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

June 18, 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

Introduction

1.1 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 1.1.1. 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 1.1.2. 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 $H^2\,(G, A)$.

1.1.1 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

$$\bar{f}_q : H^q(G, A) \to H^q(G, B) \tag{1.1}$$

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 1.1.3. *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 1.1.4. *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 1.1.5. 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 1.1.6. *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 1.1.7. *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 1.1.8. 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 1.1.9. 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 1.1.10. *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 1.1.11. 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

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

Chapter 2

Norm Equation

2.1 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 + 7458503899406259437S*l.1^5 - 5615783539450029762S*l.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 42590842877721166250*l.1^6 + 26116648601645555000*l.1^5 - 73527459338485500375*l.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
```

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 Local Fundamental Class using Serre's Approach:

Input: L/K be ramified p-adic field extension and $a = \omega\,(1 + p * Random(k))$.

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

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 $\epsilon^e := \gamma$, 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 $\tilde{\beta}$.

```
> R<x>:=PolynomialRing(Integers());
> K:=pAdicField(5,20);
> L:=ext<UnramifiedExtension(K,6)|x^9+20>;
> kk:=RingOfIntegers(K);
> l:=RingOfIntegers(L);
> f,mf:=ResidueClassField(kk);
> F,mF:=ResidueClassField(l);
> pi:=UniformizingElement(kk);
> Pi:=UniformizingElement(l);
> mu:=(1+Pi*l.1^2);
> Norm(mu,kk);
-32441541670284
```

```
> a:=$1;
> fa:=mf(a);
> q:=#F;
> e:=RamificationIndex(L,K);
> r:=Gcd(e,q-1);
> r;
9
> e;
9
> J :=[b: b in F| Norm(b) eq mf(a) and IsPower(b, 9)];
> #J;
434
> J[120];
F.1^4284
> y:=4284;
> k:=-y*Modinv(4,9) mod ((q-1));
> k;
1260
> y+4*k mod ((q-1));
9324
> $1 div 9;
1036
> z:=$1;
> Norm(F.1^(z*e)) eq Norm(F.1^y);
true
> zz := BaseRing(l)!(F.1^z);
> Parent(zz);
Unramified extension defined by the polynomial x^6 + x^4 + 4*x^3 + x^2 + 2
 over 5-adic ring mod 5^20
> quo<BaseRing(l)| UniformizingElement(BaseRing(l))^20 >;
Unramified extension of Quotient of the 5-adic ring modulo the ideal generated
by 5^20 modulo x^6 + x^4 + 4*x^3 + x^2 + 2
> TeichmuellerLift(F.1^z, $1);
1460431311730*$.1^5 - 22847830757203*$.1^4 + 22594378813347*$.1^3 +
    26080130363300*$.1^2 + 32456939542293*$.1 - 38115834103681
> t:=$1;
> Norm(t)/a-1;
3575157952127*5 + O(5^20)
> l!BaseRing(l)!F.1^z;
43719153629260*$.1^5 + 21726433361167*$.1^4 - 30972319764843*$.1^3 -
    3424888499040*$.1^2 + 8506756284243*$.1 - 13239816221281
> $1^((5^6)^20);
1460431311730*$.1^5 - 22847830757203*$.1^4 + 22594378813347*$.1^3 +
    26080130363300*$.1^2 + 32456939542293*$.1 - 38115834103681
> s:=$1;
> Norm(Norm(s))/a-1;
3575157952127*5 + O(5^20)
> l!BaseRing(l)!F.1^z;
43719153629260*$.1^5 + 21726433361167*$.1^4 - 30972319764843*$.1^3 -
    3424888499040*$.1^2 + 8506756284243*$.1 - 13239816221281
> $1^((5^6)^100);
1460431311730*$.1^5 - 22847830757203*$.1^4 + 22594378813347*$.1^3 +
    26080130363300*$.1^2 + 32456939542293*$.1 - 38115834103681
> s:=$1;
```

```
> Norm(Norm(s))/a-1;
3575157952127*5 + O(5^20)
> l!BaseRing(l)!F.1^z;
43719153629260*$.1^5 + 21726433361167*$.1^4 - 30972319764843*$.1^3 -
    3424888499040*$.1^2 + 8506756284243*$.1 - 13239816221281
> $1^((5^6)^10);
1460431311730*$.1^5 - 22847830757203*$.1^4 + 22594378813347*$.1^3 +
    26080130363300*$.1^2 + 32456939542293*$.1 - 38115834103681
> s:=$1;
> Norm(Norm(s))/a-1;
3575157952127*5 + O(5^20)

R<x>:=PolynomialRing(Integers());
K:=pAdicField(5,20);
L:=ext<UnramifiedExtension(K,6)|x^9+20>;
kk:=RingOfIntegers(K);
l:=RingOfIntegers(L);
f,mf:=ResidueClassField(kk);
F,mF:=ResidueClassField(l);
pi:=UniformizingElement(kk);
Pi:=UniformizingElement(l);
mu:=(1+Pi*l.1^2);
Norm(mu,kk);
a:=$1;
fa:=mf(a);
q:=#F;
e:=RamificationIndex(L,K);
r:=Gcd(e,q-1);
r;
e;
J :=[b: b in F| Norm(b) eq mf(a) and IsPower(b, 9)];
#J;
J[120];
y:=4284;
k:=-y*Modinv(4,9) mod ((q-1));
k;
y+4*k mod ((q-1));
$1 div 9;
z:=$1;
Norm(F.1^(z*e)) eq Norm(F.1^y);
zz := BaseRing(l)!(F.1^z);
Parent(zz);
quo<BaseRing(l)| UniformizingElement(BaseRing(l))^20 >;
TeichmuellerLift(F.1^z, $1);
t:=$1;
Norm(t)/a-1;
l!BaseRing(l)!F.1^z;
$1^((5^6)^20);
s:=$1;
Norm(Norm(s))/a-1;
l!BaseRing(l)!F.1^z;
$1^((5^6)^100);
s:=$1;
Norm(Norm(s))/a-1;
```

```
l!BaseRing(l)!F.1^z;
$1^((5^6)^10);
s:=$1;
Norm(Norm(s))/a-1;
```

```
> R<x>:=PolynomialRing(Integers());
> K:=pAdicField(5,20);
> L:=ext<UnramifiedExtension(K,6)|x^9+20>;
> kk:=RingOfIntegers(K);
> l:=RingOfIntegers(L);
> f,mf:=ResidueClassField(kk);
> F,mF:=ResidueClassField(l);
> pi:=UniformizingElement(kk);
> a:=2*(1+pi*kk.1^2);
> fa:=mf(a);
> q:=#F;
> e:=RamificationIndex(L,K);
> r:=Gcd(e,q-1);
> r;
9
> e;
9
> J :=[b: b in F| Norm(b) eq mf(a) and IsPower(b, 9)];
> #J;
434
> J[120];
F.1^4293
> y:=4293;
> k:=-y*Modinv(4,9) mod ((q-1));
> k;
1197
> y+4*k mod ((q-1));
9081
> $1 div 9;
1009
> z:=$1;
> Norm(F.1^(z*e)) eq Norm(F.1^y);
true
> zz := BaseRing(l)!(F.1^z);
> Parent(zz);
Unramified extension defined by the polynomial x^6 + x^4 + 4*x^3 + x^2 + 2
 over 5-adic ring mod 5^20
> quo<BaseRing(l)| UniformizingElement(BaseRing(l))^20 >;
Unramified extension of Quotient of the 5-adic ring modulo the ideal generated
by 5^20 modulo x^6 + x^4 + 4*x^3 + x^2 + 2
> TeichmuellerLift(F.1^z, $1);
1862586676453*$.1^5 - 5785193003422*$.1^4 + 36744167270945*$.1^3 -
    42560942525731*$.1^2 + 29658407580449*$.1 - 33210603142769
> t:=$1;
> Norm(t)/a-1;
-3439145893768*5 + O(5^20)
> l!BaseRing(l)!F.1^z;
-6706161466012*$.1^5 + 10767251860883*$.1^4 + 39839038481700*$.1^3 +
    185612827344*$.1^2 + 195573044180l4*$.1 + 17589748453091
```

