. *$\hat{H}^2(G, l^*)$ is cyclic of order n.*

Proof. Take $p = 1$, $q = 2$ and $A = l^*$ in previous lemma. Hence $[\hat{H}^2(G, l^*)]$ divides n. But we have shown that $\hat{H}^2(G, l^*)$ contains a cyclic group of order n. Hence $\hat{H}^2(G, l^*)$ is cyclic group generated by $u_{l/k}$ such that $inv_l(u_{l/k}) = 1/n$. □

By definition $Br(k) = \varinjlim \hat{H}^2(G, l^*)$ where l runs through finite Galois extensions. But $\hat{H}^2(G, l^*) \subset \hat{H}^2(\Gamma_k, k^*_{nr})$ hence $Br(k) \subset \hat{H}^2(\Gamma_k, k^*_{nr})$. Thus we have proved

Theorem 5.6. *$Br(k) = \hat{H}^2(\Gamma_k, k^*_{nr})$*

5.3 Local Reciprocity Map

We use Tate's theorem from pg115 of [CF10] for the following theorem.

Theorem 5.7. *The map $\hat{H}^q(G, \mathbb{Z}) \to \hat{H}^{q+2}(G, l^*)$ given $a \mapsto a.u_{l/k}$ is an isomorphism.*

Proof. For every subgroup H of G we have field k' over k in l such that $H = Gal(l/k')$. We have $\hat{H}^1(H, l^*) = 0$ for all subgroups H. We have shown already shown $\hat{H}^2(H, l^*)$ is generated by $u_{l/k'}$ such that $inv_{k'}(u_{l/k'}) = 1/m$, $m = [l : k']$. Observe that

$$inv_{k'}(Resu_{l/k}) = [k' : k] inv_k(u_{l/k}) = [k' : k]/n = 1/m$$

Hence $inv_{k'}(u_{l/k'}) = inv_{k'}(u_{l/k'})$. The above arguement is true for all the Sylow subgroups of G. Hence by applying Tate's theorem we arrive at the result. □

In the case $q = -2$ we have $\hat{H}^{-2}(G,\mathbb{Z}) = H_1(G,\mathbb{Z}) = G^{ab}$ and $\hat{H}^0(G,l^*) = k^*/N_{l/k}l^*$. Thus we have an isomorphism

$$\theta : k^*/N_{l/k}l^* \to G^{ab}$$

This map which is the inverse of the above isomorphism is **Local reciprocity map**.
Let $k^{'}$ be a separable extension over k and l be a finite extension $k^{'}$. Let $G = Gal(l/k)$ and $H = Gal(l/k^{'})$. With this notation we have

$$\begin{array}{ccc}
\hat{H}^q(G,\mathbb{Z}) & \xrightarrow{.u_l/k} & \hat{H}^{q+2}(G,l^*) \\
\downarrow{\scriptstyle res} & & \downarrow{\scriptstyle res} \\
\hat{H}^q(H,\mathbb{Z}) & \xrightarrow{.u_l/k^{'}} & \hat{H}^{q+2}(H,l^*)
\end{array}$$

Consider $\alpha \in \hat{H}^q(G,\mathbb{Z})$ then $res(\alpha.u_{l/k}) = res(\alpha).res(u_{l/k}) = res(\alpha).u_{l/k'}$, refer pg107 of [CF10]. Since cup product is isomorphism. We can reverse the isomorphism and taking $q = -2$ we have

$$\begin{array}{ccc}
k^*/N_{l/k}l^* & \xrightarrow{\theta_{l/k}} & Gal(l/k)^{ab} \\
\downarrow{\scriptstyle incl} & & \downarrow{\scriptstyle res} \\
k^*/N_{l/k'l^*} & \xrightarrow{\theta_{l/k'}} & Gal(l/k^{'})^{ab}
\end{array}$$

The above restriction map is also known as **Transfer**.
Let ${G_k}^{ab}$ denote maximal abelian extension over k. Then ${G_k}^{ab} = \varinjlim Gal(l/k)^{ab}$. Taking inverse limits

$$\begin{array}{ccc}
k^* & \xrightarrow{\theta_k} & {G_k}^{ab} \\
\downarrow{\scriptstyle incl} & & \downarrow{\scriptstyle transfer} \\
{k^{'}}^* & \xrightarrow{\theta_{k'}} & {G_{k'}}^{ab}
\end{array}$$

Similarly from

$$\begin{array}{ccc} \hat{H}^q(G,\mathbb{Z}) & \xrightarrow{.u_l/k} & \hat{H}^{q+2}(G,l^*) \\ cores \uparrow & & cores \uparrow \\ \hat{H}^q(H,\mathbb{Z}) & \xrightarrow{.u_l/k'} & \hat{H}^{q+2}(H,l^*) \end{array}$$

we have

$$\begin{array}{ccc} k'^* & \xrightarrow{\theta_{k'}} & {G_{k'}}^{ab} \\ \downarrow N_{k'/k} & & \downarrow incl \\ k^* & \xrightarrow{\theta_k} & {G_k}^{ab} \end{array}$$

From the sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ we have

$$\hat{H}^1(G,\mathbb{Q}) \to \hat{H}^1(G,\mathbb{Q}/\mathbb{Z}) \to \hat{H}^2(G,\mathbb{Z}) \to \hat{H}^2(G,\mathbb{Q})$$

Since $\mathbb{Q}$ has trivial cohomology the connection homomorphism $\delta : \hat{H}^1(G,\mathbb{Q}/\mathbb{Z}) \to \hat{H}^2(G,\mathbb{Z})$ is an isomorphism. $\hat{H}^1(G,\mathbb{Q}/\mathbb{Z}) = Hom(G,\mathbb{Q}/\mathbb{Z})$ and let $\chi \in Hom(G,\mathbb{Q}/\mathbb{Z})$. Let $a \in k^*$ and it's image in $\hat{H}^0(G,l^*)$ be denoted by $\bar{a}$. $\bar{a}.\delta(\chi) \in \hat{H}^2(G,l^*)$

Lemma 5.8. *With the above notation* $\chi(\theta(\bar{a})) = inv_k(\bar{a}.\delta(\chi))$

We can explicitly derive in the unramified case.

Proposition 5.9. *Let l/k be an unramified extension and σ be the generator of $Gal(l/k)$. If v_k is the normalized valuation of k then $\theta(\bar{a}) = \sigma^{v_k(a)}$.*

Proof. Let $a = N_{l/k}(b)$ for some $b \in l^*$. $v_k(N_{l/k}b) = fv_l(b)$, since v_k is unramified we have $f = n$. Hence $\sigma^{v_k(a)} = \sigma^{n.v_l(b)} = 1$ since σ is generator of group of order n. Therefore $\theta(\bar{a}) = \sigma^{v_k(a)}$ is well defined. By the previous lemma $\chi(\theta(\bar{a})) = inv_k(\bar{a}.\delta(\chi))$. Drop the k in v_k we have

$$inv_k(\bar{a}.\delta(\chi)) = \gamma \circ \delta^{-1} \circ v(\bar{a}.\delta(\chi)) = \gamma(\delta^{-1}(v(\bar{a})\delta(\chi)) = v(\bar{a})\gamma(\chi)$$

$$\chi(\theta(\bar{a})) = v(\bar{a})\chi(\sigma) = \chi(\sigma^{v(a)})$$

This is true for all χ, hence $\theta(\bar{a}) = \sigma^{v_k(a)}$. ∎

5.4 Characterization of Reciprocity Map

Let l be an abelian extension of k containing k_{ur}. Let k_π denote the fixed field of σ, the frobenius element of $G(k_{ur}/k)$. Then k_π and k_{ur} are linearly disjoint($k_{ur} \cap k_\pi = k$) and $l = k_{ur} \otimes k_\pi$.

