TU KAISERSLAUTERN

DOCTORAL THESIS

Computation of the Local Fundamental Classes

Author:
Aslam Ali

Supervisor:
Prof. Dr. Claus Fieker

A thesis submitted in fulfilment of the requirements
for the degree of Master of Science

in the

July 3, 2020

I, Aslam Ali, declare that this thesis titled, 'Computation of the Local Fundamental Classes' and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed: _____

_____ Date: _____

“Thanks to my solid academic training, today I can write hundreds of words on virtually any topic without possessing a shred of information, which is how I got a good job in journalism.”

Dave Barry

Abstract

The Thesis Abstract is written here (and usually kept to just this page). The page is kept centered vertically so can expand into the blank space above the title too…

Acknowledgements

The acknowledgements and the people to thank go here, don't forget to include your project advisor...

Contents

List of Figures

List of Tables

For/Dedicated to/To my...

Chapter 1

Preleminaries

1.1 Basic Definitons

In my research I will be working mostly on number fields. A field extension L/K is said to be algebraic if every element $\alpha \in L$ is algebraic over K, that is, for every $\alpha \in L$ there exists some nonzero polynomial in $f \in K[x]$ such that α is a zero of f. In my work I will always assume the algebraic field extension. The algebraic field extension L/K is called an algebraic number field when $K = \mathbb{Q}$.

Definition 1.1.1. A Galois field extension is an algebraic field extension L/K which is normal and separable.

In the Galois field extension L/K, the Galois group $\mathrm{Gal}(L/K)$ is the set of all automorphisms of L, denoted by $\mathrm{Aut}(L/K)$, which fixes the elements of K, that is, the base field satifies $K = L^{\mathrm{Aut}(L/K)}$. In fact the fundamental theorem of Galois theory asserts that for any finite Galois field extension L/K, there is a one to one correspondence between its intermediate fields and subgroups of its Galois group which we will apply in many places in our computations. For any subgroup $H \subset \mathrm{Gal}(L/K)$, L^H denotes the fixed field corresponding to the group H. An element $\alpha \in L$ is said to be integrable over $\mathbb{Z}$ if there exists some monic polynomial $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$

Definition 1.1.2. The maximal order for an extension $L/\mathbb{Q}$ is denoted by $\mathcal{O}_L$ or $\mathbb{Z}_L$ is the set of all integrable elements of L over $\mathbb{Z}$.

An order of R of any number field L is a unitary subring $R \subset L$ which is finitely generated as $\mathbb{Z}$-module and field of fractions $Q(R) = L$. One can find the details of computation of maximal order in the lecture note of Fieker.

Definition 1.1.3. Let R be a commutative and unitary integral domain and $Q(R)$ its field of fractions. An R-submodule $B \leq Q(R)$ is called a fractional ideal if there exists $0 \neq \alpha \in R$ such that $\alpha \cdot B \subset R$. A fractional ideal A is said to be invertible if there is some fractional ideal B such that $AB = R$.

Fractional ideals are not ideals in the usual sense.

Theorem 1.1.4. *Let L be an algebraic number field with maximal order $\mathcal{O}_L$, then the fractional ideals of $\mathcal{O}_L$ form an abelian and it is denoted by I_L. The identity element is $1 = \mathcal{O}_L$ and the inverse of a fractional ideal A is*

$$A^{-1} = \{x \in \mathcal{O}_L \mid xA \subset \mathcal{O}_L\} = [O_L : A].$$

Proof. [Neu99a], Proposition 3.8. □

The fractional principal ideal $(\alpha) = \alpha\mathcal{O}_L, \alpha \in L^\times$, form a subgroup of the group of ideals I_L, which we denote by P_L. The quotient group $I_L/P_L = Cl_L$ is finite and called the ideal class group of L. The cardinality of this group Cl_L is called the class number for L and it is denoted by h_L. One can see [Fie06] for details on the computation of ideal class group.

Theorem 1.1.5. *Let $\mathcal{O}$ be any order of a number filed, then there are unit $\zeta, \epsilon_1, \ldots, \epsilon_r \in \mathcal{O}^*$ such that*

1. *torsion unit group $TU(\mathcal{O}) = \langle\zeta\rangle$,*
2. *$(\epsilon_i)_i$ are free,*
3. *$\mathcal{O}^* = \langle\zeta, \epsilon_1, \ldots, \epsilon_r\rangle$.*

If $\mathcal{O}$ is the maximal order of number field L then $r = r_1 + r_2 - 1$ is the rank of unit group of $\mathcal{O}$, where r_1 is the number of real embeddings and r_2 is the number of conjugates pairs of complex embeddings of L. For any Galois field extension $L/\mathbb{Q}$ of degree n, either $r_1 = 0$ or $r_2 = 0$ and $n = r_1 + 2 \cdot r_2$.

Definition 1.1.6. Let K be a field. A discrete valuation on K is a function $\mathrm{v} : K \to \mathbb{Z} \cup \{\infty\}$, such that for every $x, y \in K$,

V1. $\mathrm{v}(x) = \infty$ if and only if $x = 0$,

V2. $\mathrm{v}(xy) = \mathrm{v}(x) + \mathrm{v}(y)$ and

V3. $\mathrm{v}(x+y) \geq \min(\mathrm{v}(x), \mathrm{v}(y))$.

Each discrete valuation on K induces a non-archimedian absolute value via $|x| = c^{\mathrm{v}(x)}$, where c is any constant with $0 < c < 1$.

An absolute $|\cdot|$ value on K defines a metric via $d(a,b) = |a-b|$ and hence form a topology on K. For any element $a \in K$, one can define the open neighbourhood of a as

$$U(a,\delta) = \{x \in K \mid |x-a| < \delta\}, \delta > 0.$$

Let $|\cdot|_1$ and $|\cdot|_2$ be two absolute values on K. From [Neu99a], they are equivalent iff $\exists\ r > 0$ such that we have $|x|_1 = |x|_2^r$ for all $x \in K$. Let K be an algebraic number field, then an equivalence class of valuations on K is called a prime or place of K.

Theorem 1.1.7. *Let K be a number field, then there is exactly one prime of K*

1. *for each prime ideal $\mathfrak{p}$ of K,*
2. *for each real embedding of K,*
3. *for each conjugate pair of complex embeddings of K.*

Proof. Milne's note □

1.2 Local Field

Example 1.2.1. *On the field of rational $\mathbb{Q}$, for every prime p, the p-adic valuation $\mathrm{v}_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ can be defined as*

$$\mathrm{v}_p(p^a \cdot \frac{r}{s}) = a$$

where p does not divide r and s.

In fact one can induce a non archimedian p-adic absolute value $|\cdot|_p$ on $\mathbb{Q}$ as

$$|\alpha|_p = p^{-\mathrm{v}_p(\alpha)}.$$

Theorem 1.2.2. *The non-trivial absolute values on $\mathbb{Q}$ are equivalent to $|\cdot|_p$ or the ordinary absolute value $|\cdot|_\infty$.*

Proof. [Neu99a] □

A field L together with an absolute value $|\cdot|$ is said to be complete if every Cauch sequnce in L converges in L, that is for evry sequence (a_n) of L, and $m, n \to \infty$ with $|a_n - a_m| \to 0$, there exists $a \in L$ such that $|a_n - a| \to 0$.

Theorem 1.2.3. *Let $(K, |\cdot|_K)$ be a pair of complete field with respect to a discrete absolute value $|\cdot|_K$ and suppose L/K be a finite separable extension of degree n. Then $|\cdot|_K$ can be extneded uniquely to a discrete absolute value $|\cdot|_L$ and $(L, |\cdot|_L)$ is complete with respect to $|\cdot|_L$ and for all $\alpha \in L$,*

$$|\alpha|_L = |N_{L/K}(\alpha)|_K^{1/n}.$$

Proof. Cassels □

$\mathbb{Q}_p$ is the completion of the $\mathbb{Q}$ with non-archimedian absolute value $|\cdot|_p$, that is, every Causchy sequence in $\mathbb{Q}_p$ converges with respect to $|\cdot|_p$. The p-adic absolute value satisfies $|a + b|_p \leq \max\{|a|_p, |b|_p \leq |a|_p + |b|_p\}$.

In this we are mainly interested in the local fields of characteristic zero which are finite extension of $\mathbb{Q}_p$ for any prime number p.