```
> $1((5^6)^20);

>> $1((5^6)^20);
     ^
Runtime error in '@': Bad argument types
Argument types given: RngIntElt, RngPadElt

> l!BaseRing(l)!F.1^z;
-6706161466012*$.1^5 + 10767251860883*$.1^4 + 39839038481700*$.1^3 +
    185612827344*$.1^2 + 195573044180l4*$.1 + 17589748453091
> $1^((5^6)^20);
1862586676453*$.1^5 - 5785193003422*$.1^4 + 36744167270945*$.1^3 -
    42560942525731*$.1^2 + 29658407580449*$.1 - 33210603142769
> s:=$1;
> Norm(s);
17264873516952*$.1^5 - 15130151538711*$.1^4 - 25159490456175*$.1^3 +
    21296605561881*$.1^2 + 22060257953098*$.1 + 32404607106365
> Norm(Norm(s))/a-1;
-3439145893768*5 + O(5^20)
> s-zz;
1862586676450*$.1^5 - 5785193003425*$.1^4 + 36744167270945*$.1^3 -
    42560942525735*$.1^2 + 29658407580445*$.1 - 33210603142770
> "s is the solution of a ";
s is the solution of a
> %P
R<x>:=PolynomialRing(Integers());
K:=pAdicField(5,20);
L:=ext<UnramifiedExtension(K,6)|x^9+20>;
kk:=RingOfIntegers(K);
l:=RingOfIntegers(L);
f,mf:=ResidueClassField(kk);
F,mF:=ResidueClassField(l);
pi:=UniformizingElement(kk);
a:=2*(1+pi*kk.1^2);
fa:=mf(a);
q:=#F;
e:=RamificationIndex(L,K);
r:=Gcd(e,q-1);
r;
e;
J :=[b: b in F| Norm(b) eq mf(a) and IsPower(b, 9)];
#J;
J[120];
y:=4293;
k:=-y*Modinv(4,9) mod ((q-1));
k;
y+4*k mod ((q-1));
$1 div 9;
z:=$1;
Norm(F.1^(z*e)) eq Norm(F.1^y);
zz := BaseRing(l)!(F.1^z);
Parent(zz);
quo<BaseRing(l)| UniformizingElement(BaseRing(l))^20 >;
TeichmuellerLift(F.1^z, $1);
```

```
t:=$1;
Norm(t)/a-1;
l!BaseRing(l)!F.1^z;
$1((5^6)^20);
l!BaseRing(l)!F.1^z;
$1^((5^6)^20);
s:=$1;
Norm(s);
Norm(Norm(s))/a-1;
s-zz;
"s is the solution of a ";

Next Example

 R<x>:=PolynomialRing(Integers());
> K:=pAdicField(7,20);
> L:=ext<UnramifiedExtension(K,6)|x^16+28>;
> kr:=RingOfIntegers(K);
> l:=RingOfIntegers(L);
> f,mf:=ResidueClassField(k);

>> f,mf:=ResidueClassField(k);
                            ^
User error: Identifier 'k' has not been declared or assigned
> F,mF:=ResidueClassField(l);
> pi:=UniformizingElement(kr);
> Pi:=UniformizingElement(l);
> mu:=1+Pi*l.1^2;
> Norm(Norm(mu));
-8137045170898335
> a:=$1;
> fa:=mf(a);

>> fa:=mf(a);
       ^
User error: Identifier 'mf' has not been declared or assigned
> q:=#F;
> e:=RamificationIndex(L,K);
> r:=Gcd(e,q-1);
> r;
16
> e;
16
> J :=[b: b in F| Norm(b) eq mf(a) and IsPower(b, 16)];

>> J :=[b: b in F| Norm(b) eq mf(a) and IsPower(b, 16)];
                                 ^
User error: Identifier 'mf' has not been declared or assigned
> f,mf:=ResidueClassField(kr);
> fa:=mf(a);
> J :=[b: b in F| Norm(b) eq mf(a) and IsPower(b, 16)];
> #J;
2451
> mu;
```

```
l.1^3 + 1
> J[120];
F.1^5712
> y:=5712;
> k:=-2*(y div 2) *Modinv(3,8) mod ((q-1) div 2);
> k;
41688
> (y)+6*k mod ((q-1));
20544
> $1 div 16;
1284
> 20544/16;
1284
> z:=1284;
> Norm(F.1^(z*e)) eq Norm(F.1^y);
true
> zz := BaseRing(l)!(F.1^z);
> Parent(zz);
Unramified extension defined by the polynomial x^6 + x^4 + 5*x^3 + 4*x^2 + 6*x +
    3
 over 7-adic ring mod 7^20
> quo<BaseRing(l)| UniformizingElement(BaseRing(l))^20 >;
Unramified extension of Quotient of the 7-adic ring modulo the ideal generated
by 7^20 modulo x^6 + x^4 + 5*x^3 + 4*x^2 + 6*x + 3
> TeichmuellerLift(F.1^z, $1);
113011905413901895*$.1^5 - 577716996561021*$.1^4 - 30541615808233612*$.1^3 +
    32367321442551517*$.1^2 + 12283907573511177*$.1 + 22458058605923541
> t:=$1;
> Norm(t)/a-1;
-35251510373001*7^3 + O(7^20)
> l!BaseRing(l)!F.1^z;
15369376248580696*$.1^5 - 28514960393147377*$.1^4 + 28246516465639782*$.1^3 +
    17307311610437550*$.1^2 + 33918027913667333*$.1 + 7103303804806215
> $1^((7^6)^20);
113011905413901895*$.1^5 - 577716996561021*$.1^4 - 30541615808233612*$.1^3 +
    32367321442551517*$.1^2 + 12283907573511177*$.1 + 22458058605923541
> Norm(Norm(s))/a-1;

>> Norm(Norm(s))/a-1;
              ^
User error: Identifier 's' has not been declared or assigned
> l!BaseRing(l)!F.1^z;
15369376248580696*$.1^5 - 28514960393147377*$.1^4 + 28246516465639782*$.1^3 +
    17307311610437550*$.1^2 + 33918027913667333*$.1 + 7103303804806215
> $1^((7^6)^20);
113011905413901895*$.1^5 - 577716996561021*$.1^4 - 30541615808233612*$.1^3 +
    32367321442551517*$.1^2 + 12283907573511177*$.1 + 22458058605923541
> s:=$1;
> Norm(Norm(s))/a-1;
-35251510373001*7^3 + O(7^20)
> l!BaseRing(l)!F.1^z;
15369376248580696*$.1^5 - 28514960393147377*$.1^4 + 28246516465639782*$.1^3 +
    17307311610437550*$.1^2 + 33918027913667333*$.1 + 7103303804806215
> Norm($1);
```