Lemma 5.10. *$f : k^* \to G(l/k)$ be an homomorphism such that*

1. $f(x)_{|k_{ur}} = \sigma^{v(x)}$
2. *For any uniformizer, π, $f(\pi)$ is identity on k_π*

Proof. $\theta_{l/k}$ and f coincide on k_{ur}. $\theta_{l/k}(\omega)$ is identity on k_{ur}, for any uniformizer ω. Therefore f and $\theta_{l/k}$ coincide on k_π. Every $a \in k^*$ can be written as $\omega.\pi^n$ for some uniformizer ω. Hence $f(x) = \theta_{l/k}(x)$. □

We can replace the second condition with
If $a \in N_{m/k}m^*$ for some finite extension m over k in l then $f(a)$ is trivial on m. Assume f satisfies the above statement. Let $k^{'}$ be a finite extension in k_π. Since $\theta_{l/k}(\pi)(x) = 1$ for all $x \in k^{'} \subset k_\pi$. Hence $\theta_{k^{'}/k}(\pi) = 1$, this implies $\pi \in N_{k^{'}/k}k^{'*}$. Hence $f(\pi)$ is trivial on $k^{'}$.
Note: We use these criterion to prove that a map is reciprocity map.

5.5 Formal Groups

A **formal group law**($F(x, y)$) is a power series in variables over a ring $\mathfrak{o}$ satisfying the conditions

1. $F(x, F(y, z)) = F(F(x, y), z)$
2. $F(0, y) = y$ and $F(x, 0) = x$
3. $F(x, y) = F(y, x)$

If $x, y \in \mathfrak{p}$ then $F(x, y) \in \mathfrak{p}$, this makes $\mathfrak{p}$ group under the binary operation $x * y = F(x, y)$. We denote this group by $F_{\mathfrak{p}}$. Similarly for any finite extension l/k we have $F(\mathfrak{P})$.
$\mathfrak{F}_\pi$ be set of formal series $f \in \mathfrak{o}[[x]]$ satisfying

1. $f(x) \equiv \pi x (mod deg 2)$

2. $f(x) \equiv x^q (mod\, \pi)$

Proposition 5.11. *Let $f, g \in \mathfrak{F}_\pi$ and $\phi_1(x_1, ..., x_m)$ be a linear form over $x_1, ..., x_m$ with coefficients in $\mathfrak{o}$. Then there exists a unique $\phi \in \mathfrak{o}[[x_1, .., x_m]]$ such that*

1. $\phi \equiv \phi_1(moddeg2)$
2. $f \circ \phi = \phi \circ (g \times ... \times g)$

Proof. We shall construct a sequence of $\phi^(m) = \sum_{i=1}^m \phi_i$ satisfying the required conditions $(mod.deg.m + 1)$. Also $\deg(\phi_m) \geq m$. For $m = 1$, $\phi^{(1)} = \phi_1$ satisfies the required conditions.

Assume by induction we have $\phi^{(m)} = \sum_{i=1}^m \phi_i$

$$\phi^{(m)} \equiv \phi_1(mod.deg.2), \;\; f \circ \phi^{(m)} \equiv \phi^{(m)} \circ (g \times .... \times g)$$

We need to find ϕ_{m+1} such that $\phi^{(m+1)} := \phi^{(m)} + \phi_{m+1}$ satisfies the conditions $(mod.deg(m+2)$. Say $f \circ \phi^{(m)}(x) \equiv \phi^{(m)}(g(x)) + E_{m+1}(mod.deg(m+2))$ where $E_{m+1} \equiv 0(mod.deg(m+1))$. We have chosen ϕ_{m+1} with degree greater than $m+1$ hence by $f(x) \equiv \pi x(moddeg2)$ we have

$$f \circ \phi^{(m+1)}(x) = f(\phi^{(m)}(x) + \phi_{m+1}(x)) \equiv f(\phi^{(m)}) + \pi\phi_{m+1}(mod.deg(m+2))$$

and similarly

$$\phi^{(m+1)}(g(x)) \equiv \phi^{(m)}(g(x)) + \pi^{(m+1)}\pi_{(m+1)}$$

$$\Rightarrow (f \circ \phi^{(m+1)} - \phi^{(m+1)} \circ g)(x) \equiv E_{m+1} + (\pi - \pi^{m+1})\phi_{m+1}$$

So we define $\phi_{m+1} := E_{m+1}(\pi - \pi^{m+1})^{-1}$. By induction hypothesis E_{m+1} is unique, therefore ϕ_{m+1} is unique. All left is to show that $\phi_{m+1} \in \mathfrak{o}[[X]]$.

$1 - \pi^m$ is a unit hence it is enough to show that $E_{m+1} \equiv 0(mod\, \pi)$. Since $f \equiv x^q(mod\, \pi)$

$$E_{m+1} \equiv f(\phi^{(m+1)}(x)) - \phi^{(m+1)}(g(x)) \equiv (\phi^{(m+1)}(x))^q - \phi^{(m+1)}(x^q) \equiv 0(mod\, \pi)$$

□

Using the above proposition the following corollaries follow

Corollary 5.12. 1. *There exists a unique formal group law $F_f \in \mathfrak{o}[[x]]$ satisfying $f(F_f(x, y)) = F_f(f(x), f(y))$*

2. *For any $a \in \mathfrak{o}$ there exists a unique $[a]_{f,g} \in \mathfrak{o}[[x]]$ satisfying*

   (a) $f \circ [a]_{f,g} = [a]_{f,g} \circ g$

(b) $[a]_f \equiv ax(mod.deg.2)$

This $[a]_{f,g}$ *is an homomorphism of* $F_{f_{\mathfrak{p}}}$ *to* $F_{g_{\mathfrak{p}}}$.

3. *For any unit* $u \in \mathfrak{o}$ $[u]_{f,g}$ *is an isomorphism between* $F_{f_{\mathfrak{p}}}$ *and* $F_g(\mathfrak{p})$

Proof. 1. Take $\phi_1[x,y] = x + y$ and $g = f$, then by above proposition we have a unique $F_f[x,y]$ satisfying satisfying $f(F_f(x,y)) = F_f(f(x), f(y))$. To prove the properties of a formal group for example $F(x,y) = F(y,x)$ take $\phi_1(x,y) = x + y$. Both $F_f(x,y)$ and $F_f(y,x)$ satisfy the conditions of the above proposition. So by uniqueness $F_f(x,y) = F_f(y,x)$. Similarly we can prove the rest of the properties.

2. Take $\phi_1(x) = ax$ in the proposition. To show that $[a]_{f,g} : F_{f_{\mathfrak{p}}} \to F_{g_{\mathfrak{p}}}$ one needs to show

$$F_f([a]_{f,g}(x), [a]_{f,g}(y)) = [a]_{f,g}F_g(x,y)$$

Take $\phi_1(x,y) = ax + ay$, both LHS and RHS above satisfy the criterion of the proposition hence by uniqueness they are equal.

3.

$$F_g \to F_f \to F_g$$

$$x \to [u]_{f,g}(x) \to [u^{-1}]_{g,f} \circ [u]_{f,g}(x)$$

For the group of endomorphisms on F_g, $[1]_{g,g}$ acts as an identity. It can be seen that $[u^{-1}]_{g,f} \circ [u]_{f,g} = [1]_{g,g}$ by using the uniqueness property of the proposition.