Proposition 1.2.4. *Let L together with non archimedian absolute value $|\cdot|$ is a finite extension of $\mathbb{Q}_p$, then $\mathcal{O}_L = \{x \in L \mid |x| \leq 1\}$ is a ring with unit group $\mathcal{O}_L^* = \{x \in L \mid |x| = 1\}$ and the unique maximal ideal $\mathfrak{p}_L = \{x \in L \mid |x| < 1\}$.*

Proof. [Neu99a], Proposition 3.8. □

The ring $\mathcal{O}_L$ of L is said to be the ring of integers of L and the quotient $\mathcal{O}_L/\mathfrak{p}_L$ is called residue class field of L. An element $\pi_L \in \mathcal{O}_L$ is said to be a uniformizing element or prime element if $\mathrm{v}_L(\pi_L) = 1$. Every element a of L^* can be uniquely represented as $a = \pi_L^m \cdot u$ where $m \in \mathbb{Z}$ and u is a unit in $\mathcal{O}_L^*$. In particular for p-adic field $\mathbb{Q}_p$ we have the ring of integers is $\mathbb{Z}_p = \mathcal{O}_{\mathbb{Q}_p} = \{a \in \mathbb{Q}_p \mid |a|_p \leq 1$ and the unique maximal ideal is $\mathfrak{P} = \{a \in \mathbb{Z}_p \mid |a|_p > 1\}$. The residue class field of $\mathbb{Q}_p$ is $\mathbb{Z}_p/\mathfrak{P} \cong \mathbb{Z}/p\mathbb{Z}$. Every element a of $\mathbb{Q}_p^*$ can be expressed uniquely as

$$a = p^m \cdot u \text{ where } m \in \mathbb{Z} \text{ and } u \in \mathbb{Z}_p^*$$

For L together with non-archimedian absolute value, we obtain the descending chain

$$\mathcal{O}_L \supseteq \mathfrak{p}_L \subseteq \mathfrak{p}_L^2 \subseteq \mathfrak{p}_L^3 \subseteq \cdots$$

of the ideals of $\mathcal{O}_L$ which forms a basis of neighbourhoods of the zero element where $\pi_L^n = \{x \in L \mid |x| < q^{-(n-1)}\}$ where $q = |\mathcal{O}_L/\mathfrak{p}_L| > 1$. Similary a basis of the element 1 of K^*, we have the

chain $\mathcal{O}_L^* = U_0 \supseteq U_1 \supseteq U_2 \supseteq U_3 \cdots$ of the subgroups of O_L^* where U_n is defined as

$$U_n = 1 + \mathfrak{p}_L^n = \left\{ x \in L^* \mid |x-1| < \frac{1}{q^{n-1}} \right\}$$

for $n > 0$. The subgroup U_n of $\mathcal{O}_{L^*}$ is called n-th higher unit group and the U_1 the principal unit group. Let us define the surjective homomorphism

$$\mathcal{O}_L^* \to (\mathcal{O}_L/\mathfrak{p}_L^n),\ x \mapsto x \bmod \mathfrak{p}_L^n.$$

Which has kernel U_n thus one obtains $\mathcal{O}_L^*/U_n \cong (\mathcal{O}_L/\mathfrak{p}_L^n)^*$. Similary if we define the surjective homomorphism $U_n \to \mathcal{O}_L/\mathfrak{p}_L$ by $x = 1 + \pi_L a \mapsto a \bmod \mathfrak{p}_L$, which has kernel clearly U_{n+1}. Therefore, we obtain $U_n/U_{n+1} = \mathcal{O}_L/\mathfrak{p}_L$.
In the thirs chapter we define the exponential function and logarithmic function the finite extension $L/\mathbb{Q}_p$ which link between U_n and $\mathfrak{p}_L$.

Definition 1.2.5. Let L/K be a finite extension of local fields over $\mathbb{Q}_p$ then L is called unramified over K if the residue class field $\mathcal{O}_L/\mathfrak{p}_L$ of L is a separable extnension of the residue class field of $\mathcal{O}_K/\mathfrak{p}_K$ of K and

$$[L : K] = [\mathcal{O}_L/\mathfrak{p}_L : \mathcal{O}_K/\mathfrak{p}_K].$$

The field L is called tamely ramified over K if the residue class field $\mathcal{O}_L/\mathfrak{p}_L$ of L is a separable extnension of the residue class field of $\mathcal{O}_K/\mathfrak{p}_K$ of K and $\mathrm{GCD}([L : K], p) = 1$ else it is wildly ramified.

In the capter "Norm Equation" we go through details of local fied extension over $\mathbb{Q}_p$.

[Neu99a, Lor08]: Theorem5.7

1.3 Global Field

A global field is an algebraic number field or a fuction field in one variable over a finite field. We only work over the case of finite extension of $\mathbb{Q}$. Let L/K be a finite Galois extension of the number fields with Galois grouop $G = \mathrm{Gal}(L/K)$. If $K \neq \mathbb{Q}$ then it L is said to be a relative field extension and in this case we have $\mathbb{Q} \leq K \leq L$. Let v be the valuation on K. If v is an archimedian valuation the the localization of K at v denoted by K_v is either $\mathbb{R}$ or $\mathbb{C}$ otherwise K_v is a finite extension p-adic field for some prime number p. Let w be a valutation of L then for every $\sigma \in G$, $w \circ \sigma$ also extends v, so the group G acts on the set of of extensions $w \mid v$.

Proposition 1.3.1. *Let L/K be a Galois field extension, then the Galois group $G = \mathrm{Gal}(L/K)$ acts transtively on the set of extensions $w \mid v$.*

Proof. [Neu99a], Proposition 9.1. □

Definition 1.3.2. For any finite Galois field extension L/K with valuation v of K, the decomposition group of an extension w of v to L is definies as

$$G_w = \{\sigma \in \mathrm{Gal}(L/K) \mid w \circ \sigma = w.\}$$

For non-archimedian valuation v let w be an extension to v. Let $\mathcal{O}_K$ and $\mathfrak{p}_K$ are the ring of integers and the maximal ideal respectively with respect to valuation v and similarly $\mathcal{O}_L$ and $\mathfrak{p}_L$ are the ring of integers and the maximal ideal respectively with respect tor valuation w. Then we obtain Inertia group denoted by I_w and the ramification group denoted by R_w which are defined below:

$$I_w := \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma x \equiv x \bmod \mathfrak{p}_L \text{ for all } x \in \mathcal{O}_L\}$$

and

$$R_w = \{\sigma \in \mathrm{Gal}(L/K) \mid \frac{\sigma x}{x} \equiv 1 \bmod \mathfrak{p}_L \text{ for all } x \in L^*\}.$$

In fact they satisfy $G_w \supseteq I_w \supseteq R_w$. From Proposition 9.9 of [Neu99a], the residue class field extension $\mathcal{O}_L/\mathfrak{p}_L/\mathcal{O}_K/\mathfrak{p}_K$ is normal and satisfies the following an exact sequence:

$$1 \to I_w \to G_w \to \mathrm{Gal}(\mathcal{O}_L/\mathfrak{p}_L/\mathcal{O}_K/\mathfrak{p}_K) \to 1.$$

Suppose L_w be the completion of L with respect to w and K_v be the completion of K with respect to v then one obtains $G_w = \mathrm{Gal}(L_w/K_v)$. From [Neu99a], one also gets

$$[L : K] = \prod_{w|v} [L_w : K_v]$$

and $N_{L/K}(a) = \prod_{w|v} N_{L_w/K_v}(a)$ and $\mathrm{T}_{L/K}(a) = \sum_{w|v} \mathrm{T}_{L_w/Kv}(a)$ where N and T are the norm and trace functions respectively.

Chapter 2

Introduction

2.1 Introduction

Let L/K be any global field extension of characteristic 0 and p be any prime in K and $\mathfrak{P}$ be the prime in L over Kp. Then $L_{\mathfrak{P}}/K_p$ be the corresponding local p-adic field extension. We want to compute the particular element $u_{L_{\mathfrak{P}}/K_p}$ of $H^2(\mathrm{Gal}(L_{\mathfrak{P}}/K_p), L_{\mathfrak{P}}^{\times})$ such that $\mathrm{inv}(u_{L_{\mathfrak{P}}/K_p}) = 1/[u_{L_{\mathfrak{P}}:K_p}]$. The element $u_{L_{\mathfrak{P}}/K_p}$ is called the local fundamental class which maps

$$u_{L_{\mathfrak{P}}/K_p} : \mathrm{Gal}(L_{\mathfrak{P}}/K_p) \times \mathrm{Gal}(L_{\mathfrak{P}}/K_p) \to L_{\mathfrak{P}}^{\times}.$$

Before going to the details of the algorithm we will present the details of the cohomology group and the maps and other necessary definitions and some results.