```
-7648411713830891*$.1^5 + 12508381009243881*$.1^4 - 12720765566185340*$.1^3 +
    34139762455834157*$.1^2 + 5350546583518233*$.1 - 24130712356577562
> Norm($1)/a-1;
-4741381599441516*7 + O(7^20)
> %P
R<x>:=PolynomialRing(Integers());
K:=pAdicField(7,20);
L:=ext<UnramifiedExtension(K,6)|x^16+28>;
kr:=RingOfIntegers(K);
l:=RingOfIntegers(L);
f,mf:=ResidueClassField(k);
F,mF:=ResidueClassField(l);
pi:=UniformizingElement(kr);
Pi:=UniformizingElement(l);
mu:=1+Pi*l.1^2;
Norm(Norm(mu));
a:=$1;
fa:=mf(a);
q:=#F;
e:=RamificationIndex(L,K);
r:=Gcd(e,q-1);
r;
e;
J :=[b: b in F| Norm(b) eq mf(a) and IsPower(b, 16)];
f,mf:=ResidueClassField(kr);
fa:=mf(a);
J :=[b: b in F| Norm(b) eq mf(a) and IsPower(b, 16)];
#J;
mu;
J[120];
y:=5712;
k:=-2*(y div 2) *Modinv(3,8) mod ((q-1) div 2);
k;
(y)+6*k mod ((q-1));
$1 div 16;
20544/16;
z:=1284;
Norm(F.1^(z*e)) eq Norm(F.1^y);
zz := BaseRing(l)!(F.1^z);
Parent(zz);
quo<BaseRing(l)| UniformizingElement(BaseRing(l))^20 >;
TeichmuellerLift(F.1^z, $1);
t:=$1;
Norm(t)/a-1;
l!BaseRing(l)!F.1^z;
$1^((7^6)^20);
Norm(Norm(s))/a-1;
l!BaseRing(l)!F.1^z;
$1^((7^6)^20);
s:=$1;
Norm(Norm(s))/a-1;
l!BaseRing(l)!F.1^z;
Norm($1);
Norm($1)/a-1;
```

2.2 ClNormEquation and TameNormEQuation

2.3 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

$$\mathrm{N}(b) = a. \tag{2.1}$$

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.

2.4 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. We briefly discuss on the extensions of $\mathbb{Q}_p$ and functions defined on them.

Definition 2.4.1. 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 $x, y \in K$,

1. $\mathrm{v}(x) = \infty$ if and only if $x = 0$,
2. $\mathrm{v}(xy) = \mathrm{v}(x) + \mathrm{v}(y)$ and
3. $\mathrm{v}(x + y) \geq \min(\mathrm{v}(x), \mathrm{v}(y))$.
   A discrete valuation induces a non-archimedian absolute value via $|x| = c^{\mathrm{v}(x)}$, where c is any constant with $0 < c < 1$.

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 2.4.2. 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 2.4.3. *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 2.4.4. *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 $\mathrm{v}(a) > e/(p-1)$.

2.5 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 2.5.1. *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. [Neu99], 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 2.5.2. *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 2.5.3.

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 $v(x-1) > \frac{e}{p-1}$ and $a \in \mathbb{Z}_p$ we get

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

Theorem 2.5.4. *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.

2.6 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 $f_a = x^n + b_{n-1}x^{n-1} + \ldots + b_1x^1 + b_0$ 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 [Neu99] 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 2.6.1. *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. [Neu99] 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 $\mathrm{N}(\alpha) = x$.

2.7 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

$$\log(\mathrm{N}_{L/K}(a)) = \sum_{\sigma \in \mathrm{G}(L/K)} \log(\sigma(a)) \tag{2.2}$$

$$= \mathrm{Tr}_{L/K}(\log(a)) \tag{2.3}$$

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.

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 $\exp(\mathrm{Tr}(x))$.

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 2.7.1.

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

2.7.1 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 $(\pi^f) \times U_L$.

2.7.2 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) $Q_3 := pAdicRing(3, 10); K := ext < UnramifiedExtension(Q_3, 2)|x^12+15*x^2+3*x+3 >$
; $a := 1 + 2 * K.1^8$;

Chapter 3

Local Fundamental Class

3.1 Local Fundamental Class for Local Field

Let K be a p-adic local field then denote $\overline{K}/K$ as a separable closure of K and L/K the sub-extension of $\overline{K}/K$, v_K denotes the discrete valuation of K, which we always think of normalized so that its smallest positive value is 1,

$$\begin{aligned}
\mathcal{O}_K &= \{x \in K | v_K(x) \geq 0\} \text{ the valuation ring,} \\
\mathfrak{p} &= \{x \in K | v_K(x) > 0\} \text{ the maximal ideal,} \\
k_K &= \mathcal{O}/\mathfrak{p} \text{ the residue field of } K, p \text{ the characteristic of } k, \\
U_K &= \mathcal{O}_K - \mathfrak{p} \text{ the unit group,} \\
U_K^1 &= 1 + \mathfrak{p} \text{ the group of principal units and} \\
U_K^n &= 1 + \mathfrak{p}^n \text{ the higher unit groups.}
\end{aligned}$$

Let L/K be local field extension then L is called unramified over K if $[L : K] = [k_L : k_K] =: f_{L/K}$. If $f_{L/K} = 1$ then L/K is totally ramified extension and in this case $e_{L/K} = [L : K]$. Note that $[L : K] = e_{L/K} \cdot f_{L/K}$.
The main part of this thesis is to compute the local fundamental class of finite Galois extension L/K. For the computation we always look for the unramified extension N/K of the same degree as the finite Galois extension L/K. So, we shortly introduce the unramified extension.

Theorem 3.1.1. *1. Suppose L/K is a finite, unramified extension then the valuation ring $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ (and so $L = K(\alpha)$) for any $\alpha \in \mathcal{O}_L$ with residue fields $k_L = k_K(\bar{\alpha})$.*

2. Suppose l/k is finite extension of finite fields then there exists an unramified extension L/K with $k_L \cong l$ over k_K.

3. *Suppose L/K is a finite, unramified extension and let L'/K be any finite extension. Then*

$$\mathrm{Hom}_K(L, L') \to \mathrm{Hom}_{k_K}(k_L, k_{L'})$$

is bijective

The unramified extension L/K is Galois if and only if k_L/k_K is Galois, and in this case we have $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L, k_K)$Reference. Let L/K be a finite local Galois field extension. Then there exists a unique maximal unramified extension M of K in L, so L/M is totally ramified and every unramified extension of K in L is contained in MReference.
Before going to details on computing the fundamental classes we have to compute the cohomology groups of the extension L/K. In order to work with cohomology groups computationally, we need a finitely presented module M. Since the module $L^\times$ is not finitely generated, so we first need to find a finitely presented module M for which $\hat{H}^2(G, M) \cong \hat{H}^2(G, L^\times)$ holds.

Lemma 3.1.2. *Let L/K be a finite Galois extension, then there exists a finitely generated module M such that $\hat{H}^2(G, M) \cong \hat{H}^2(G, L^\times)$. It is given by $M = L^\times/\exp(\mathscr{L})$ for a suitable projective sublattice $\mathscr{L}$ of $\mathcal{O}_L$, where $\mathscr{L}$ can be constructed computationally.*

Proof. Reference4, Lemma 2.1. □

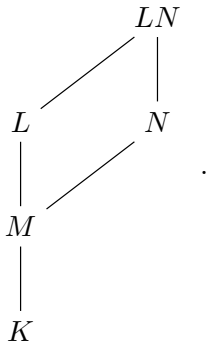
Suppose $\theta \in \mathcal{O}_L$ is a normal basis element for the extension L/K. Then

$$\{\sigma\theta \mid \sigma \in G\}$$

is a basis of L/K. More details on normal bases can be found in Reference12. However, one discovers that almost every element in $\mathcal{O}_L$ is a normal basis element and one can assume that $v_L(\theta) > e(L/\mathbb{Q}_p)/(p-1)$, where $e(L/\mathbb{Q}_p)$ denotes the ramification index of $L/\mathbb{Q}_p$. Proposition 3.1 from [Ble03] sates that $\mathscr{L} = \mathbb{Z}[G]\theta$ is a full projective sublattice of $\mathcal{O}_L$ on which the exponential map is well defined and injective.
Let E/F be a global Galois extension with $\mathrm{Gal}(E/F) = \Gamma$ and $\mathfrak{P}$ a prime ideal in E dividing a prime ideal $\mathfrak{p}$ of F. Also suppose that $E_\mathfrak{P} = L$ and $F_\mathfrak{p} = K$. Then $E_\mathfrak{P}/F_\mathfrak{p}$ is a local Galois extension such that $G := \mathrm{Gal}(E_\mathfrak{P}/F_\mathfrak{p}) = \Gamma_\mathfrak{P} = \mathrm{Gal}(L/K)$.
If k is chosen such that $\mathfrak{P}^k \subset \mathscr{L}$, then the module $L^f := L^\times/\exp(\mathscr{L})$ is the cokernel of $\exp(\mathscr{L}) \to E_\mathfrak{P}^\times/U_{E_\mathfrak{P}}^{(k)}$ and it suffices to compute the values of the exponential function up to a certain precision. Now onward, L^f will always denote a finitely generated module for which we have the isomorphism of cohomology $\hat{H}^2(G, L^f) \simeq \hat{H}^2(G, L^\times)$. Now the cohomology of group with values in module L^f can be computed by applying linear algebra methods to the standard resolution of L^f. To compute the cohomology group $\hat{H}^2(G, L^f)$ we use the maps from and to $Z^2(G, L^f)$, the group

of cocycles. Hence, for cocycles $G \times G \to L^{\times}$ one can then algorithmically decide whether they are coboundaries (mapped to zero in $\hat{H}^2(G, L^f)$) or whether they differ by a coboundary (mapped to the same element of $\hat{H}^2(G, L^f)$).

To compute the local fundamental class of a finite Galois extension L/K we use the following strategy: we choose first the unramified extension N/K of the same degree as the extension L/K, then by lemma above this implies LN/L is an unramified extension. Let us denote the maximal unramified extension in L/K be M so that we get $M = L \cap N$ and



. (3.1)

Let us denote $G = \mathrm{Gal}(L/K)$, $C = \mathrm{Gal}(N/K)$ $C' = \mathrm{Gal}(LN/L)$ and $\Gamma = \mathrm{Gal}(LN/K)$. Since N/K is finite unramified extension, so it will be easy to compute the fundamental class in it. Then the local fundamental class of L is defined to be the fundamental class of N by identifying their cohomology groups as subgroups of $\hat{H}^2(\Gamma, (LN)^{\times})$ using inflation maps:

$$\begin{array}{ccc} & & \hat{H}^2(C, N^{\times}) \\ & & \Big\downarrow \mathrm{inf} \\ \hat{H}^2(G, L^{\times}) & \xhookrightarrow{\mathrm{inf}} & \hat{H}^2(\Gamma, (LN)^{\times}) \end{array}$$

Manual and Debeerst tried to solve the local fundamental class in their papers but the solving the norm equation was not much effective so they took lot of time to compute the norm equation.

We have already seen the effective algorithms to solve the norm equations of local fields. We also have the fast algorithm in the dissertation of Debeerst, in which he uses the approach of Serre to compute the local fundamental class. We apply our norm equation in their algorithm to compute the local fundamental class. We have written our codes to solve the Frobenius equations which is very fast in the comparison of his functions.

Frobenius Equation $x^{\phi-1} = c$

We also have applied the effective way of solving the Frobenius equation. After making the norm equation very fast we found that solving the above equations was expensive. This is the case when q is very large then the factorisation of polynomial over the finite field was taking much memory and the time too. Then instead of factorisation of special polynomials over the finite field we convert this problem to solve through the vector space. Factorisation of polynomials of high degree over finite fields consumes much time. But once the polynomial is in the form of Artin-Schreier polynomial then we convert into the vectors space and then define an equation which solves for a solution. After that we can have all the solutions and then we can find all the roots of the polynomial. Due to this, we are able to decrease the computation time of local fundamental class.

We have written our codes to solve the Frobenius equations which is very fast in the comparison of his codes and it consumes less memory while solving even in large p-adic field extension as well as for high value of p.

Example 3.1.1. 229-adic field extension and its ramified extension of degree 6 will require much memory to solve. So we solve using the Artin polynomial and get the local fundamental class through **Algorithm** 2.