□

5.6 Reciprocity map and Existence Theorem

Denote $[a]_{f,f}$ as $[a]_f$. Let $\mathfrak{m}$ denote the maximal ideal in separable closure of k. $M_f = F_{f_{\mathfrak{m}}}$, we define $\mathfrak{o}-$ module structure on M_f by defining $a.x = [a]_f(x)$.

$$E_f := \left\{x \in M_f : [\pi^n]_{f,f}(x) = 0 \; for\; some\; n\right\}$$

and $k_\pi := k(E_f)$.

Lemma 5.13. *As* $\mathfrak{o}$*-modules* E_f *and* $k/\mathfrak{o}$ *are isomorphic.*

Proof. $E_f^n := \left\{x \in E_f : [\pi^n|_{f,f}(x) = 0\right\}$. Define a $\mathfrak{o}$-module homomorphism

$$k/\mathfrak{o} \to E_f$$

$$\pi^{-1} \to a_1, \ a_1 \in E_f^1$$

$$\pi^{-2} \to a_2, \ a_2 \in E_f^2$$

choose a_2 such that $\pi.a_2 = a_1$ Since E_f^1 is divisible we can always choose an element like a_2. Continuing with a_3,.. so on we define an isomorphism. $\square$

Lemma 5.14. *The map*

$$G(k_\pi/k) \to Aut_{\mathfrak{o}}(E_f)$$

$$\sigma \to \sigma_{|E_f}$$

is an isomorphism.

Proof. If σ is identity on E_f then it is identity on $K(E_f)$, hence it is an injection. We prove the surjectivity by showing that the order is same.

‘

$$E_f \cong k/\mathfrak{o} \Rightarrow Aut(E_f) \cong Aut(k/\mathfrak{o})$$

Note that

$$\mathfrak{o} \cong End_{\mathfrak{o}}(k/\mathfrak{o})$$

$$x \to \psi_x; \ \psi_x(a) = ax$$

Hence $Aut(k/\mathfrak{o}) \cong U_k$.

Since by definition $[\pi]_f \equiv \pi.x(mod.deg2)$ and $f(x) \equiv \pi.x(mod.deg2)$ we can take $[\pi]_f = f$. Since F_f are isomorphic, take $f(x) = \pi.x + x^q$. Define $k_\pi^n = k(E_f^n)$ and $a \in E_f^n - E_f^{n-1}$. $\pi^n.a = 0 \Rightarrow f \circ f ... \circ f = f^n(a) = 0$. Take $\phi(x) = f^n(x)/f^{n-1}(x) = (f^{n-1}(x))^{q-1} + \pi$. Note that $\phi(x)$ is Eisenstein polynomial of degree $q^{n-1}(q-1)$ and all the roots lie in $E_f^n - E_f^{n-1}$. This implies if we define $k_\pi^n = k(E_f^n)$ then $|G(k_\pi^n/k)| \geq q^{n-1}(q-1)$. We have already seen that $|U_k/U_k^n| = q^{n-1}(q-1)$. We have $G(k_\pi/k) = \varprojlim G(k_\pi^n/k)$ and $\varprojlim U_k/U_k^n = U_k$. This prooves the surjectivity. $\square$

This shows k_π^n/k is an abelian extension. And also observe that since π is constant in Eisenstein polynomial, $\pi \in N_{k_\pi^n/k} k_\pi^{n*}$.

$$\begin{array}{ccc} k^* & \xrightarrow{\theta_k} & G_k^{ab} \\ \downarrow j & & \downarrow res \\ N_{k_\pi^n/k} k_\pi^{n*} & \xrightarrow{\theta_{k_\pi^n/k}} & G(k_\pi^n/k) \end{array}$$

From the above commutative diagram $\theta_k(\pi)$ is identity on k_π^n, since $\pi \in N_{k_\pi^n/k}k_\pi^{n*}$. This implies $k_\pi \subset (k^{ab})^{<\theta_k(\pi)>}$. Hence k_π and k_{ur} are disjoint, that is $k_\pi \cap k_{ur} = k$. Define $l_\pi = k_{ur}.k_\pi$.

Let $\hat{k_{ur}}$ denote completion of k_{ur} and $\hat{\mathfrak{o}}_{nr}$ denote its ring of integers. Let ω be another uniformizer of k_{ur}. Let $g \in \mathfrak{F}_\omega$ and $f \in \mathfrak{F}_\pi$.

Proposition 5.15. *There exists $\phi \in \hat{\mathfrak{o}}_{ur}[[x]]$ with $\phi(x) \equiv \eta x (mod.deg.2)$ where η is a unit, such that $\sigma.\phi = \phi \circ [u]_f$ and ϕ is an $\mathfrak{o}$-module isomorphism of M_f and M_g.*

Proof. The proof is similar to the proof of proposition5.11, where we use successive approximations to construct ϕ. □

Lemma 5.16. *ϕ in the above proposition is invertible.*

Proof. Let $\phi(x) = \eta.x + a_1.x^2 + ...$ We need to find $\psi(x) = b_1.x + b_2.x^2 + ...$ such that $x = \eta.\psi(x) + a_1.\psi(x)^2 + ...$ So we have $\eta.b_1 = 1 \Rightarrow b_1 = \eta^{-1}$, $\eta.b_2 + a_1.b_1^2 = 0 \Rightarrow b_2 = \eta^{-1}(-a_1.b_1^2)$. Inductively we can get all b_i. □

Lemma 5.17. *l_π is independent of uniformizer*

Proof. Take $\alpha \in k_{ur}.k_\pi$, $\alpha = \sum \alpha_i.\beta_i$ where $\alpha_i \in k_{ur}$ and $\beta_i \in k_\pi$. Say $\beta \in k_\pi$, $\beta = \sum c_i.e_i = \sum c_i.\phi(e_i^{'})$ for some $e_i^{'} \in k_\omega$. Hence we have $\beta \in \hat{k_{ur}}.k_\omega \Rightarrow \alpha \in \hat{k_{ur}}.k_\omega \subset \hat{k_{ur}.k_\omega}$.

Take an $\alpha \in k_{ur}.k_\pi \subset \hat{k_{ur}.k_\omega}$, say $F = k_{ur}.k_\omega$. Assume $\exists \sigma \in G(\hat{F}/F)$ such that $\sigma(\alpha) \neq \alpha$.

$$\alpha = \lim \alpha,\ \alpha_n \in F$$

$$\Rightarrow \exists\, n,\ |\alpha - \alpha_n| < |\alpha - \sigma(\alpha)| = |\alpha - \alpha_n - \sigma(\alpha - \alpha_n)| \leq |\alpha - \alpha_n|$$

This gives us contradiction to assumption that a σ choosen exists. This implies $k_{ur}.k_\pi \subset k_{ur}.k_\omega$. Similarly we can show $k_{ur}.k_\pi \supset k_{ur}.k_\omega$ prooving the lemma. □

Lemma 5.18. *Define the map $r_\pi : k^* \longrightarrow Gal(l_\pi/k)$ by*

1. *$r_\pi(\pi)$ is 1 on k_π and is σ on k_{ur}*

2. *$r_\pi(u)$ is $[u^{-1}]$ on k_π and is 1 on k_{ur}*

r_π is independent of the uniformizer.