Definition 2.1.1. The group ring $\mathbb{Z}[G]$ of a group G consists of the finite formal sums of group elements with coefficients in $\mathbb{Z}$ i.e.

$$\mathbb{Z}[G] = \left\{ \sum a_g g \mid a_g \in \mathbb{Z} \ \ \forall g \in G, \text{ all but finitely many } a_g = 0 \right\}$$

The operations are defined as

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g$$

and

$$\left\{ \sum_{g \in G} a_g g \right\} \left\{ \sum_{g \in G} b_g g \right\} = \sum_{g \in G, k \in G} \left(a_k b_{k^{-1} g} \right) g.$$

Let G be a finite group and the complete free resolution of the group G be

$$\cdots \xleftarrow{d_{-2}} X_{-2} \xleftarrow{d_{-1}} X_{-1} \xleftarrow{d_0} X_0 \xleftarrow{d_1} X_1 \xleftarrow{d_2} X_2 \xleftarrow{d_3} \cdots$$

where, $X_q = X_{-q-1} = \bigoplus \mathbb{Z}[G](\sigma_1, \ldots, \sigma_q)$ and for $q = 0$ we assume

$$X_0 = X_{-1} = \mathbb{Z}[G],$$

where we choose the identity element $1 \in \mathbb{Z}[G]$ as the generating 0-tuple. X_q's are free G-modules and d_q are G-homomorphisms.
For A a G-module, define the group of q cochains

$$A_q = C^q(G, A) = \mathrm{Hom}_G\,(X_q, A) =: A_{-q-1},$$

which consists of all G-homomorphisms $x : X_q \to A$. Then, we obtain the sequence
$\cdots \xrightarrow{\delta_{-2}} A_{-2} \xrightarrow{\delta_{-1}} A_{-1} \xrightarrow{\delta_0} A_0 \xrightarrow{\delta_1} A_1 \xrightarrow{\delta_2} A_2 \xrightarrow{\delta_3} \cdots.$
where, $\delta_{q+1} \circ \delta_q = 0$ due to $d_q \circ d_{q+1} = 0$. Therefore, $\mathrm{Im}\,\delta_q \subset \ker \delta_{q+1}$.
One can find the details of the maps d_q and $\delta_q : A_{q-1} \longrightarrow A_q$ in book Sharifi, Neukirch : The cohomology groups measure how far the q-cochain complex $C(G, A)$ is from being exact. $Z^q = \ker \delta_{q+1}$, $R^q = \mathrm{Im}\,\delta_q$ and call the elements in Z^q the q- cocycles and the elements in R^q as q-coboundaries.

Definition 2.1.2. Let G be a finite group and A be a G-module. Then the q^{th} cohomology group of G with coefficients in A is defined as $\hat{H}^q\,(G, A) = Z^q/R^q$, which is also said to be the Tate cohomology group of dimension (degree) q of the G-module A.

For $q \in \mathbb{Z}$ we also write q^{th} Tate cohomology group as

$$\hat{H}^q\,(G, A) = \begin{cases} H_{-q-1}\,(G, A) \text{ if } q \leq -2 \\ H_0\,(G, A) \text{ if } q = -1 \\ H^0\,(G, A) \text{ if } q = 0 \\ H^q\,(G, A) \text{ if } q \geq 1 \end{cases}$$

where, $H^q\,(G, A)$ are the usual cohomology groups and $H_q\,(G, A)$ are the usual homology groups. From now on $H^q\,(G, A)$ denotes the Tate cohomology groups. Our main target is to compute the the local fundamental class in $H^2\,(G, A)$.

2.1.1 Mappings on Cohomology

In this section we study how these groups behave in case either the module A or the group G changes.

If A and B are two G-modules and $f : A \to B$ be a G-homomorphism, then f canonically induces a homomorphism

$$\bar{f}_q : H^q(G, A) \to H^q(G, B) \tag{2.1}$$

which arises in the following way:
Let A_q and B_q be the cochains of A and B respectively. From the map

$$x(\sigma_1, \ldots, \sigma_q) \mapsto fx(\sigma_1, \ldots, \sigma_q)$$

we get a homomorphism $f_q : A_q \to B_q$ with the property that $\delta_{q+1} \circ f_q = f_{q+1} \circ \delta_{q+1}$. Therefore these maps fit into the infinite commutative diagram:

$$\begin{array}{ccccccc} \cdots & \longrightarrow & A_q & \xrightarrow{\delta_{q+1}} & A_{q+1} & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle f_q} & & \downarrow{\scriptstyle f_{q+1}} & & \\ \cdots & \longrightarrow & B_q & \xrightarrow{\delta - q+1} & B_{q+1} & \longrightarrow & \cdots \end{array}$$

which means precisely that $x(\sigma_1, \ldots, \sigma_q) \mapsto fx(\sigma_1, \ldots, \sigma_q)$ takes cocycles to cocycles and coboundaries to coboundaries and hence we obtain (1). If $c \in H^q(G, A)$, the image $\bar{f}_q c$ is obtained by choosing a cocycle x from the class c, and taking the cohomology class of the cocycle fx of the module B.

Proposition 2.1.3. *If* $0 \to A \xrightarrow{i} B \xrightarrow{j} C \to 0$ *is an exact sequence of G-modules and G-homomorphisms, then there exists a canonical homomorphism*

$$\delta_q : H^q(G, C) \to H^{q+1}(G, A).$$

The map δ_q *is called the connecting homomorphism or also the* δ*-homomorphism.*

Theorem 2.1.4. *Let* $0 \to A \xrightarrow{i} B \xrightarrow{j} C \to 0$ *be an exact sequence of G-modules and G-homomorphisms. Then the induced infinite sequence*

$$\cdots \to H^q(G, A) \xrightarrow{\bar{i_q}} H^q(G, B) \xrightarrow{\bar{j_q}} H^q(G, C) \xrightarrow{\delta_q} H^{q+1}(G, A) \to \cdots$$

is also exact. It is called the **long exact cohomology sequence.**

Definition 2.1.5. Let U be a subgroup of G

1. Let $e : U \to G$ be the inclusion map. Then the maps $\mathrm{res} : H^i(G, A) \to H^i(U, A)$ induced by the compatible pair (e, Id_A) on cohomology where Id_A is the identity map on A, are known as restriction maps.

2. Suppose that U is normal in G. Let $q : G \to G/U$ be the quotient map and let $i : A^U \to A$ be the inclusion map. Then the maps

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

induced by the pair (q, i) are known as inflation maps.

Theorem 2.1.6. *Let G be a cyclic group and let A be a G-module. Then*

$$H^q(G, A) \cong H^{q+2}(G, A) \text{ for all } q \in \mathbb{Z}.$$

Theorem 2.1.7. *Let G be a finite group and $V \leq G$ and for each $n \in \mathbb{Z}$, the homomorphism*

$$\delta^2 : H^2(V, \mathbb{Z}) \to H^{n+2}(V, C)$$

is given by the cup-product $\alpha \mapsto \mathrm{res}^G_V(u) \cup \alpha$. Then the following statements are equivalent:

1. *$C(u)$ is a cohomologically trivial $G-$module,*
2. *C is a class module with fundamental class,*
3. *δ^2 is an isomorphism for all $n \in \mathbb{Z}$.*

Remark 2.1.8. If C is a class module for group G then from above theorem we obtain an isomorphism map

$$(\delta^2)^{-1} : H^2(V, C) \to H^0(V, \mathbb{Z}), \quad u_V \mapsto \frac{1}{\#V} \mod \mathbb{Z},$$

where $u \in H^2(G, C)$. This map is called an invariant map and we denote it by inv.

Definition 2.1.9. Let L/K be a normal extension. The uniquely determined element $u_{L/K} \in H^2(L/K)$ such that

$$\mathrm{inv}_{L/K}(u_{L/K}) = \frac{1}{[L : K]} + \mathbb{Z}$$

is called the fundamental class of L/K.

Proposition 2.1.10. *Let $N \supset L \supset K$ be extensions with N/K normal. then*

1. *$u_{L/K} = (u_{N/K})^{[N:L]}$, L/K is normal,*
2. *$\mathrm{res}_L(u_{N/K}) = u_{N/L}$*

3. $\mathrm{cor}_K(u_{N/L}) = (u_{N/K})^{[L:K]}$.

Definition 2.1.11. A formation (G, A) (or $(G, \{G_K\}_{K\in X}, A)$) is called a class formation if it satisfies the following two axioms:

Axiom I: $H^1(L/K) = 1$ for every normal extension L/K.