```
>  K1:=NumberField(CyclotomicPolynomial(18));
> K:=Compositum(NumberField(x^2-29),K1);
> Kp:=Completion(K,Decomposition(K,29)[1,1]);
> AbsoluteDegree(Kp);
12
> time CLocalFundamentalClassSerre_check(Kp,BaseField(Kp),80);

Runtime error: Precision of automorphisms of L (bounded) not high enough to
compute the cocyle!
> ChangePrecision(~Kp,120);
> time CLocalFundamentalClassSerre_check(Kp,BaseField(Kp),80);
Mapping from: Cartesian Product<GrpPerm: $, Degree 2, Order 2, GrpPerm: $,
Degree 2, Order 2> to FldPad: Kp given by a rule [no inverse]
Unramified extension defined by the polynomial x^2 + 28*$.1 + 27
 over Totally ramified extension defined by a map over Unramified extension
defined by a map over 29-adic ring mod 29^60

Time: 704.410
> time CLocalFundamentalClassSerre(Kp,BaseField(Kp),80);
Current total memory usage: 81863.2MB, failed memory request: 32.0MB
System error: Out of memory.
All virtual memory has been exhausted so Magma cannot perform this statement.

>  ChangePrecision(~Kp,60);
> time CLocalFundamentalClassSerre_check(Kp,BaseField(Kp),45);
Mapping from: Cartesian Product<GrpPerm: $, Degree 2, Order 2, GrpPerm: $,
Degree 2, Order 2> to FldPad: Kp given by a rule [no inverse]
Unramified extension defined by the polynomial x^2 + 28*$.1 + 27
 over Totally ramified extension defined by a map over Unramified extension
```

```
defined by a map over 29-adic ring mod 29^30
Time: 17.390
>  time CLocalFundamentalClassSerre(Kp,BaseField(Kp),45);