Proof. Let us see how $r_\pi(\omega)$ and $r_\omega(\omega)$ act on $k_\omega = k(E_g)$. Take $\lambda \in E_g$

$$r_\pi(\omega)(\lambda) = r_\pi(\pi.u)(\lambda) = r_\pi(\pi)(r_\pi(u)(\phi(\mu))),\ \mu \in E_f$$

Since $r_\pi(u)$ is identity on $\hat{\mathfrak{O}}$ and $\phi \in \hat{\mathfrak{O}}[[x]]$

$$r_\pi(\pi)(\phi(r_\pi(u)(\mu)) = r_\pi(\pi)(\phi([u^{-1}]_f(\mu))),\ [u^{-1}]_f(\mu) \in k_\pi$$

$$\Rightarrow r_\pi(\pi)(\phi)(u^{-1}\mu) = \phi(\mu) = \lambda$$

$$\Rightarrow r_\pi(\omega) = r_\omega(\omega)$$

□

Since $r_\pi(\pi)$ is identity on k_π and Frobenius on k_{ur}, it is the reciprocity map.

Theorem 5.19 (**Existence Theorem**). *For every open subroup M of finite index m in k^* there is a finite abelian extension l/k such that $N_{l/k}l^* = M$.*

Proof. Since $1 \in M$, $|x-1| < \epsilon \subset M$ implies ${U_k}^n \subset M$ for some n. M is of index m implies $\pi^m \in M$. Say $l_{n,m} = k_\pi^n.k_m$ where k_m is unramified extension of degree m. Consider $u.\pi^a \in l_{n,m}$, $u.\pi^a \in N_{l_{n,m}}l^*_{n,m} \Leftrightarrow \theta_{l_{n,m}}(u.\pi^a) = 1$.

$\theta_{l_{n,m}}(u.\pi^a)$ acts as $[u^{-1}]$ on k_π^n and we know $G(k_\pi^n/k) \cong U_k/U_k^n$. Therefore $[u^{-1}]$ is identity if and only if $u \in U_k^n$. $\theta_{l_{n,m}}(u.\pi^a)$ acts as σ^a where σ is Frobenius element on k_m. Therefore $\theta_{l_{n,m}}(u.\pi^a)$ is identity on k_m if and only if $a \equiv 0(mod.m)$. Hence we have $u.\pi^a \in U_k^n.\pi^m$. This implies $N_{l_{n,m}}l^*_{n,m} \subset M$. For case of convinience denote $N_{l_{n,m}}l^*_{n,m}$ by Nl^*. We have isomorphism

$$\theta_l : k^*/Nl^* \to G(l/k)$$

Let $H = \theta_l(M)$. Let l' be abelian extension such that $G(l'/k) = G^{ab}/H$. This implies $N_{l'/k}l'^* = M$. □

Chapter 6

Global Class Field Theory

6.1 Main Theorem

k denotes a finite extension of $\mathbb{Q}$. l a finite abelian extension of k with Galois group G and order n. $\mathfrak{m}_k$ denotes the set of all normalized valuations of k. v is used to denote a normalized valuation of k and w for l.
Let $\sigma \in G$, for $a \in l$, $|a|_{\sigma w} := |\sigma^{-1} a|_w$. l_w denote completion of l with respect to w. Then we have isomorphism $\sigma : l_w \to l_{\sigma w}$.

Lemma 6.1. *Let v be restriction of w to k. l_w/k_v is a Galois extension with Galois group given by*

$$G_w = \left\{ \sigma \in G : \sigma w = w \right\}$$

Proof. Observe that $G_w \subset Gal(l_w/k_v)$. σ_i, $i \in [r]$ be representative of G/G_w.

$$|G| = r.|G_w| \leq \sum_{i=1}^{r} [l_w : k_v] \leq \sum_{w|v} [l_w ; k_v] = |G|$$

From the isomorphism $\sigma : l_w \to l_{\sigma w}$, $[l_w : k_v]$ is constant over w dividing v. Hence by the above inequality we know that G acts transitively on the set of w dividing v and $|G_w| = [l_w : k_v]$. $\square$

Note that $G_{\sigma w} = \sigma G_w \sigma^{-1}$. If l/k is an abelian extension we use l_v to denote l_w since $G_{\sigma w}$ is same for all σ. Throught this section S denotes(unless mentioned) the set of all archimedean and ramified primes of k. We define the homomorphism

$$F_{l/k} : I_S \to G$$

$$v \to \sigma_v$$

where σ_v is the Frobenius element of unramified extension l_v/k_v. The aim of the Class Field theory is to understand the finite abelian extensions of a Field. The main theorem can be summarized into four points

1. **Reciprocity Law**. There exists a continous homomorphism $\psi_{l/k} : J_k \to G$ satisfying the conditions
   (a) $\psi_{l/k}(k^*) = 1$
   (b) $\psi_{l/k}(x) = F_{l/k}((x)^S)$ for all $x \in J_k^S$
2. $\psi_{l/k}(k^* N_{l/k} J_L) = 1$ and we have an isomorphism $\psi_{l/k} : C_k/N_{l/k}C_l \to Gal(l/k)$
3. For abelian extensions $m \supset l \supset k$ we have the following commutative diagram.

$$\begin{array}{ccc} C_k/N_{m/k}C_m & \xrightarrow{\psi_{l/k}} & Gal(m/k) \\ \downarrow j & & \downarrow res \\ C_k/N_{l/k}C_l & \xrightarrow{\psi_{l/k}} & Gal(l/k) \end{array}$$

   Here res takes an element in $Gal(m/k)$ to it's restriction on l. j is the natural surjective map.
4. **Existence Theorem**. Given a subgroup N of finite index in C_k there exists a unique abelian extension l/k such that $N_{l/k}C_l = N$

6.2 Cohomology of Ideles

$A_l = A_k \otimes_k l$, action of $\sigma \in G$ on A_l can be seen as action of $1 \otimes \sigma$ on $A_k \otimes_k l$.

Lemma 6.2. $\hat{H}^r(G, J_l) \cong \coprod_{v \in \mathfrak{M}_k} \hat{H}^r(G_v, {l_v}^*)$

Proof. Let

$$J_{l,S} = \prod_{v \in S}(\prod_{w|v} {l_w}^*) \prod_{v \notin S}(\prod_{w|v} U_w)$$

observe that $J_l = \varinjlim_S J_{l,S}$, $S \to \mathfrak{M}_k$. Since U_w has trivial cohomology,

$$\hat{H}^r(G, J_{l,S}) = \prod_{v \in S} \hat{H}^r(G, \prod_{w|v} {l_w}^*)$$

$\prod_{w|v} l_w{}^* \cong Hom_{G^w}(\mathbb{Z}[G], l_w{}^*)$, hence by Shapiro's lemma we have $\hat{H}^r(G, \prod_{w|v} l_w{}^*) \cong \hat{H}^r(G^v, l_v{}^*)$. Taking $S \to \mathfrak{M}_k$ proves the lemma. □

Consequence

1. $\hat{H}^1(G, J_l) = 0$
2. $\hat{H}^2(G, J_l) \cong \coprod_{v\in\mathfrak{M}_k} (\mathbb{Z}/n_v\mathbb{Z})$ where $n_v = [l_v : k_v]$

Theorem 6.3 (First Inequality)**.** *If l/k is cyclic of degree n then $[J_k/k^* N_{l/k} J_l] \geq n$*