Axiom II: For every normal extension L/K there is an isomorphism

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

the invariant map, with following properties:

(a) If $N \supset L \supset K$ is a tower of normal extensions, then

$$\mathrm{inv}_{L/K} = \mathrm{inv}_{N/K}|_{H^2(L/K)}.$$

(b) If $N \supset L \supset K$ is a tower of normal extensions with N/K normal, then

$$\mathrm{inv}_{N/L} \circ \mathrm{res}_L = [L:K] \cdot \mathrm{inv}_{N/K}\,.$$

Definition 2.1.12. Let $L/\mathbb{Q}$ be a number field extension and $\mathfrak{p}$ be the prime ideal of the ring of intgers $\mathcal{O}_L$ of L. A $\mathfrak{p}$-adic integer is defined as a sequence $\alpha = (\alpha_i)_{i\geq 0}$ where $\alpha_i \in \mathcal{O}_L/\mathfrak{p}^i$ and $\alpha_{i+1} \equiv \alpha_i \bmod \mathfrak{p}^i$. The set of all $\mathfrak{p}$-adic integers, denoted by $\mathcal{O}_{L,\mathfrak{p}}$, forms an integral domain and its field of fractions, denoted by $L_\mathfrak{p}$, is called ⊩-adic completion of L at ⊩.

Chapter 3

Norm Equation

3.1 Norm Equation

For an unramified extension to compute the Norm Equation we follow the Satoh's paper. Since we know $N(U_L) = N(U_K)$, where U_L and U_K are the unit groups of the Field L and K resp, we can say that every unit element in K is a normed element in L.
We present the algorithm to compute the Norm Equation in the Totally ramified p-adic field extension.

Algorithm 1

Input: L/K be totally ramified p-adic ring extension, $\pi \in L$ be uniformizer and $a \in K$.

Output: Find $x \in L$ such that $Norm(x) = a$.

1: Define $b := \frac{a}{N(\pi)^{V(a)}}$.
2: Solve $N(\tilde{x}) = b$.
3: Define F, f the residue field extensions of L and K resp.
4: Solve $N_{F/f}(\mu) = b \pmod{p}$.
5: Define $c := b/N(\mu)$.
6: Solve $N_{L/K}(\tilde{\tilde{x}}) = c$.
7: Return $x := \mu \cdot \pi^{(V(a))} \cdot \tilde{\tilde{x}}$.

Example:

```
> R<x>:=PolynomialRing(Rationals());
>  K:=pAdicField(5,30);
> L:=ext<K| x^7+25*x^2+5>;
>  k:=RingOfIntegers(K);
>  l:=RingOfIntegers(L);
>  a:=5*2/3*Random(k);
> IsUnit(a);
```

```
true
> pi:=UniformizingElement(l);
> b:=a/Norm(pi)^Valuation(a);
> U,mU:=UnitGroup(k);
> NormEquation(l,mU,b);
true -7873108737688188625O*l.1^6 + 74585038994062594375*l.1^5 - 561578353945002976251.1^4 - 52776966890
O(l.1^203)
> _,w:=$1;
> f,mf:=ResidueClassField(k);
> F,mF:=ResidueClassField(l);
> mf(b);
3
> mF(w);
2
> mu:=b/mF(w)@@ mF;
> mu in k;
true
> y:=mF(w)@@ mF;
> c:=b/Norm(y);
> NormEquation(l,mU,c);
true 425908428777211662501.1^6 + 261166486016455550001.1^5 - 735274593384855003751.1^4 + 460593183770
O(l.1^203)
> _,w1:=$1;
> w11:=w1*y*pi^Valuation(a);
> Norm(w11)/a-1;
O(5^28)
```

Now we give the next algorithm by changing the precxision.

Algorithm 2

Input: L/K be a finite totally ramified p-adic ring extension, $\pi \in L$ be uniformizer and $a \in K$ up to precision "n".

Output: Find $\alpha \in L$ such that $V(N(\alpha)/a - 1) \geq n$.

1: Figure out the precision of K and L.

2: Define L'/K' such that L'/K'" = "L/K and precision $(L') \geq n$.

3: Findin $\alpha \in L'$ using the previous algorithm such that $V'(N(\alpha)/a - 1) \geq n$.

4: Return $L!\alpha$

```
> R<x>:=PolynomialRing(Rationals());
>  K:=pAdicField(5,20);
> L:=ext<K|x^7+15>;
> k:=RingOfIntegers(K);
> l:=RingOfIntegers(L);
> pi:=UniformizingElement(l);
> a:=3*(1+k.1*Random(k));
> KK:=pAdicField(5,50);
> LL:=ext<KK|x^7+15>;
> kk:=RingOfIntegers(KK);
> ll:=RingOfIntegers(LL);
```

```
> UU,mUU:=UnitGroup(kk);
> KKa:=KK!a;
> ChangePrecision(~KKa,50);
> Parent(KKa);
5-adic field mod 5^50
> PI:=UniformizingElement(kk);
> bb:=KKa/Norm(PI)^Valuation(KKa);
> NormEquation(ll,mUU,bb);
true -6105615095200869000735533732265625*ll.1^6 +
    39519312090040221641210367427021875*ll.1^5 -
    44117491210717703484480794577856250*ll.1^4 +
    32233062018129624486956962421912 50*ll.1^3 +
    14367323616830108457959875907344750*ll.1^2 -
    38913080750009108811263908469198450*ll.1 +
    39504377608946897770758593522892959
> _,z:=$1;
> ff,mff:=ResidueClassField(kk);
> FF,mFF:=ResidueClassField(ll);
>  y:=mFF(z)@@ mFF;
>  Parent(y);
Totally ramified extension defined by the polynomial x^7 + 15
 over 5-adic ring mod 5^50
> FieldOfFractions($1);
Totally ramified extension defined by the polynomial x^7 + 15
 over 5-adic field mod 5^50
> $1!y;
4 + O(LL.1^350)
> y1:=$1;
> cc:=bb/Norm(y1);
> NormEquation(ll,mUU,cc);
true -3616536214210510131140119147750000 0*ll.1^6 +
    87784867820819001222023492420093 75*ll.1^5 -
    43643284374068024402604802526300000*ll.1^4 +
    93465502342896448463448377568368 75*ll.1^3 -
    26185594066026751474997106828827875*ll.1^2 -
    14936832657718115605325666448354300*ll.1 +
    32080554894739855251162281742539646
> _,z2:=$1;
> zz:=z2*y1*(PI)^Valuation(KKa);
> Valuation(Norm(zz)/KKa-1);
50
> l!Eltseq(zz);
-14555949062500*l.1^6 - 44057621806250*l.1^5 - 40944724340625*l.1^4 +
    3374464847500*l.1^3 + 13098563594750*l.1^2 + 19203103067175*l.1 -
    27691877497666
>  alpha:=$1;
> Valuation(Norm(alpha)/a-1);
20
```

In ramified local field extension L/K, norm equation fails for few unit elements of K. To find such elements we can find through computing the norm group of L which is the subgroup of U_K. In fact the norm equation fails for any unit elements of K which are multiples of such elements.

```
> K := pAdicRing(2,10);
> K := UnramifiedExtension(K,2);
> L := ext<K|x^12+12*x+26>;
> U,mU := UnitGroup(K);
> N,mN := NormGroup(L,mU);
> #quo<U|N>;
3
> T := TeichmuellerSystem(K);
> AttachSpec("spec");
> q,mq:=quo<U|N>;
> A:=[x@@mq@mU : x in q];
> #A;
3
> ClNormEquation(L,A[2]);
Norm fails
> ClNormEquation(L,A[3]);
Norm fails
> T:=TeichmuellerSystem(K);
> #T;
4
> ClNormEquation(L,T[3]);
Norm fails
> ClNormEquation(L,T[4]);
Norm fails
```

In fact for uniformizing elements π_L and π_K of L and K respectively, the element π_K^f is also the normed element of L where f is inertia degree of L/K.

After computing the Norm Equation of the Totally Ramified Extension we want to combine it with of Unramified extension. Now we would like to combine the norm equation of unramified with norm equation of Totally ramified so that we compute of the ramified extensions. Since $N(U_L) \subset U_K$ we can assume that not every element of U_K is a normed element but once it is the norm element then it is not unique. It may have more than one solution. This we can look by converting our field extensions to finite residue field extensions as described below.

$$\begin{array}{lll} L & \mathbb{F}_q & \ni \epsilon \\ \Big| e & \Big| & \\ N & \mathbb{F}_q & N(\epsilon) = \epsilon^e \\ \Big| f & \Big| & \\ K & \mathbb{F}_p & N_{\mathbb{F}_q/\mathbb{F}_p}(\epsilon) = \omega \end{array} .$$

We take $a = \omega\,(1 + p * Random(K)) \in U_K$. Then $\omega \in \mathbb{F}_p$. Clearly we can find many solutions in $\mathbb{F}_q$ such that their norms equal ω. But not all the solutions of $\mathbb{F}_q$ will be power of e. In this way we

try to find an element in $\mathbb{F}_q$ such that it is e^{th}-power. Finally we correspod the solution to our ring extension by finding the preimages of our residue field map. We present this idea in the following alogorithm.