Current total memory usage: 81863.2MB, failed memory request: 32.0MB
System error: Out of memory.
All virtual memory has been exhausted so Magma cannot perform this statement.
```

Solving the local fundamental class for unramified Galois extension is an easy task.
In this, For any L/K number field extension. Let $L_{\mathfrak{P}}$ be the completion any prime ideal of $\mathfrak{P}$ of L and the e be the ramification index of $L_{\mathfrak{P}}$. Suppose the precision $L_{\mathfrak{P}}$ be n then we can compute the local fundamental class of $L_{\mathfrak{P}}$ up to precision $n - e - 1$.

To construct the local fundamental class, we consider the module L^f described as earlier. Let $\mathscr{L}$ be as above Lemma 2.1 such that $L^f = L^\times/\exp(\mathscr{L})$ is cohomologically isomorphic to $L^\times$ and let k be the smallest integer such that $\mathfrak{P}^k \subset \mathscr{L}$. We also have the surjective homomorphism $Z^2(G, L^\times/U_L^{(k)}) \twoheadrightarrow \hat{H}^2(G, L^f)$ by Remark [???] and every element of $\hat{H}^2(G, L^f)$ is represented by a cocycle of precision k. Therefore, it is sufficient to compute the local fundamental class in $\hat{H}^2(G, L^\times/U_L^{(k)})$.
Considering all notations as above we have the commutative diagram

$$\begin{array}{ccc}
 & & \hat{H}^2(C, N^\times) \\
 & & \downarrow{\scriptstyle \inf} \\
\hat{H}^2(G, L^\times) & \xhookrightarrow{\inf} & \hat{H}^2(\Gamma, (LN)^\times) \\
\downarrow & & \downarrow \\
\hat{H}^2(G, L^\times/U_L^{(n)}) & \xhookrightarrow{\inf} & \hat{H}^2(\Gamma, (LN)^\times/U_{LN}^{(n)})
\end{array}$$

in which the bottom inflation map is injective by Lemma 3.1.5 .
Since the modules $L^\times/U_L^{(n)}$ and $(LN)^\times/U_{LN}^{(n)}$ are finitely generated, we can compute their cohomology groups. The local fundamental class $u_{N/K}$ of the finite unramified extension N/K is represented as the cocycle of the form Remark 2.6.6 and we can compute $\inf(u_{N/K}) \in Z^2(\Gamma, (LN)^\times)$ and its image in $\hat{H}^2(\Gamma, (LN)^\times/U_{LN}^{(n)})$. From above diagram, using $[LN : L] = [LN : N]$ and the Proposition 2.2.7, we get the image of the fundamental class $u_{L/K}$ of L/K under the map $\inf : \hat{H}^2(G, L^\times) \to \hat{H}^2(\Gamma, (LN)^\times)$ and image of the fundamental class $u_{N/K}$ of N/K under the map $\inf : \hat{H}^2(H, N^\times) \to \hat{H}^2(\Gamma, (LN)^\times)$ coincide i.e. $\inf(u_{L/K}) = \inf(u_{N/K})$.
We compute inflation of each generator of the cohomology group $\hat{H}^2(G, L^\times/U_L^{(n)})$ in $\hat{H}^2(\Gamma, (LN)^\times/U_{LN}^{(n)})$.

One of these generators must coincide with the image of $\inf(u_{N/K})$ and it represents the fundamental class in $\hat{H}^2(G, L^\times/U_L^{(n)})$.
We summarize all the above in the following algorithm:

Algorithm 7 Local Fundamental Class by Direct Method

Input: A finite Galois extension L/K over $\mathbb{Q}_p$ with group G and a precision n.

Output: The local fundamental class $u_{L/k} \in \hat{H}^2(G, L^\times/U_L^{(n)})$ up to the finite precision n.

1: Choose N as an unramified extension of K of degree $[L : K]$ and c a cocycle representing the local fundamental class $u_{N/K}$.

2: Compute the image under the map

3:
$$\hat{H}^2(C, N^\times) \xhookrightarrow{\inf} \hat{H}^2(\Gamma, (LN)^\times) \longrightarrow \hat{H}^2(\Gamma, (LN)^\times/U_{LN}^{(n)}).$$

4: Find the preimage under the map $\hat{H}^2(G, L^\times/U_L^{(n)}) \xhookrightarrow{\inf} \hat{H}^2(\Gamma, (LN)^\times/U_{LN}^{(n)})$.

Computation of cohomology group is an expensive task so Debeerst presents an another algorithm using an exercise from "Local Fields of Serre" which computes the local fundamental class effectively.

Algorithm 8 Local Fundamental Class using Serre's Approach:

Input: A finite Galois extension L/K over $\mathbb{Q}_p$ with group G and a precision $k \in \mathbb{N}$.

Output: The local fundamental class $u_{L/K} \in Z^2(G, L^\times/U_L^{(k)})$ up to the finite precision k.

1: Let π_K and π_L be uniformizing elements of K and L respectively, E the maximal unramified subextension of L/K, $e = [L : E]$ the ramification index and d the inertia degree. Let M be the unramified extension of L of degree e and $L_{nr} = \prod_d M$.

2: Solve the norm equation $N_{M/L}(v) = u$ with $u = \pi_K \pi_L^{-e} \in U_L$ and $v \in U_M$ and define $\pi = v\pi_L$.

3: For each $\sigma \in G$ compute $u_\sigma \in M$ such that $u_\sigma^{\varphi^d - 1} = \frac{\hat{\sigma}(\pi)}{\pi} \mod U_M^{(k+2)}$.

4: Define $\beta \in C^1(G, L_{nr}^\times)$ and $\gamma \in C^2(G, L^\times)$ by equations (3.8) and (3.9).

5: **Return** γ^{-1}.

This algorithm is fast because we only compute the cocycles $Z^2(G, L^\times/U_L^{(k)})$ instead of computing the cohomology group of L/K. We have algorithms in [thisssssss] which solves norm equations effectively. In the step (2) of the above algorithm we define $u = \pi_K/\pi_L^e$. In fact due to loss of precision in while applying division the precision of u will be decreased by e. So, we can compute the local fundamental class of L/K up to precision $k - e$.

3.1.1 Brauer Group:

The Brauer group of a local field K is $B(K) = H^2(K_s/K)$ where K_s is the separable closure of K. To compute $B(K)$ we first look at the maximal unramified subextension K_{nr} of K_s such that $K \subset K_{nr} \subset K_s$. The residue class field of K_{nr} is $\overline{k}$, the algebraic closure of k (where k is the residue class field of K). $\mathrm{Gal}(K_{nr}/K) = \mathrm{Gal}(\overline{k}/k)$ is cyclic being finite extension.

Theorem 3.1.3. $H^2(K_{nr}/K) = B(K)$.

Theorem 3.1.4. *The valuation map $v : K_{nr}^* \to \mathbb{Z}$ induces an isomorphism $H^2(K_{nr}/K) \to H^2(\widehat{\mathbb{Z}}/\mathbb{Z})$.*