Proof. $[h(G, C_l)] \leq [C_k/N_{l/k}C_l]$ and $J_k/k^*N_{l/k}J_l \cong C_k/N_{l/k}C_l$. So it is enough to show that $[h(G, C_l)] = n$. Choose $S^{'} \subset \mathfrak{M}_l$ to be set of archimedean, unramified and primes generating I_l/l^*. Then we have $J_l = l^* J_{l,S}$ where S is restiction of $S^{'}$ to k.

$$C_l = J_l/l^* = J_{l,S}/J_{l,S} \cap l^*$$

call $J_{l,S} \cap l^*$ as l_S. So we have $h(C_l).h(l_S) = h(J_{l,S})$

$$h(J_{l,S}) = h(\prod_{v\in S}(\prod_{w|v} l_w^*) \times \prod_{v\notin S}(\prod_{w|v} U_w)) = h(\prod_{v\in S}(\prod_{w|v} l_w^*))$$

$$= \prod_{v\in S} h(\prod_{w|v} l_w^*) = \prod_{v\in S} h(G_v, l_v^*) = \prod_{v\in S} n_v$$

$V := \{f : S^{'} \to \mathbb{R}\}$. $\sigma \in G$. $(\sigma.f)w := f(\sigma^{-1}w)$. V is a vector space over $\mathbb{R}$ of dimension $|S^{'}|$. The set $W = \{f : f(S^{'}) \subset \mathbb{Z}\}$ spans V.

$$W \cong \prod_{w\in S'} \mathbb{Z} = \prod_{v\in S}(\prod_{w|v} \mathbb{Z})$$

$$f \to \prod_{w\in S'} f(w)$$

$\sigma.\prod_{w|v} \mathbb{Z} \subset \prod_{w|v} \mathbb{Z}$. Hence by Shapiro's lemma we have

$$\hat{H}^r(G, W) \cong \prod_{v\in S} \hat{H}^r(G_v, Z)$$

Here G_v acts trivially on $\mathbb{Z}$

$$\Rightarrow h(N) = \prod_{v\in S} [\hat{H}^0(G_v, \mathbb{Z}]/[\hat{H}^1(G_v, \mathbb{Z})] = \prod_{v\in S} n_v$$

.

Now we construct another lattice that spans V but with Herbrand quotient $nh(l_S)$. Define

$$\gamma : l_S \to V$$

$$a \to f_a, \; f_a(w) = log|a|_w$$

by the proof of Dirichlet's theorem we note that kernel of γ is finite and image is lattice spanning $X = \left\{ f : \sum_{w \in S'} f(w) = 0 \right\}$. Hence, $V \cong X \oplus \mathbb{R}$. Now the lattice $U = img(\gamma) \oplus \mathbb{Z}$ spans V.

$$h(U) = h(img).h(\mathbb{Z}) = nh(l_S)$$

Since W and U both span same vector space we have $h(W) = h(U)$ refer pg110 in [CF10] $nh(l_S) = \prod_{v \in S} n_v = h(j_{l,S})$. This proves $h(C_l) = n$ □

Lemma 6.4. *Let l/k be a cyclic extension of prime order n. Let $k_n = k[\zeta_n]$, ζ_n is primitive n^{th} root of unity. Let $k_n^{'} = lk_n$, if $[C_{k_n}/NC_{k_n^{'}}]$ divides n so does $[C_k/NC_l]$*

Proof. The proof follows from the following diagram

$$\begin{array}{ccccccc}
C_l & \xrightarrow{N_{l/k}} & C_k & \longrightarrow & C_k/N_{l/k}C_l & \longrightarrow & 0 \\
\downarrow{\scriptstyle Con} & & \downarrow{\scriptstyle con} & & \downarrow{\scriptstyle Con} & & \\
C_{k_n'} & \xrightarrow{N_{k_n'/k_n}} & C_{k_n} & \longrightarrow & C_{k_n}/N_{k_n'/k_n}C_{k_n'} & \longrightarrow & 0 \\
\downarrow{\scriptstyle N_{k_n'/k}} & & \downarrow{\scriptstyle N_{k_n/k}} & & \downarrow{\scriptstyle N_{k_n'/l}} & & \\
C_l & \xrightarrow{N_{/k}} & C_k & \longrightarrow & C_k/N_{l/k}C_l & \longrightarrow & 0
\end{array}$$

Let $[k_n : k] = m$. By definition of norm map if $a \in C_k$ then $a^n \in N_{l/k}C_l$.

$$N_{k_n/k} \circ Con_{k_n/k} : C_k/N_{l/k}C_l \to C_k/N_{l/k}C_l$$

$$a \to a^m$$

Since $(m, n) = 1$ there exists k_1 and k_2 such that $mk_1 + nk_2 = 1$. Hence the map $N_{k_n/k} \circ Con_{k_n/k}$ is surjective, $a^{k_1} \to a$. Thus lemma follows from the fact the map $N_{k_n/k} : C_{k_n}/N_{k_n'/k_n}C_{k_n'} \to C_k/N_{l/k}C_l$ is surjective. □

Theorem 6.5. *Let k contain n^{th} roots of unity for some prime n. l be an abelian extension with Galois group, $G \cong (\mathbb{Z}/n\mathbb{Z})^r$. Then $[C_k/N_{l/k}C_l]|n^r$.*

Proof. By Kummer theory (refer corollary on pg90 of [CF10]) $l = k[a_1^{1/n}, ..., a_r^{1/n}]$ for some $a_i \in k$. Let S be a finite subset of $\mathfrak{m}_k$ containing all the archimedean, ramified and unramified primes that generate I_k/k^*. And also let S contain primes which divide n and primes such that $a_i \in \mathfrak{o}_v^*$ for all $v \notin S$. Let U_S denote the set of S units, that is, $a \in U_S$ implies $a \in \mathfrak{o}_v^*$ for all $v \notin S$. Let $M = k[U_S^{1/n}]$, by Dirichlet's unit theorem U_S has finite basis. Let $[M : k] = n^s$. Let w be a prime of l, above a $v \notin S$. M/k is unramified outside S hence $F_{M/l}(w)$ makes sense and it generates $G_w(M/l)$. Let $G(M/l)$ be generated by $F_{M/l}(w_i),\ i = 1, 2.., t$ where w_i are unramified. $T = \{v_i\}$ be the corresponding restrictions of w_i to k. Claim is that $l_{w_i} = k_{v_i}$ for all $i \in [t]$. Let $v \in \{v_i\}$, $G_v(M/k)$ is cyclic subgroup of $(\mathbb{Z}/n\mathbb{Z})^s$, implies $G_v(M/k) = \mathbb{Z}/n\mathbb{Z}$ or (0). $M_{w'} \supset l_w \supset k_v$, $G_w(M/l) = F_{M/l}(w)$ is non trivial.

$$G_v(l/k) = G_v(M/k)/G_w(M/l) \Rightarrow G(l_w/k_v) = G(M_{w'}/k_v)/G(l_w/k_v)$$

$$\Rightarrow G_v(l/k) = (0) \Rightarrow G_v(M/k) = G_w(M/k)$$

$$\Rightarrow l_w = k_v \textit{ and } F_{M/l}(w) = F_{l/k}(v)$$

Claim: $l^{*n} \cap U_S = \{a \in U_S : a \in k_v^n \,\forall\, v \in \{v_i\}\}$. If $a \in l^{*n} \cap U_S$, $a \in \mathfrak{o}_v^*$ for all $v \in \{v_i\}$. $a = b^n$ for some $b \in l$ and $v_w(a) = 0$ since $\mathfrak{o}_v^* = \mathfrak{o}_w^*$. This implies $b \in \mathfrak{o}_w^*$ hence $a \in {\mathfrak{o}_w^*}^n \subset k_v^n$. Now assume $a \in U_s$

$$\Rightarrow a = b^n,\ b \in k_v$$

$$F_{M_w/k_v} a^{1/n} = a^{1/n}$$

$F_{M_w/k_v} = F_{M_w/l_w} \Rightarrow a \in l^n$. This proves the claim.