Algorithm 3 Norm equation of residual part

Input: L/K be ramified p-adic field extension and $a = \omega \cdot u$ where u is unit in principal unit group of K.

Output: $\beta \in L$ scuh that $Norm(\beta) = \omega$.

1: Compute the residue field extension $\mathbb{F}_q$ and $\mathbb{F}_p$ of L and K resp.
2: Try to find ϵ in $\mathbb{F}_q$ such that $\epsilon = \epsilon^e =: \gamma$, where e is the ramification idex of L/K.
3: If $gcd(e, q-1) = 1$, then done.
4: If $gcd(e, q-1) = r$ then $gcd(e, p-1) = s|r$.
5: Compute $\gamma = g^x \sim g^x \cdot g^{(p-1)y} = g^{x+(p-1)y} \equiv g^{ze}$, then $Norm(g^{ze} = \omega)$.
6: Compute the preimage of g^{ze} in the ring of integers of L and let us denote it by β.

3.2 ClNormEquation and TameNormEQuation

3.3 Abstract

Let L/K be a finite Galois extension of p-adic fields of characteristic 0 and U_L and U_K be the unit groups of L and K respectively. Let $\mathrm{N} : L \to K$ be the norm map. In unramified extension $\mathrm{N}_{|U_L}$ is surjective to U_K. That is for every $a \in U_K$ we find $b \in U_L$ such that

$$\mathrm{N}(b) = a. \tag{3.1}$$

Similarly, if L/K is totally ramified extension then the norm group of L contains the group of the forms $U_K^n \times (\pi)$ where U_K^n and π are the higher unit groups of k and prime element of K respectively.
So in this, we mainly present algorithms to compute the norm equation of p-adic field extensions in an effective way.

3.4 Introduction

The norm equation which we are going to discuss here has the key role in algebraic number theory. It has many applications in class field theory. Although the norm equation is available in MAGMA, but it is not an effective way of computation. We first read some theory regarding the norm groups so that we will have the idea of the elements having the solution of type (1) since not every element is a normed element. Finally we present algorithms to find the solutions of norm equation.

In the field of real numbers $\mathbb{R}$, we can find the sequence of rational numbers which converges to a number which may not be rational. But $\mathbb{Q}_p$ is an extension of rational number field in which every convergent sequence converges in itself. The case of $\mathbb{R}$ is well understood.

Every field K with non-trivial discrete valuation v associates the subring of

$$\mathcal{O}_K = \{x \in K \mid \mathrm{v}(x) \geq 0\} \text{ of } K.$$

From [FV02], we know $\mathcal{O}_K$ forms a local ring with unique maximal ideal $\mathfrak{p}_K = \{x \in K \mid \mathrm{v}(x) > 0\}$ which coincides with the set of non-invertible elements of $\mathcal{O}_K$. An element $\pi \in \mathcal{O}_K$ is said to be a uniformizing element if $\mathrm{v}(K^\times) = \langle \mathrm{v}(\pi) \rangle$.
Let p be a prime integer. Then p-adic valuation on $\mathbb{Q}$ is the function $\mathrm{v}_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ defined by $\mathrm{v}_p(x) = \max\{r : p^r \text{ divides } x\}$. Note that $\mathrm{v}_p(0) = \infty$. With this valuation we can define the non-archimedian absolute value denoted by $|.|_p$ as $|.|_p : \mathbb{Q} \to \mathbb{R}$ such that $|x|_p = p^{-v_p(x)}$.
Note that, $|\mathbb{Q}_p^\times|_p = \{p^{-\mathrm{v}_p(x)} \mid x \in \mathbb{Q}_p^\times\} = \{1/p^n \mid n \in \mathbb{Z}\}$ is an infinite cyclic group.

Definition 3.4.1. Let p be a prime in $\mathbb{Z}$. $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|.|_p$ where $|.|_p$ is defined as above.

Equilvalently, from [Sat02] we can express $\mathbb{Q}_p$ as

$$\mathbb{Q}_p = \{\sum_{n=m}^{\infty} a_n p^n \mid m \in \mathbb{Z}, a_n \in \{0, 1, \ldots, p-1\}.$$

In the field of real number we have the isomorphism between $\mathbb{R}^+ \cong \mathbb{R}_{>0}^\times$ given by the maps $x \mapsto e^x$ and $\log(t) \leftarrow\!\shortmid t$ where $\mathbb{R}^+$ and $\mathbb{R}_{>0}^\times$ are the additive and multiplicative group of real numbers and e is the base of natural logarithm $\log$. But in contrast of this the exponential and logarithmic function does not converge always in p-adic field.

Proposition 3.4.2. *Let $a \in \mathbb{Q}_p$ then*

1. *the series $\exp_p(a) = \exp(a) = \sum_{n=1}^{\infty} a^n/n!$ converges iff $a \in p\mathbb{Z}_p$ for $p \neq 2$, and it converges iff $a \in 4\mathbb{Z}_p$ for $p = 2$,*
2. *$\log_p(a) = \log(a) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}(a-1)$ converges iff $a - 1 \in p\mathbb{Z}_p$ and*
3. *if a_1 and a_2 are in the domain of convergence exponential function and b_1 and b_2 are in the domain of convergence of logarithmic function then*

$$\exp(a_1 + a_2) = \exp(a_1) \cdot \exp(a_2)\,, \ \log(b_1 b_2) = \log(b_1) + \log(b_2)$$

.

Proof. Satoh 70. □

Lemma 3.4.3. *For every $x \in U_L^1$,*

$$\mathrm{v}(x-1) > \frac{e}{p-1} \Rightarrow \mathrm{v}(x^p-1) = \mathrm{v}(x-1) + e,$$

where $e = \mathrm{v}(p)$ is the ramification index of L and v is the surjective valuation function on L.

Proof. Lorenz page-88. □

For $a \in \mathbb{R}_{>0}$, we know

$$\log(a) = \lim_{h\to 0} \frac{a^h - 1}{h}.$$

In the same pattern, for any local field L of characteristic 0 and for every $a \in U_L$, we define

$$\log_p(a) = \log(a) = \lim_{n\to\infty} \frac{a^{p^n} - 1}{p^n}.$$

The $\log_p$ function satisfies the usual power series $\log_p(1-a) = -\sum_{n=1}^{\infty} \frac{a^n}{n}$ and this series converges for $\mathrm{v}(a) > 0$. The $\exp_p$ function has also the similar structure defined as $\exp_p(a) = \sum_{n=0}^{\infty} \frac{a^n}{n!}$, and this series converges for $\mathrm{v}(a) > e/(p-1)$.

3.5 Unit group

Let $(K, |.|)$ be a non-archimedian local field. Then $\mathcal{O}_K := \{a \in K : |a| \leq 1\}$ is the ring of integers and $\mathfrak{p}_K := \{a \in K : |a| < 1\}$ is the unique non-zero prime ideal in $\mathcal{O}_K$. $\mathcal{O}_K$ is also said to be the valuation ring of K and the ideal $\mathfrak{p}_K$ as a valuation ideal of K. The residue class field of K is defined by $\overline{K} = \mathcal{O}_K/\mathfrak{p}_K$ which is a finite filed of characteristic p. The unit group of $\mathcal{O}_K$ is $U_K = \mathcal{O}_K \setminus \mathfrak{p}_K$ the unit group. The group of higher principal unit U_K^n is defined as

$$U_K^n = U^n = 1 + \mathfrak{p}_K^n = \{x \in \mathcal{O}_K \mid x \equiv 1 \bmod \mathfrak{p}_K^n\}.$$

In particular, $U_K^1 = 1 + \mathfrak{p}_K = \{x \in \mathcal{O}_K \mid x \equiv 1 \bmod \mathfrak{p}_K\}$ is said to be the principal unit group.
Consider the non-archimedian field extension L/K and the absolute value $|\cdot|$ on L. Let $\mathcal{O}_L$ and $\mathfrak{p}_L$ are valuation ring and the valuation ideal of L, and that of K are $\mathcal{O}_K$ and $\mathfrak{p}_K$. Let $\overline{L} = \mathcal{O}_L/\mathfrak{p}_L$ and $\overline{K} = \mathcal{O}_K/\mathfrak{p}_K$. Since $\mathfrak{p}_K = \mathcal{O}_K \cap \mathfrak{p}_L$ we obtain the injective natural homomorphism $\overline{K} \to \overline{L}$ and we call $\overline{K}$ is a subfield of $\overline{L}$.