Abelian Extension of Local Field:
Let L/K be fin. ext. of local fields with Galois group $G := G(L/K)$ of order n.We know $H^2(L/K)$ is of order n and contains a generator $u_{L/K}$ known as local fundamental class such that $\mathrm{inv}(u_{L/K}) = 1/n \in \mathbb{Q}/\mathbb{Z}$. Also we know that $H^1(G, L^*) = 0$.
Let us suppose $H \leq G$ of order m. Since H is the Galois group of L/K' for some $K \subset K'$, we have $H^1(H, L^*) = 0$ and $H^2(H, L^*)$ is cyclic of order m and generated by $u_{L/K'} := Res(u_{L/K})$.

Definition 3.1.5. Cup product

Theorem 3.1.6. *For all $q \in \mathbb{Z}$, the map $\alpha \longmapsto \alpha \cdot u_{L/K}$ given by the cup-product is an isomorphism of $H^2(G, \mathbb{Z})$ onto $H^2(G, L^*)$.*

Application of lfc in local fields:

Theorem 3.1.7. *The cup-product by $u_{L/K}$ defines an isomorphism of $G^{ab}(L/K)$ onto $K^*/N_{L/K}(L^*)$.*

Let $\theta = \theta_{L/K}$ be the isomorphism of $K^*/N_{L/K}L^*$ on to G^{ab} which is inverse to the cup-product by $u_{L/K}$. This map θ is called the local reciprocity map or norm residue symbol.
Suppose $\alpha \in K^*$ corresponds to $\overline{\alpha} \in K^*/N_{L/K}L^*$. Then we write $\theta_{L/K}(\overline{\alpha}) = (\alpha, L/K)$. The norm residue symbol tells whether $\alpha \in K^*$ is a norm or not in L^*. If $(\alpha, L/K) = 0$ then we mean α is a norm from L^*.

Definition 3.1.8. A subgroup U of K^* is called a norm subgroup if there exists a finite abelian extension L/K with $U = N_{L/K}L^*$.

Norm groups are closely related to the reciprocity map

$$\theta_K : K^* \to G_K^{ab} = G(K^{ab}/K).$$

Proposition 3.1.9. *The map $L \longmapsto NL^*$ is a bijection of the set of finite abelian extension of K onto the set of norm subgroups of K^*.*

Proposition 3.1.10. *Let E/K be a finite extension and L/K be the largest abelian extension contained in E. Then we have*

$$N_{E/K}E^* = N_{L/K}L^*.$$

page: 143 Cassel

Chapter 4

Global Fundamental Class

4.1 Global fundamental class

In this we have been through his thesis and found that few of his assumptions are not necessary to include in the algorithm. In this the expensive part is to check the criterion of S1 - S4 conditions. It is all to known that the computation of class group and computation of S-unit group are expensive. We can see how the time increase while computing the global fundamental class for higher degree field extensions. place it after algorithm In the global field K the idèle class group C_K plays the role what the multiplicative group of fields played in the local class field theory. Let $G = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group where $\overline{K}$ is the separable closure of K. Let $\mathfrak{P}(K)$ be the set of all places of K including archimedians. For a place $\mathfrak{p} \in \mathfrak{P}(K)$, $K_\mathfrak{p}$ is the completion of K at $\mathfrak{p}$. The idèle group I_K of K is defined as $I_K = \prod_\mathfrak{p} K_\mathfrak{p}^\times$ and the idèle class group C_K of K is defined as

$$C_K = I_K/K^\times.$$

Suppose L/K be a finite Galois extension of number fields, $G = \mathrm{Gal}(L/K)$ and consider the exact sequence

$$0 \to L^\times \to I_L \to C_L.$$

Then we obtain a cohomology sequence

$$0 \to H^0(G, L^\times) \to H^0(G, I_L) \to H^0(G, C_L) \to H^1(G, L^\times).$$

This becomes

$$0 \to L^{\times G} \to I_L^{\times G} \to C_L^{\times G} \to 0,$$

since $H^1(G, L^\times) = 0$ and we get $C_L^G = I_L^{\times G}/L^{\times G} = I_K/K^\times = C_K$.

Instead of working over idèle class group C_L we work over S-idèle class group $C_{L,S}$ which we describe below:

Main theorem on the abelian extensions(TAKAGI-ARTIN):172 Cassel

Theorem 4.1.1. *1. Every abelian extension L/K satisfies the reciprocity law (i.e. there is an Artin map $\psi_{L/K}$).*

2. *The Artin map $\psi_{L/K}$ is surjective with kernel $K^* N_{L/K}(J_L)$ and hence induces an isomorphism of $C_K/N_{L/K}(C_L)$ onto $G(L/K)$.*

3. *If $M \supset L \supset K$ are the abelian extensions, then the diagram*

$$\begin{array}{ccc} C_K/N_{M/K}C_M & \xrightarrow{\psi_{M/K}} & G(M/K) \\ \downarrow j & & \downarrow \theta \\ C_K/N_{M/K}C_M & \xrightarrow{\psi_{L/K}} & G(L/K) \end{array}$$

commutes (wher θ is the usual map and j is the natural surjective map which exists because $N_{M/K}C_M \subset N_{L/K}C_L$).

4. *(**Existence Theorem.**) For every open subgroup N of finite index in C_K there exists a unique abelian extension L/K (in a fixed algebraic closure of K) such that $N_{L/K}C_L = N$.*

Cohomology of Idele Classes: We have the exact sequences

$$0 \to L^* \to J_L \to C_L \to 0.$$

The action of G on C_L is that induced by its action on J_L.

Proposition 4.1.2. $C_K \simeq C_L^G$.

Proof. The above exact sequence gives rise to cohomology sequence

$$0 \to H^0(G, L^*) \to H^0(G, J_L) \to H^0(G, C_L) \to H^1(G, L^*),$$

that is

$$0 \to K^* \to J_K \to C_L^G \to 0.$$

□

Let K be a number field and S a nonempty set of primes in K containing the set S_∞ of infinite primes in K. The ring of S-integers of K is defined as

$$\mathcal{O}_{K,S} = \cap_{p \notin S} \mathcal{O}_p = \{a \in K \mid v_p(a) \geq 0 \ \forall p \notin S\}$$

where $\mathcal{O}_p$ is the ring of integers of K_p. Its group of units $\mathcal{O}_{K,S}^\times$ and its ideal class group $Cl_S(K)$ (it is the quotient of the usual ideal class group Cl_K of K by the subgroup generated by the classes of all prime ideals in S) play a particularly important role. $Cl_S(K)$ is finite and is called the S-ideal class group.
Let $\overline{k}$ be the separable closure of the number field k. Assume that k_S be the maximal subextension of k in $\overline{k}$ which is unramified outside S. The ring of k_S is denoted by