Define

$$U = \prod_{v \in S} k_v^{*n} \times \prod_{v \in T} k_v^* \times \prod_{v \notin S \cup T} U_v$$

$a_v \in k_v$, $v \in S$, since $k_v^*/N_{l/k}l^* \cong G_v \subset \mathbb{Z}/n\mathbb{Z}^r$ $a_v^n \in N_{l/k}l^*$. $a_v \in k_v^*$, $v \in T$, since $l_w = k_v$, $a_v \in N_{l/k}l^*$. $a_v \in U_v$ for v unramified, $a_v \in N_{l/k}l^*$ since $N_{l/k}U_l = U_k$. Hence $E \subset N_{l/k}J_l$. So to prove the lemma it is enough to show $[J_k/k^*E]$ divides n^r.

$J_k = k^* J_{k,S} = k^* J_{k,S\cup T}$ and

$$[k^* J_{k,S\cup T}/k^* E][k^* \cap J_{k,S\cup T}/k^* \cap E] = [J_{k,S\cup T}/E]$$

Claim: $[J_{k,S\cup T}/E]/[k^* \cap J_{k,S\cup T}/k^* \cap E] = n^r$

$$[J_{k,S\cup T}/E] = \prod_{v \in S} [k^*/k^{*n}]$$

$$h(k_v^*) = n/|n|_v = [k_v^*/k_v^{*n}]/n$$

Since $|n|_v = 1$ for all $v \notin S$ we have

$$[J_{k,S\cup T}/E] = \prod_{v\in S} n^2/|n|_v = n^{2s}\prod_{v\in S} 1/|n|_v = n^{2s}\prod_{v\in \mathfrak{m}_k} 1/|n|_v = n^{2s}$$

By Dirichlet unit theorem the cardinality of basis for U_S is s. Thus we have $[m : k] = n^s$, $[l : k] = n^r$ and $[m : l] = n^t$ where $s = r + t$. By Kummer theory(pg91 [CF10]) we have $[U_S \cap m^{*n} : U_S \cap k^{*n}] = [U_S; U_S^n] = n^s$. Replacing S by $S \cup T$ we have $[U_{S\cup T}; U_{S\cup T}^n] = n^{s+t}$. So it is enough to show $k^* \cap E = k_{S\cup T}^n$. This follows from the fact that $k_S \to \prod_{v\in T} U_v/U_v^n$, refer pg184 [CF10]. □

Now applying the ugly lemma and using previous two lemmas we have

Theorem 6.6. *If l/k is Galois extension of degree n then*

1. *$[\hat{H}^0(G, C_l)]$ and $[\hat{H}^2(G, C_l)]$ divide n.*
2. *$\hat{H}^1(G, C_l) = 0$.*

6.3 Reciprocity Map

Define

$$\psi_{l/k}(x) = \prod_{v\in\mathfrak{M}_k} \psi_v(x_v)$$

where ψ_v is the local reciprocity map. Since v is unramified and x_v is unit for almost all v the product is well defined. The continuity of the local map implies the continuity of the product. If $x \in J_k^S$ then

$$F_{L/k}((x)^S) = \prod_{v\notin S} F_{L^v/k_v}(x_v) = \prod_{v\notin S} \psi_v(x_v) = \psi_{L/k}(x)$$

So it remains to show that $\prod \psi_v(x) = 1$ for all $x \in k$. We prove this first in the cyclotomic extension case, that is $l = k[\zeta]$.

Lemma 6.7. *If $l = k[\zeta]$ for some root of unity ζ, then $\prod_{v\in\mathfrak{M}_k} \psi_v(a) = 1$ for all $a \in k$.*

Proof. $(N_{k/\mathbb{Q}}x)_p = \prod_{v|p} N_{k_v/\mathbb{Q}_p} x_v$ and locally we have seen that $\psi_p(N_{k_v/\mathbb{Q}_p}x) = \psi_v(x)$. Hence

$$\prod_{v\in\mathfrak{M}_k} \psi_v(a) = \prod_p \psi_p(\prod_{v|p} N_{k_v/\mathbb{Q}_p}(a))$$

So it is enough to prove the lemma for a cyclotomic extension l over $\mathbb{Q}$
Let ζ be m^{th} root of unity and S be a finite set of primes of $\mathbb{Q}$ conatining the archimedean and ramified primes. If $(a,m) = 1$ then $(a)^S = \sum v_{p_i}(a)p_i$ where $p_i \not| a$. This implies $F_{l/\mathbb{Q}}((a)^S)\zeta = \zeta^{\prod p_i^{v_{p_i} a}} = \zeta^a$. Let $a \in \mathbb{Q}$ such that $|a-1|_p < |m|_p$ for all $p \in S$. $a = 1 + mr$ for some $r \in \mathbb{Z}$. $(b,c) = 1$ implies $(b,m) = 1$ and $(c,m) = 1$. Hence $F_{l/\mathbb{Q}}((b)^S)\zeta = \zeta^b = \zeta^c = F_{l/\mathbb{Q}}((c)^S)\zeta$. $(a)^S = (b)^S - (c)^S$, $F_{l/\mathbb{Q}}((a)^S)\zeta = \zeta^{b/c} = \zeta$. Hence $F_{l/\mathbb{Q}}(a)^S = 1$. We found a ϵ such that for all $a \in \mathbb{Q}$ such that $|a-1|_p < \epsilon$, $p \in S$, $F_{l/\mathbb{Q}}(a)^S = 1$. This property is called admissibility. Using the above property we construct a continous $\psi : J_{\mathbb{Q}} \to G(l/\mathbb{Q})$ such that $\psi(\mathbb{Q}) = 1$. Take $x \in J_{\mathbb{Q}}$, by weak approximation theorem there exists $(a_n) \in \mathbb{Q}$ such that $a_n \to x_p^{-1}$ for all $p \in S$.

$$\psi(x) := \lim_n F_{l/\mathbb{Q}}(a_n x)^S$$

Well definedness follows from admissibility. If $a_n/a_m \to 1$

$$F_{l/\mathbb{Q}}(a_n x)^S / F_{l/k}(a_m x)^S = F_{l/\mathbb{Q}}(a_n/a_m)^S$$

by admissibility we have $F_{l/\mathbb{Q}}(a_n/a_m)^S \to 1$. Taking $a_n = a^{-1}$ we have $\psi(a) = 1$ for all $a \in \mathbb{Q}$.
Homomorphism property of $F_{l/\mathbb{Q}}$ implies that ψ defined is a homomorphism. $\psi_p(x) := \psi((x)_p)$ where $((x)_p)p_i = \delta_{pp_i}$. All is left to show is that ψ_p are indeed the local reciprocity maps.
From the commutative diagram whose proof will be given in next section

$$\begin{array}{ccc} J_{k'} & \xrightarrow{\psi_{L'/k'}} & Gal(L'/k') \\ \downarrow N_{k'/k} & & \downarrow res \\ J_k & \xrightarrow{\psi_{L/k}} & Gal(L/k) \end{array}$$

we can take l to be the maximal cyclotomic extension. We have $\psi_p : l_p \to G(l_p/\mathbb{Q}_p)$. Since unramified extensions are cyclotomic, $\mathbb{Q}_p^{nr} \subset l_p$. $\psi_p(a)_{|\mathbb{Q}_p} = F^{v_p(a)}$ where F is frobenious element of $\mathbb{Q}_p^{nr}$. This follows from definition. For any finite extension m over $\mathbb{Q}_p$, $\psi_p(a)$ leaves m fixed. From the lemma in characterization of reciprocity map section, these three properties show that ψ_p is a local reciprocity map. This proves the lemma. $\square$

Theorem 6.8. *If $a \in Br(k)$ then $\sum inv_v(a) = 0$*

Proof. We will first prove this in the case where $a \in \hat{H}^2(G, l^*)$ for some cyclic cylotomic extension l.