The degree $f = f(L/K) = [\overline{L} : \overline{K}]$ is called the residue class degree or inertia degree of L/K and the ramification index of L/K is defined as $e = e(L/K) = \frac{[L:K]}{f(L/K)}$. The extension L/K is called

unramified extension if $[L : K] = f(L/K)$ and **totally ramified** extension if $f(L/K) = 1$. If $[L : K]$ is neither $f(L/K)$ nor $e(L/K)$, then it is called **ramified** extension. For an intermediate field M of L/K we obtain

$$f(L/K) = f(L/M) \cdot f(M/K) \text{ and } e(L/K) = e(L/M) \cdot e(M/K).$$

Proposition 3.5.1. *Let L be a non-archimedian local field then the group $L^\times$ has direct product decomposition $L^\times = U_L \times (\pi)$ where π is a prime element of $\mathfrak{P}_L$ and $(\pi) = \{\pi^n\}_{n\in\mathbb{Z}}$ is the infinite cyclic subgroup of $L^\times$ generated by π.*

Proof. [Neu99b], Proposition 3.1.

□

For each $m \in \mathbb{N}$, let W_m be the group of m^{th} roots of unity in algebraic closure of L. Then

$$L^\times = \langle\pi\rangle \times U_L = (\pi) \times \mathbb{F}_q^\times \times U_L^1.$$

where $\mathbb{F}_q$ is the residue class field of L. Let $W_{q-1} = \langle\zeta_L\rangle$ be the $(q-1)^{th}$ roots of unity in L then $\mathbb{F}_q^\times \cong W_{q-1}$. Other than $(q-1)^{th}$ roots of unity, we also have W_{p^∞} which is the group of roots of unity in U_L^1 of p-power order. We call W_{p^∞} as the p-power torsion unit group of L.

Theorem 3.5.2. *Let L be a non-archimedian local field. The map $\log : U_L^1 \to L$ defined as above is continuous and satisfies $\log(ab) = \log(a)\log(b)$. Its kernel is the group W_{p^∞}. Let $e = v_L(p) > 0$ be the ramification index of $L/\mathbb{Q}_p$. For each $r \in \mathbb{N}$ such that $r > \frac{e}{p-1}$, the log function $\log : U_L^r \to \mathfrak{p}_L^r$ is an isomorphism. This isomorphism*

$$U_L^r \cong \mathfrak{p}_L^r, \text{ for } r > \frac{e}{p-1}$$

is also an isomorphism of $\mathbb{Z}_p$-modules.

Proof. [Lor08], Theorem 8, page-87.

□

Let $x \in U_L^1$ such that $x^n = 1$ for some $n \in \mathbb{N}$. Then $n\log(x) = \log(x^n) = \log(1) = 0$. So, $\log(x) = 0$. For $r > \frac{e}{p-1}$, if $\log(x) = 0$ then from above theorem $x^{p^r} \in U_L^r$. Applying log we get

$$\log(x^{p^r}) = p^r \log(x) = 0 \Rightarrow x^{p^r} = 1.$$

Remark 3.5.3. 1. The p-power torsion units of U^1 are the elements of the group $W(U_L^1) = W_{p^\infty} = W_{p^r}(L)$, where $r > \frac{e}{p-1}$.

2. The exponential function defined as $\exp : \mathfrak{p}^r \to U^r$ such that $\exp(x+y) = \exp(x) \cdot \exp(y)$ is the inverse of logarithm function $\log : U^r \to \mathfrak{p}^r$ where $r > \frac{e}{p-1}$. So, for every $x \in U^r$ such that $\mathrm{v}(x-1) > \frac{e}{p-1}$ and $a \in \mathbb{Z}_p$ we get

$$x^a = \exp^{a \log(x)}.$$

Theorem 3.5.4. *Let L be a non-archimedian local field of characteristic 0. The principal unit group U_L^1 has the following structure*

$$U_L^1 = W_{p^\infty} \times \mathbb{Z}_p^n$$

as a $\mathbb{Z}_p$-module where $n := [L : \mathbb{Q}_p]$.

Proof. [Lor08], page-90, Theorem 9. □

One can find the precise generators of principal unit group from [Pau06]. The author of [Pau06] presents theorems through which one can easily compute the generators of the local field extensions. We use thsese generators while solving the norm equations. We have written the function "CUnitGroupGenerators" using those results and this is much faster than the function "UnitGroupGenerators" of MAGMA.

3.6 Norm Group

Let L/K be a finite Galois extension of degree n then L is a K-vector space. Suppose $B = \{\alpha_1, \ldots, \alpha_n\}$ be the basis of L/K and $a \in L$. Then $\phi_a : L \to L$ defined by $x \mapsto ax$ is clearly K-linear map. Thus we obtain the representaion matrix of a as a matrix $M_a \in K^{n \times n}$ such that

$$a(\alpha_1, \ldots, \alpha_n) = (\alpha_1, \ldots, \alpha_n) M_a.$$

The characteristic polynomial of a is defined as $f_a = \det(aI_n - M_a) \in K[x]$. So, we obtain $f_a = x^n + b_{n-1}x^{n-1} + \ldots + b_1 x^1 + b_0$ where all $b_i \in K$. We define the norm of a over L/K as

$$\mathrm{N}_{L/K}(a) = (-1)^n b_0 = \det(M_a)$$

and the trace of a over L/K is as

$$\mathrm{Tr}_{L/K} = -b_{n-1} = \mathrm{Tr}(M_a).$$

Due to the fact of the map $L \to K^{n\times n}$ defined by $x \mapsto M_x$ is K-algebra homomorphism, we obtain the multiplicative group homomorphism $N_{L/K} : L^\times \to K^\times$ such that $\mathrm{N}_{L/K}(ab) = \mathrm{N}_{L/K}(a)\,\mathrm{N}_{L/K}(b)$ and $\mathrm{N}_{L/K}(\mu a)\mu^n = \mathrm{N}_{L/K}(a)$ for all $a, b \in L$ and $\mu \in K$.
The K- linear map $\mathrm{Tr}_{L/K} : L \to K$ such that
$\mathrm{Tr}_{L/K}(a+b) = \mathrm{Tr}_{L/K}(a) + \mathrm{Tr}_{L/K}(b)$ and
$\mathrm{Tr}_{L/K}(\mu a) = \mu\,\mathrm{Tr}_{L/K}(a)$ for all $a, b \in L$ and $\mu \in K$. We can also compute the norm of a using the Galois group as

$$\mathrm{N}_{L/K}(a) = \prod_{\sigma\in \mathrm{G}(L/K)} \sigma(a)$$

where $\mathrm{G}(L/K)$ is the Galois group of L/K. The Group G contains the automorphisms of L fixing the elements of field K. So for any $a \in K$ we get $\mathrm{N}_{L/K}(a) = a^{[L:K]}$. Also, for $a \in L$, the trace of a is defined as the sum of all of it's Galois conjugates

$$i.e.\ \mathrm{Tr}(a) = \sum_{\sigma\in \mathrm{G}(L/K)} \sigma(a).$$

Note, if $a \in K$, then $\mathrm{Tr}_{L/K}(a) = [L : K] \cdot a$.
For $L/M/K$ a tower of field extensions, we have $\mathrm{Tr}_{L/K} = \mathrm{Tr}_{M/K} \circ \mathrm{Tr}_{L/M}$ and $\mathrm{N}_{L/K} = \mathrm{N}_{M/K} \circ \mathrm{N}_{L/M}$.
In an unramified extension, from [Neu99b] we have the fact that $\mathrm{N}(U_L) = U_K$. This means every unit of base field K is a norm of an element of L.

$$i.e. \quad \forall a \in U_K \ \ \exists b \in U_L : \ \mathrm{N}(b) = a.$$

But the situation is different in the ramified field extensions.

Theorem 3.6.1. *Let L/K be a totally ramified extension. Then the norm groups of L are precisely the groups which contain the groups of the form $U_K^n \times (\pi)$ for some appropriate $n \in \mathbb{N}$.*

Proof. [Neu99b] Theorem 7.17. □

From the above theorem we can observe that there may be many units in K which are not normed element. It is difficult to find those elements of K which are not normed element. However if L/K is tamely ramified extension then from [Pau06] we know that the norm group $\mathrm{N}(L)$ contains the principal unit group U_K^1. If $x \in K$ is normed element then we present algorithms in the next section to find the element of L having $\mathrm{N}(\alpha) = x$.

3.7 Solving Norm Equations

Although there are many ways of solving the norm equations, we present two ways in this section.