$$\mathcal{O}_S = \cup_{K/k} \mathcal{O}_{K,S},$$

where the union is taken over all finite extensions K of k in k_S.
Now we know the S-idèle group

$$I_{K,S} := \prod_{p \in S} K_p^\times.$$

It contains the group of S-units $\mathcal{O}_{K,S}^\times$ as a discrete subgroup and we set

$$C_{K,S} = I_{K,S}/\mathcal{O}_{K,S}^\times$$

. In spite of the analogy with the formation of idèle class group $C_K = I_K/K^\times$, it is not this group which takes the role C_K in the S-theory. The reason is that if we take K/k as Galois with $G = \mathrm{Gal}(K/k)$ then $C_{k,S}$ is not always the fixed module $C_{K,S}^G$.
Consider the group

$$C_S(K) = I_K/K^\times U_{K,S}$$

instead of $C_{K,S}$, where $U_{K,S}$ is the compact subgroup

$$U_{K,S} = \prod_{p \in S} \{1\} \times \prod_{p \notin S} U_p$$

of the full idèle group I_K where U_p is the group of units of $\mathcal{O}_p$. Since $K^\times \cap U_{K,S} = 1$, we may regard $U_{K,S}$ as a subgroup of $C_K = I_K/K^\times$ and we may also write $C_S(K) = C_K/U_{K,S}$. This group is called the "S-idèle class group". If K/k is Galois then $U_{K,S}$ is cohomologically trivial since

$$H^i(G, U_{K,S}) = \sum_{p \notin S} H^i(G_p, U_p)$$

where cohomologies on right side are trivial because of the unramified extension. (U_p^i/U_p^{i+1}, for $i \geq 1$, is isomorphic F_{K_p}, residue class field of K_p and since it is cohomologically trivial and

$U_p^1 = \varprojlim U_p^1/U_p^i$ and so trivial. Also exact sec of $0 \to U_p^1 \to U_{K_p} \to F_{K_p}^\times \to 0$ and trivial comes due to long exact seq).

If K/k is Galois, then we have the exact sequence of $G(K/k)$-modules

$$0 \to U_{K,S} \to C_K \xrightarrow{\pi} C_S(K) \to 0.$$

Theorem 4.1.3. *For every finite Galois extension K/k and every $i \in \mathbb{Z}$,*

$$H^i(G(K/k), C_S(K)) \cong H^i(G(K/k), C_K).$$

Proposition 4.1.4. *(8.3.5)(Neukirch454) $C_{K,S}$ is an open subgroup of $C_S(K)$ and there is an exact sequence*

$$0 \longrightarrow C_{K,S} \longrightarrow C_S(K) \xrightarrow{\pi} Cl_S(K) \longrightarrow 0.$$

In particular, $C_{K,S} = C_S(K)$ if S omits only finitely many primes.

Note: If S omits only finitely many prime ideals, then $O_{K,S}$ is Dedekind ring with finitely many prime ideals and is hence a PID (because of page-454, Neukirch). Therefore in this case $Cl_S(K) = 0$ and $C_{K,S} \simeq C_S(K)$. We choose S sufficiently large so that $Cl_S(K) = 0$ so that we can work with $C_{L,S}$ instead of $C_S(K)$. Because of the finiteness of class group $Cl(K)$ of K and every ideal class of $Cl(K)$ is represented by an ideal which can be factorised into finite number of prime ideals one can easily find S such that $Cl_S(K) = 0$.
In order to represent $C_{F,S} \subset C_{K,S}$ by the same set of places one must have $Cl_S(F) = 0$ for subfield $F \subset L$. Suppose $L/M/K$ be a tower of number field extensions, then to represent $C_{K,S} \subset C_{L,S}$ and $C_{M,S} \subset C_{L,S}$ one must find S so that $Cl_S(K) = Cl_S(M) = Cl_S(L) = 0$.

Remark 4.1.5. Let L/K be finite number fields extension, $G = \mathrm{Gal}(L/K)$ and S satisfies::

S1. for every $\mathfrak{p} \in S$, $\sigma(\mathfrak{p}) \in S$ where $\sigma \in \mathrm{Gal}(L/K)$.

S2. S contains all ramified places of L.

S3. S contains all the infinite places of L

S4. S is large enough so that $Cl_S(F) = 0$ for all $F \leq L$.

Then one can represent $C_{F,S} \subset C_{L,S}$ for all subfields of $F \leq L$ and hence $H^i(G, C_{L,S}) \simeq H^i(G, C_L)$ because of $S4$. In fact, for every subgroup $G_F \leq G$ with $F = L^{G_F}$ we get

$$H^i(G_F, C_{F,S}) \simeq H^i(G_F, C_F).$$

Lemma 4.1.6. *Let v be an infinite place of L, $i_v : L \hookrightarrow L_v$ be the corresponding embedding and $G = \mathrm{Gal}(L/K)$. Consider the finitely generated G_v-submodule W of $L_v^\times$ which satisfies:*

1. *$i_v(U_{L,S}) \subset W$ and $W/i_v(U_{L,S})$ is torsion free and*
2. *$W \hookrightarrow L_v^\times$ induces an isomorphism in G_v-cohomology.*

Then there exists such a W with extra property that if W_v is any other G_v-submodule for which above conditions hold, there is a G_v-homomorphism $f : W \to W_v$ for which $f|_{i_v(U_{L,S})} = \mathrm{Id}$ and f induces an isomorphism in cohomology.

Proof. Chinburg, Lemma 2.1, Debeerst Proposition 3.3. □

Suppose v be the infinite place of L over the place u of K. Then $G_v = 1$ if v is real else $G_v = \{1, \sigma_v\}$ where σ_v is complex conjugation automorphism. If v is real then $K_u = \mathbb{R} = L_v$ and $H^i(G_v, L_v^\times) = 0$ for all i. In this case $W = i_v(U_{L,S})$ satisfies trivially the above lemma.

4.1.1 Finitely generated module for complex infinite place v

For every complex number field the big problem is to compute the finitely generated module. Although the algorithm is available in Debeerst but its very complicated to apply it. Once it is done one can apply the same procedure and can solve the global fundamental class. The big remark is still left to find the alternative way of computing the module so that we compute this for higher field extension too. This will be as one of the future work.

Definition 4.1.7. A submodule N of an R-module M is called a pure submodule if

$$\alpha N = N \cap \alpha M \text{ for every } \alpha \in R.$$

Consequences of the above definition : 1) Any direct summand of a module is a pure submodule. 2) A submodule N of torsion-free module M is pure iff $\forall m \in M \& \forall \alpha \in R, \alpha m \in N \implies m \in N$. 3) If M/N is torsion-free, then N is pure. If M is torsion-free and N is a pure submodule of M, then M/N is torsion free.

Theorem 4.1.8. *Let M be a free module with a finite basis over a PID R and $N \subset M$ be a submodule then N is free iff N is a direct summand of M.*