Consider $a \in k^*$ and let $\bar{a}$ be its image in $\hat{H}^0(G, l^*)$. If $\delta_\chi \in \hat{H}^2(G, \mathbb{Z})$ then $\bar{a}.\delta_\chi \in$

$\hat{H}^2(G, l^*) \subset Br(k)$. let $\hat{a}$ be image of a in $\hat{H}^0(G, J_l)$, then we have

$$inv(\bar{a}.\delta_\chi) = \sum_v inv_v(\hat{a}.\delta_\chi)$$

The map $l^* \to J_l \to l^v$ induces

$$\hat{H}^2(G, l^*) \xrightarrow{\text{j}} \hat{H}^2(G, J_l) \xrightarrow{\text{res}} \hat{H}^2(G_v, l^v)$$

by definition $inv_v(\hat{a}.\delta_\chi) = inv_v(j.res(\hat{a}.\delta_\chi)) = inv_v(\hat{a}.\delta_{\chi_v}) = \chi_v(\psi_v(a))$

$$\chi(\psi_{l/k}(a)) = \chi(\prod_v \psi_v(a)) = \sum_v \chi_v(\psi_v(a)) = \sum_v inv_v(\hat{a}.\delta_\chi)$$

Since we proved reciprocity law for cyclotomic extension, we have $\chi(\psi_{l/k}(a)) = 0$, implies $\sum_v inv_v(\hat{a}.\delta_\chi) = 0$. This proves the lemma for cyclotomic case.
To prove the general case we show that every $a \in Br(k)$ comes from a cyclic cyclotomic extension. For a Galois extension l/k we have the exact sequence

$$0 \to \hat{H}^2(G, l^*) \xrightarrow{\text{infl}} Br(k) \xrightarrow{\text{res}} Br(l)$$

From the above exact sequence we have $res_{l/k}(a) = 0$ if and only if $a \in Br(k)$ comes from a $\hat{H}^2(G, l^*)$. let w be a prime of l whose restriction to k is v. locally we know

$$inv_w(res_{l/k}(a)) = [l_w : k_v]inv_v(a)$$

Therefore $res_{l/k}(a) = 0$ if and only if $[l_w : k_v]inv_v(a) = 0$ for all w over v. So we need to find a cyclic cyclotomic extension l/k such that $[l_w : k_v]inv_v(a) = 0$ for every v. But $inv_v(a) = 0$ for almost all v, hence we boil down to proving the lemma

Lemma 6.9. *Given a finite set of primes $S \subset \mathfrak{M}_k$ and a positive integer z. There exists a cyclic cyclotomic extension l over k such that $[l_w : k_v]$ is divisible by z at non archimedean places and by 2 at archimedean places.*

Proof. t be a positive integer and p an odd prime. let $m = \mathbb{Q}(\zeta_{p^t})$, then $G(m/k) \cong \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}/p^{t-1}\mathbb{Z}$. let m' be field with Galois group $\mathbb{Z}/p^{t-1}\mathbb{Z}$

$$[m : m'] = p - 1$$

$$\Rightarrow [m_q : m'_q] \leq p - 1$$

for a prime q. Hence we have $[m'_q; \mathbb{Q}_q] \to \infty$ as $t \to \infty$.

Now for $p = 2$, take $m = \mathbb{Q}(\zeta_{2^t})$. If ζ is a primitive element then $\mathbb{Q}(\zeta - \zeta^{-1})$ forms a cyclic group of order 2^{t-2}. Since $i \in \mathbb{Q}(\zeta - \zeta^{-1})$, $\mathbb{Q}(\zeta - \zeta^{-1})$ is complex. Hence the local degrees are divisible by 2. So given $z = \prod p_i^{n_i}$ the required l would be the compositum of required fields generated above. $\square$

$\square$

By the above theorem we have $\chi(\psi_{l/k}(a)) = 0$ for all characters χ hence $\psi_{l/k}(a) = 1$. This proves the reciprocity law.

Lemma 6.10. *For abelian extension l/k and l'/k' we have*

$$\begin{array}{ccc} J_{k'} & \xrightarrow{\psi_{l'/k'}} & Gal(l'/k') \\ \downarrow N_{k'/k} & & \downarrow res \\ J_k & \xrightarrow{\psi_{l/k}} & Gal(l/k) \end{array}$$

Proof. let S' denote the finite set of primes consisting ramified and archimedean primes.

$$\begin{array}{ccccc} J_{k'}^{S'} & \xrightarrow{j} & I_{k'}^{S'} & \xrightarrow{F_{l'/k'}} & Gal(l'/k') \\ \downarrow N_{k'/k} & & \downarrow N_{k'/k} & & \downarrow res \\ J_k^S & \xrightarrow{j} & I_k^S & \xrightarrow{F_{l/k}} & Gal(l/k) \end{array}$$

let S denote the restriction of these primes to l. Fix a prime v of k not in S. let $\alpha \in J_{k'}^{S'}$ such that $\alpha_w = 1$ for all $w \not| v$.

$$N_{k'/k}(j(\alpha)) = N_{k'/k}(\sum_{w|v} w(\alpha_w)w) = \sum_{w|v} w(\alpha_w)N_{k'/k}(w) = \sum_{w|v} w(\alpha_w)f_w v$$

$N_{k'/k}(\alpha)_v = \prod_{w|v} N_{k'_w/k_v}\alpha_w$ Hence

$$j(N_{k'/k}(\alpha) = \sum_{w|v} j(N_{k'_w/k_v}\alpha_w) = \sum_{w|v} v(N_{k'_w/k_v}\alpha_w)v = \sum_{w|v} w(\alpha_w)f_w v$$

This proves the left rectangle. let σ_w denote the Frobenius element for the unramified extension l'_w/k'_v.

$$F_{l/k}N_{k'/k}w = F_{l/k}f_w v = (\sigma_v)^{f_w}$$

$$res(F_{l'/k'}w) = res(\sigma_w) = \sigma_v^{f_w}$$

This proves the second rectangle. But $\psi_{l/k}(x) = F_{l/k}(x)^S$ for all $x \in J_k^S$. Hence $F_{l/k} \circ j = \psi_{l/k}$, thus we have shown

$$\begin{array}{ccc} J_{k'}^{S'} & \xrightarrow{\psi_{l'/k'}} & Gal(l'/k') \\ \downarrow N_{k'/k} & & \downarrow res \\ J_k^S & \xrightarrow{\psi_{l/k}} & Gal(l/k) \end{array}$$

The lemma follows from the fact that $k^* J_k^S$ is dense in J_k. □

Substituting k' and l' by l we have $\psi_{l/k}(N_{l/k}J_l) = 1$, hence $\psi_{l/k}(k^* N_{l/k} J_l) = 1$. Since $C_k/N_{l/k}C_l \cong J_k/k^* N_{l/k} J_l$ we can define the map

$$\psi_{l/k} : C_k/N_{l/k}C_l \to Gal(l/k)$$

Using the cohomology inequalities we now show that this is indeed an isomorphism.
Surjectivity: We note two lemmas of the first inequality