Using unit group generators:

For finite local field extension L/K and $a \in K^\times$, we are looking for an element in $b \in L$ such that $\mathrm{N}(b) = a$. Let $\{\eta_1, \eta_2 \ldots, \eta_r\}$ be the set of generators of principal unit group of L then the direct decomposition of multiplicative group of L becomes

$$L^\times \quad = \quad \langle \pi \rangle \times \langle \zeta_L \rangle \times \langle \eta_1, \eta_2 \ldots, \eta_r \rangle$$

If a is a normed element then $a \in \mathrm{N}(L^\times)$.

$$i.e. \quad a \in \langle \mathrm{N}(\pi) \rangle \times \langle \mathrm{N}(\zeta_L) \rangle \times \langle \mathrm{N}(\eta_1), \mathrm{N}(\eta_2) \ldots, \mathrm{N}(\eta_r) \rangle.$$

So, we determine b using the representation of a in $\langle \mathrm{N}(\pi), \mathrm{N}(\zeta_L), \mathrm{N}(\eta_1), \mathrm{N}(\eta_2) \ldots, \mathrm{N}(\eta_r) \rangle$. The set $\{b \cdot \epsilon \mid \mathrm{N}(\epsilon) = 1\}$ consists of all solutions of norm equation of a. If we include ζ_L in the principal unit group generators then we can write $U_L = \langle \zeta_L, \eta_1, \eta_2 \ldots, \eta_r \rangle$.

Algorithm 4 Norm equation using unit group generators

Input: L/K be a finite Galois field extensions $a \in U_K$.
Output: Find $b \in L$ such that $\mathrm{N}_{L/K}(b) = a$.

1: Compute the unit group generators of L and let it be $\{\eta_1, \eta_2 \ldots, \eta_r\}$.
2: Compute the free abelian group F of rank r with basis $\{F_1, F_2, \ldots, F_r\}$.
3: Define a homomorphism map $\psi : F \to U_K$ such that $\sum_1^r x_i \cdot F_i \mapsto \sum_i^r x_i \cdot \mathrm{N}(\eta_i)$.
4: If $a \notin \psi(F)$ then **return** no solution,
5: else

1. Compute the pre-image $\psi^{-1}(a) := \sum_1^r b_i \cdot F_i$.
2. **return** $b := \sum_1^r b_i \cdot \eta_i$.

In fact this algorithm is already applied in MAGMA and available. We compute the unit group grnerators of the local field which is much faster than of MAGMA. Using our generators we solve the norm equations much faster than the function NormEquation of MAGMA. We have written the codes of unit group generators in the file "NormEquation.m" and call the function "ClNormEquation" which solves the norm equations.

We have made the above algorithm much faster than before but if we have the local field extensions of high degree then computation of unit group consumes more time while solving norm equations. To get rid of the computation of unit group while solving the norm equations of particular type of elements of the field we present effective algorithms in the following sub-section.

Using trace and logarithms:

Let us suppose $x \in U_L^1$ so that $\log(x)$ converges. Then from [Iwa72] we have

$$\log(\sigma(x)) = \sigma(\log(x))$$

for every $\sigma \in \mathrm{G}(L/K)$

Let us suppose all the notation as above then for $a \in U_L^r$ where $r > \frac{e}{p-1}$ we have

$$\mathrm{N}_{L/K}(a) = \prod_{\sigma \in \mathrm{G}(L/K)} \sigma(a).$$

Applying the logarithm, we get

$$\log(\mathrm{N}_{L/K}(a)) = \sum_{\sigma \in \mathrm{G}(L/K)} \log(\sigma(a)) \tag{3.2}$$

$$= \mathrm{Tr}_{L/K}(\log(a)) \tag{3.3}$$

Thus, one can compute the norm using formula $\mathrm{N}_{L/K}(a) = \exp(\mathrm{Tr}(\log(a)))$ if the element is in the domain of convergence of $\exp$ and $\log$. Since we are interested in solving the norm equation that is for an element $a \in K$ we check whether there exists an element $b \in L$ such that $\mathrm{N}_{L/K}(b) = a$. In order to find $b \in L$ we will solve the trace equation from (3). As solving the trace equation is much simpler task than solving the norm equation since the process is linear, we solve the norm equation much faster.
Note that $a \in K$ is in the domain of convergence of $\log$ and $\exp$. In order to find the $b \in L$ such that $\mathrm{N}_{L/K}(b) = a$, we use the following strategy:
Applying $\log$ we get

$$\log(\mathrm{N}_{L/K}(b)) = \log(a)$$

Using the Satoh's formula for computing norm, we get

$$\log(\exp(\mathrm{Tr}(\log(b)))) = \log(a).$$

Since $\exp$ and $\log$ are isomorphism to each other we obtain

$$\mathrm{Tr}(\log(b)) = \log(a).$$

Since $\log(b) \in L$, we look for the element of $x \in L$ such that $\mathrm{Tr}(x) = \log(a)$ and then finally we compute $\exp(x)$ which will be our required element in L if a does not contain any torsion unit.
Clearly, in this method we solve the trace equation instead of norm equation.
We have $\mathrm{N}(U_L) = U_K$ in any unramified extension and suppose that the residue class fields of L

and K are $\mathbb{F}_L$ and $\mathbb{F}_K$ respectively. Since the norm map is surjective on finite fields, so $\mathrm{N} : \mathbb{F}_L^\times \to \mathbb{F}_K^\times$ is surjective.

In fact, $L^\times = (\pi) \times \mathbb{F}_q^\times \times U_L^1$. Since the norm is multiplicative that is, $\mathrm{N}(ab) = \mathrm{N}(a) \cdot \mathrm{N}(b)$, we will solve the norm equation factorising the element as in the above form.
In brief, for an unramified extension L and its residue class field $\mathbb{F}_q$ we have the map known as Teichmüller lift $i.e\ T : \mathbb{F}_q \to \mathcal{O}_L$ defined as follows:

- $T(0) = 0$.
- For $\overline{a} \in \mathbb{F}_q$, $T(\overline{a})$ is the unique $(q-1)^{th}$ root of unity with residual part equals to $\overline{a}$.

For the computation of the Teichmüller lift one can find algorithm in ([Coh93],[Sat02]).

we present in this the algorithms which will solve the norm equations for particular types of element of the field without using the unit group generators of the field. Instead of computing unit group generators, here we apply the functions such as division, logarithm, trace and exponential which are not expensive in the sense of computation time and because of this we can solve the norm equation in very short time for large degree of local field extensions.
The following algorithm solves the norm equation of part of W_{q-1} that is the residual part of the field. From decomposition of the multiplicative group of the local field we can factorise each part

Algorithm 5

Input: L/K be finite unramified extension of p-adic fields. Let $a \in U_K$ such that $a \in W_{q-1}$ in the residue class field of K i.e a is $(q-1)^{th}$ root of unity.
Output: $\alpha \in L$ such that $\mathrm{N}(\alpha) = a$.
1: Compute the $\mathbb{F}_{q^f}$ residue class field of L where $f := f(L/K)$, and let $\overline{a} \in \mathbb{F}_q^\times$.
2: Compute $\overline{b} \in \mathbb{F}_{q^f}^\times$ such that $\mathrm{N}(\overline{b}) = \overline{a}$ using NormEqution of MAGMA over finite fields.
3: Compute a lift by powering ($i.e$. Teichmüller lift from Satoh) $\alpha \in L$ of $\overline{b}$ such that $\mathrm{N}(\alpha) = a$.

of any field element and then solve the norm equations separately. We know that $\log$ and $\exp$ are inverse to each other if the field element is in the domain of convergence of them. Thus in this situation $\log$, trace and $\exp$ work well and these functions are much faster even in the large degree of local field extensions. So, using this we present below a secure algorithm.

Clearly, the function trace is not identically zero, so we can find many elements $\alpha \in L$ such that $\mathrm{trace}(\alpha) \neq 0$. In particular, we search such an element and then it will be easy to compute $x \in L$ satisfying $2(b)$. We present an example which shows the computation time of two versions of norm equation.
Example 3.7.1.

```
>K:=pAdicRing(5,30);
```

Algorithm 6 norm equation of torsion free unit

Input: L/K be finite extension of p-adic fields , $a \in U_K$ is a torsion free unit.
Output: $\alpha \in L$ such that $\mathrm{N}(\alpha) = a$.

1: If $\mathrm{v}(a-1) \leq e/(p-1)$ then solve using Algorithm 1.
2: If $\mathrm{v}(a-1) > e/(p-1)$ then solve as below:
3: Compute $x \in L$ such that $\mathrm{Tr}(x) = \log(a)$ and $\mathrm{v}(x) > 0$.
4: Return $\exp(\mathrm{Tr}(x))$.

```
>L:=ext<UnramifiedExtension(K,2)|x^12+5>;
> Precision(L);
360
>a:=1+2*L.1^5;
>Attach("NormEquation.m");
>time b:=ClNormEquation(UnramifiedExtension(L,12),a);
Time: 3.080
> Valuation(Norm(b)/a-1);
360
> L_ur:= UnramifiedExtension(L,12);
> time U,mU:=UnitGroup(L);
Time: 69.760
> time _,b:=NormEquation(L_ur,mU,a);
......much expensive.more than a week.
```

3.7.1 Algorithm:

Input : E/L be a finite unramified p-adic field extension, Π and π be uniformizer of $\mathcal{O}_E$ and $\mathcal{O}_L$ respectively and $a \in U_L$ up to finite precision $n \in \mathbb{N}$.
Output: Find $\alpha \in E$ such that $\mathrm{N}(\alpha) = a$.