Lemma 6.11. *If D is a subgroup of J_k satisfying $(a) D \subset N_{l/k}J_l$ and $(b) k^* D$ is dense in J_k then $l = k$*

Proof. Consider a cyclic field extension M over k in l. From local theory $N_{M_w/k_v} {M_w}^*$ are open sets of k_v and contain U_v for all v unramified. This implies $N_{M/k}J_M$ is open so closed in J_k. Hence $k^* N_{M/k} J_M$ is closed in J_k. $D \subset N_{l/k} J_k \subset N_{M/k} J_M$, from hypothesis we have $k^* N_{M/K} J_M$ dense J_k. Hence is entire J_k and from first inequality $M = k$, implying $l = k$. □

Lemma 6.12. *let S be finite set of primes in $\mathfrak{M}_k$ containing the archimedean and ramified primes. For a finite abelian extension l/k the map $F_{l/k} : I^S \to Gal(l/k)$ is surjective.*

Proof. let H be subgroup of G generated by $F_{l/k}v$ for all $v \notin S$ and $M = l^H$. For v unramified since $Gal(M/k) = G/H$ $F_{l/k}v(x) = x$ for all $x \in M$. Hence $M_w = k_v$ for all $v \notin S$, this implies from local theory $k_v = N_{M_w}/k_v M_w$. let $D = {J_k}^S$ $D \subset N_{M/k}J_M$ and from weak approximation theorem $D^* J_k^S$ is dense in J_k. From above consequence we conclude $M = k$ hence $H = G$. Since $\psi_{l/k}(x) = F_{l/k}((x)^S)$ for all $x \in J_k^S$ we have $\psi_{l/k}$ surjective. □

Injectivity follows from the second inequality. $\hat{H}^0(G, C_l) = C_k/N_{l/k}C_l$ divides $[l : k]$ hence if $[\hat{H}^0(G, C_l)] \leq [l : k]$ we have $[\hat{H}^0(G, C_l)] = [l : k]$. And injectivity follows from surjectivity.

In this section we prove the diagram

$$\begin{array}{ccc} C_k/N_{M/k}C_M & \xrightarrow{\psi_{M/k}} & Gal(M/k) \\ \downarrow j & & \downarrow res \\ C_k/N_{l/k}C_l & \xrightarrow{\psi_{l/k}} & Gal(l/k) \end{array}$$

j in the above diagram is the natural injection obtained by observing that $N_{M/k}C_M \subset N_{l/k}C_l$. Consider fields $l' \supset l$ and $k' \supset k$ such that l/k and l'/k' are finite abelian extensions.

Now in the commuatative diagram proved in the last subsection put $l' = M$ and $k' = k$. We can replace J_k by C_k since $\psi(k^*) = 1$. Taking kernel will preserves the commutativity. Thus the diagram follows. From this commuatative diagram we can pass to inverse limit to get homomorphism

$$\psi_k : C_k \to \varprojlim G(l/k) \cong G(k^{ab}/k)$$

where l runs through finite abelian extensions and k^{ab} is maximal abelian extension. Thus we have

$$G(k^{ab}/k) \cong \varprojlim (C_k/N_{l/k}l^*)$$

Thus if we prove existence theorem we will have

$$G(k^{ab}/k) \cong \varprojlim (C_k/N)$$

where N runs though open subgroups of finite index of C_k.

Throught this section H denotes an open subgroup of C_k of finite index n. Call H normic if and only if there exists an abelian extension L/k so that $H = N_{L/k}C_L$. Observe two points

1. If H is normic and is contained in H_1 then H_1 is normic. Let $H = N_{L/k}C_L$ we have the isomorphism $\psi_{L/k} : C_k/H \to G$. Say $\psi_{L/k}(H_1) = G_1$, this gives a map $\psi_{L^{G_1}/k} : C_k \to G/G_1$ with kernel $H_1 = N_{L_{G^1}/k}C_{L_{G^1}}$.
2. Similarly we can also show that if H_1, H_2 are normic so is $H_1 \cap H_2$.

Lemma 6.13. *Let n be a prime and k a field not of characteristic n and containing the n^{th} roots of unity. Then H is normic.*

Proof. Let H' be inverge image of H in J_k. Since H' is open for some finite set S, $\prod_{v\in S} 1 \times \prod_{v\notin S} U_v \subset H'$. H is of index n, so $J_k^n \subset H'$. Since H' is a group we have $\prod_{v\in S} k^{*n} \times \prod_{v\notin S} U_v \subset H'$. By the proof of second inequality there exists an abelian extension l such that $k^*N_{l/k}j_l = k^* \prod_{v\in S} k^{*n} \times \prod_{v\notin S} U_v = k^*U$, say. Thus $N_{l/k}C_l = Uk^*/k^* \subset H'/k^* = H$, Since H contains a norm group, itself is a norm group. □

Lemma 6.14. *If L/k is cyclic and $N_{L/k}^{-1}(H)$ is normic in L then H is normic.*

We use induction on index for proof of existence theorem. Let $[C_k : H] = n$ and p be a prime dividing n. If $n = 1$ then k itself suffices as the abelian extension. Let $k_1 = k[\zeta_p]$ and $H_1 = N_{k_1/k}^{-1}H$, then by above lemma it is enough to show H_1 is normic. $N_{k_1/k} : C_{k_1}/N_{k_1/k}H_1 \to C_k/H$ is injective hence $[C_{k_1} : H_1]$ divides $[C_k : H]$. $[C_{k_1} : H_1] = n$ otherwise by induction hypothesis H_1 is normic.

Choose H_2 such that $H \subset H_2$ and $[C_{k_1} : H_2] = p$. H_2 is normic since it is of prime index. Say $H_2 = N_{m/k}m^*$, m is a cyclic extension. $H_3 = N_{m/k_1}^{-1}H_1$. $N_{m/k_1} : C_m/H_3 \to C_{k_1}/H_1$ is injection with image H_2/H_1. Hence $[C_m/H_3] < [C_{k_1}/H_1] = n$, by induction hypothesis H_3 is normic. Applying previous lemma H_1 is normic. This implies H is normic. This proves the existence theorem.

Chapter 7

Conclusion

For a local field k, we have seen that for every finite extension l/k there exists a subgroup N of k^* such that we have an isomorphism

$$\theta_{l/k} : k^*/N \to Gal(l/k)^{ab}$$

This N is equal to $N_{l/k}l^*$.

For a number field k we have seen that for every finite abelian extension l/k we have isomorphism

$$\psi_{l/k} : C_k/N_{l/k}C_l \to Gal(l/k)$$

For a number field k we have constructed the map

$$\psi_k : C_k \to \varprojlim G(l/k) \cong G(k^{ab}/k)$$

Existence theorem gives us correspondence between norm subgroups of finite index in C_k and finite abelian extensions. Thus we have

$$G(k^{ab}/k) \cong \varprojlim(C_k/N)$$

where N runs though open subgroups of finite index of C_k.

Bibliography

[CF10] J.W.S. Cassels and A. Fröhlich. *Algebraic Number Theory: Proceedings of an Instructional Conference Organized bY the London Mathematical Society (a NATO Advanced Study Institute) with the Support of the International Mathematical Union.* London Mathematical Society, 2010.