1. Factorize a as $a = a_f \cdot a_u \cdot a_t$ where a_u is torsion free unit element and a_t is p-power torsion unit element and a_f is in residue field of L.
2. Compute $a_f^{'} \in E$ using the Algorithm 5.2 for a_f.
3. Compute $a_u^{'} \in E$ using the Algorithm 5.3 whose norm is a_u.
4. Solve the norm equation of torsion unit a_t as $a_t^{'}$ using Algorithm 5.1.
5. Return the product: $a_u^{'} \cdot a_t^{'} \cdot a_f^{'}$.

In the unramified extension not only we can solve the norm equation of unit but also for the elements including valuation parts. Since $\mathrm{N}(\Pi) = \pi^f$ where f is the Inertia degree of L. So we can compute the solution of norm equation of $(\pi^f) \times U_L$.

3.7.2 Algorithm:

Input : E/L be a finite totally ramified p-adic field extension, $a \in U_L^n$ be an element in the norm group of E, up to finite precision n.
Output: Find $\alpha \in E$ such that $\mathrm{N}(\alpha) = a$.

1. $a = a_u \cdot a_t$ where a_t is p-power torsion unit part of a and a_u is free of torsion unit.
2. To solve for a_t do
   - if $a_t \neq 1$ then using algorithm 5.1, compute $a_t^{'}$ such that $\mathrm{N}(a_t^{'}) = a_t^{'}$.
   - else $a_t^{'} = 1$.
3. To solve for a_u do
   - choose suitable $r \in \mathcal{O}_N$ such that $r/\operatorname{trace}(r) =: r_1$ is defined.
   - $s \leftarrow \operatorname{trace}(r_1 \cdot \log(a_u))$.
   - $a_u^{'} \leftarrow \exp(s)$.
4. Return $a_t^{'} \cdot a_u^{'}$.

To verify it we apply the norm:

$$\begin{aligned}
\mathrm{N}(a_t^{'} \cdot a_u^{'}) &= \mathrm{N}(a_t^{'}) \cdot \mathrm{N}(a_u^{'}) \\
&= a_t \cdot \exp(\operatorname{trace}(\log(\exp(r_1 \cdot \log(a_u))))) \\
&= a_t \cdot \cdot \exp(\operatorname{trace}(r_1 \cdot \log(a_u))) \\
&= a_t \cdot \exp(\log(a_u)) \quad \text{since, } \operatorname{trace} \text{ is linear} \\
&= a_t \cdot a_u = a.
\end{aligned}$$

For the computation in p-adic field extension, the problem is to present the elements in an exact form. We want in this to solve the norm equation of unit element of the ring of integers of the field. For a local field L, assume $\mathcal{O}_L$ be the ring of integers and π be the uniformizing element of $\mathcal{O}_L$. The element $x \in \mathcal{O}_L$ can be written in the infinite series of π. But for the computation purpose we would like to truncate the infinite expansion of x to a finite sum. That means we work in the quotient ring $\mathcal{O}_L/\pi^n\mathcal{O}_L$ for $n \in \mathbb{N}$. The integer n is said to be the precision of the ring $\mathcal{O}_L$. All we presented the algorithms above have been applied only in the field of finite precision. Since the quotient ring is of finite structure so its elements can be presented exactly and hence we can apply our algorithms to solve the norm equation. The exponential function of MAGMA in local field extension has some flaws, so I have written my own codes for exponential function which

loses the precision. Also while applying the above algorithms we use division which also loses the precision. One can find more details of precision loss in [**?**]. We are still trying to manage the precision loss during division and exponential function.
The above algorithms we presented can solve the norm equation in either unramified extension or totally ramified extensions effectively. But when the local field L has both the ramification index and the inertia degree over K greater than 1, then we solve the norm equation with command "MyNormEquation" in MAGMA. Suppose $L/M/K$ be a tower of local field extensions then we can solve the norm equation of L/K by iterating over intermediate fields. In our algorithms we apply the functions such as $\log$ and $\exp$, so we have to check in each intermediate field whether the solution is in the convergence of them. In this case, to get rid of solving the norm equation in each intermediate fields one can solve with command "MyNormEquation" which also works effectively with our new way of computation of unit group generators.
The following examples and table show the effectiveness of our algorithms.

Fields above in the table are defined as below:
1) $K := ext < UnramifiedExtension(Q_5, 2)|x^5 + 10 * x + 5 >$;
2) $K := ext < UnramifiedExtension(Q_5, 2)|x^7 + 10 * x + 5 >$;
3) $K := ext < UnramifiedExtension(Q_5, 2)|x^10 + 15 * x^2 + 5 * x + 5 >$;
4) $K := ext < UnramifiedExtension(Q_5, 2)|x^11 + 15 * x^2 + 5 * x + 5 >$;
6) $Q_3 := pAdicRing(3, 10)$; & $K := ext < Q_3|x^15 + 3 * x^5 + 3 >$;
7) $K := ext < Q_3|x^16 + 3 * x^5 + 3 >$;
8) $K := ext < Q_3|x^18 + 3 * x^5 + 3 >$;
9) $K := ext < Q_3|x^20+3*x^5+3 >$; 10) $Q_3 := pAdicRing(3, 5); K := ext < UnramifiedExtension(Q_3, 2)|x^12+ 15 * x^2 + 3 * x + 3 >; a := 1 + 2 * K.1^8$;
11)$Q_3 := pAdicRing(3, 5); K := ext < UnramifiedExtension(Q_3, 2)|x^12+15*x^2+3*x+3 >;$
$a := 1 + 2 * K.1^8$;
12) $Q_3 := pAdicRing(3, 5); K := ext < UnramifiedExtension(Q_3, 2)|x^12+15*x^2+3*x+3 >;$
$a := 1 + 2 * K.1^8$;
13) $Q_3 := pAdicRing(3, 10); K := ext < UnramifiedExtension(Q_3, 2)|x^12+15*x^2+3*x+3 >$
; $a := 1 + 2 * K.1^8$;

Remark 3.7.2. We computed the norm equation for any unit element of ring of integer $\mathcal{O}_K$ of K in the finite extension L/K. Due to the fact $N(U_L) \subset U_K$ we can compute the elements of which do not have solution once we have the map from O_K to unit group U_K. We see below how to find such elements:

```
> x := PolynomialRing(Integers()).1;
> K := pAdicRing(3,10);
> M := UnramifiedExtension(K,2);
```

```
> L:= ext<M| x^4+3*x+3>;
> U,mU := UnitGroup(M);
> N,mN := NormGroup(L, mU);
> q,mq := quo<U|N>;
> F := [x@@mq@mU: x in q];
> [NormEquation(L,mU,F[i]): i in [2..#F]];
[ false, false, false ]
```

From above example we can see that there are three elements in U_M whic has no solution for norm equation.

Appendix A

Frequently Asked Questions

A.1 How do I change the colors of links?

The color of links can be changed to your liking using:

`\hypersetup{urlcolor=red}`, or

`\hypersetup{citecolor=green}`, or

`\hypersetup{allcolor=blue}`.

If you want to completely hide the links, you can use:

`\hypersetup{allcolors=.}`, or even better:

`\hypersetup{hidelinks}`.

If you want to have obvious links in the PDF but not the printed text, use:

`\hypersetup{colorlinks=false}`.

Bibliography

[Coh93] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[Fie06] Claus Fieker. Applications of the class field theory of global fields. In *Discovering mathematics with Magma*, volume 19 of *Algorithms Comput. Math.*, pages 31–62. Springer, Berlin, 2006.

[FV02] I. B. Fesenko and S. V. Vostokov. *Local fields and their extensions*, volume 121 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, second edition, 2002. With a foreword by I. R. Shafarevich.

[Iwa72] Kenkichi Iwasawa. *Lectures on p-adic L-functions*. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1972. Annals of Mathematics Studies, No. 74.

[Lor08] Falko Lorenz. *Algebra. Vol. II*. Universitext. Springer, New York, 2008. Fields with structure, algebras and advanced topics, Translated from the German by Silvio Levy, With the collaboration of Levy.

[Neu99a] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Neu99b] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Pau06] Sebastian Pauli. Constructing class fields over local fields. *J. Théor. Nombres Bordeaux*, 18(3):627–652, 2006.

[Sat02] Takakazu Satoh. On p-adic point counting algorithms for elliptic curves over finite fields. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 43–66. Springer, Berlin, 2002.