Proof. 74.4 curtis Reiner □

Theorem 4.1.9. *Let R be an integral domain and U be a rectangular matrix with coefficients in R. Then*

$$A \sim diag\{\gamma_1, \ldots, \gamma_r, 0, \ldots, 0\}, \quad \gamma_i \in R, \gamma_i \neq 0,$$

where $\gamma_i \mid \gamma_{i+1}$ for $1 \leq i \leq r-1$.

Proof. Curtis , Theorem 16.6. □

Remark 4.1.10. We will explain in details of the remark presented in the thesis. Consider the finitely generated torsion free module M and a cyclic group $G = \{1, \sigma\}$ acting on M. Let $s = 1+\sigma$ and suppose the kernel of the map s is k, which is a $\mathbb{Z}[G]$-submodule of M. In fact k is free submodule of M since $k \simeq I_G M$. Moreover, k is a $\mathbb{Z}$ direct summand of M. Thus there exists a $\mathbb{Z}$-submodule C of M such that $M = k \oplus C$ as $\mathbb{Z}$-modules. Note that C need not be a $\mathbb{Z}[G]$-submodule of M. Define $\{x + (s)\} \cdot y = xy$ for $x \in \mathbb{Z}[G], y \in k$ then k is a left $R \simeq \mathbb{Z}[G]/(s)$ module. k is torsion free R-module.

The image $(\sigma-1)M$ is in the kernel of $\sigma+1$. We know the $H^{-1}(G, M) = 0$ that is , ${}_{N_G}M/I_G(M) = 1$. So the rank of k and C are equal and let it be n. Let the basis for k be $\{b_1 \ldots b_n\}$ then using Smith normal form one can compute the basis for C such as

$$k = \mathbb{Z}b_1 + \ldots \mathbb{Z}b_n$$

and

$$C = \mathbb{Z}e_1 b_1 + \ldots \mathbb{Z}e_n b_n$$

where $e_i \in \mathbb{Z}$.

From the relation $(\sigma - 1)k \subset (\sigma - 1)C \subset k$ one can obtain $\mathbb{Z}2b_i \subseteq \mathbb{Z}e_i b_i \subseteq \mathbb{Z}b_i$. This shows $e_i \in \{1, 2\}$.
Let $r \in \mathbb{N}$ such that $e_i = 1$ for $1 \leq i \leq r$ and $e_i = 2$ for $r+1 \leq i \leq n$. From above relation, the quotient $Q = C/(\sigma - 1)k \simeq (\mathbb{Z}/2\mathbb{Z})^r$ is generated by the image $b_1^*, \ldots b_r^*$ of $b_1, \ldots b_r$. Define the surjective homoorphism $\phi : C \to Q$ such that $c \mapsto (\sigma - 1)c + (\sigma - 1)k$. Let the $\mathbb{Z}$-basis of C be $\{c_1^{'}, \ldots c_n^{'}\}$ then $k \geq r$ since phi maps C onto Q. Let $A = (\bar{a}_{ij}) \in Mat(\mathbb{Z}/2\mathbb{Z})$ be the representation matrix of the map ϕ such that

$$\phi(c_i^{'}) = \sum_{j=1}^{r} \bar{a}_{ij} b_j^*.$$

Suppose $\{c_1, \ldots, c_n\}$ be another $\mathbb{Z}[G]$- basis of C such that $c_i = \sum_{j=1}^{k} u_{ij} c_j^{'}$ where $u_{ij} \in \mathbb{Z}$ for all $1 \leq i \leq n$. Then the matrix $U = (u_(ij)$ is unimodular over $\mathbb{Z}$. The matrix $\bar{A}$ is replaced by $\bar{U}\bar{A}$ when we replace the basis $\{c_1^{'}, \ldots c_n^{'}\}$ with $\{c_1, \ldots, c_n\}$. From above Theorem 4.3, one can

conclude that there exists unimodular matrix U over $\mathbb{Z}$ so that

$$\bar{U}\bar{A} = \begin{pmatrix} \bar{l}_1 & 0 & \dots & 0 \\ 0 & \bar{l}_2 & \dots & 0 \\ . & . & \dots & 0 \\ 0 & 0 & \dots & \bar{l}_r \\ 0 & 0 & \dots & 0 \\ . & . & \dots & . \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

takes the diagonal form with the entries $l_i \in \mathbb{Z}$ such that $\bar{l}_i$ are non zero elements in $\mathbb{Z}/2\mathbb{Z}$ for $1 \le i \le r$. For such choice of U, we have

$$\phi(c_i) = \begin{cases} \bar{l}_i b_i^* & \text{if } 1 \le i \le r \\ 0 & \text{if } r+1 \le i \le k \end{cases}.$$

Find $\gamma_i \in k$ such that $(\sigma - 1)c_i - l_i b_i = (\sigma - 1)\gamma_i$ for $1 \le i \le r$ (In fact $(\sigma - 1)c_i - l_i b_i$ is square. for every $b_i^* \exists w \in C : phi(w) = b_i^*$). and $(\sigma - 1)c_j = (\sigma - 1)\gamma_j$ for $r + 1 \le j \le n$. Then clearly, $y_i = c_i - \gamma_i$ satisfies $\sigma y_i = l_i b_i + y_i$ for $1 \le i \le r$ and $\sigma y_j = y_j$ for $r + 1 \le j \le n$.
For $1 \le i \le r$, we have $\sigma y_i = l_i b_i + y_i$. Then
$\sigma(\sigma y_i) = \sigma(l_i b_i + y_i) = (\sigma + 1)(l_i b_i) + y_i = y_i$. Thus we obtain

$$M = (\mathbb{Z}b_1 \oplus \mathbb{Z}y_1) \oplus \cdots \oplus (\mathbb{Z}b_r \oplus \mathbb{Z}y_r) \oplus \mathbb{Z}b_{r+1} \oplus \cdots \oplus \mathbb{Z}b_n \oplus \mathbb{Z}y_{r+1} \oplus \cdots \oplus \mathbb{Z}y_k$$

with $\mathbb{Z}[G]$-module isomorphism $\mathbb{Z}b_j \simeq \mathbb{Z}^-$, $\mathbb{Z}y_j \simeq \mathbb{Z}^+$ for $j > r$ and

$$\mathbb{Z}[G] \simeq \mathbb{Z}b_i \oplus \mathbb{Z}y_i \text{ , } 1 \mapsto -y_i - (l_i' + 1)b_i$$

where $l_i' = (l_i - 1)/2$.

Once we have the $US/US.1 = Z^a \oplus Z[G]^b$, we will apply the morphism ψ so that the generators of Z^{a-1} are G_v-invariant. For that we give the following algorithm to compute such generators:

Algorithm 9 Generators:

Input: Generators of Z^a $i.e. V = \{x_1, \dots x_a\}, \zeta$ as torsion unit and the G_v-action.

Output: Find $\{x'_1, \dots x'_a\}$ such that $x'_2, \dots x'_a$ are Gv-invariants.

1: $e_1 = x_1$.
2: For $i \in \{2..a\}$ do
3: find a_1 such that $\psi(e_1) = \zeta^{a_1} \cdot e_1$,
4: find a_i such that $\psi(x_i) = \zeta^{a_i} \cdot x_i$,
5: find $e\&f$ such that $e \cdot a_1 + f \cdot a_i = gcd(a_1, a_2) = d$.
6: $e'_1 = e \cdot e_1 + f \cdot x_i$.
7: $x'_i = -(a_2/d) \cdot e_1 + (a_1/d) \cdot x_2$.
8: $e_1 = e'_1$ and go to step 3.
9: **return** $\{e_1, x'_2, \dots, x'_a\}$.

Once we have the $Z[G_v]$-module we will induce the $Z[G]$-module.

Using the proof of Lemma 3.1 presented [Chinburg] and following the algorithm 3.7 from [Debeerst] we give the details to construct finitely generated G_v-module for infinite place of L.

Algorithm 10 G_v-module for infinite place:

Input: L/K finite Galois extension of number fields, v a complex infinite place of L with decomposition group $G_v = \{1, \sigma\}$.

Output: Finitely generated $\mathbb{Z}[G_v]$-module W_v.

1: Compute the S-unit group $U = U_{L,S}$ using [Coh00,Alg7.4.6] and compute its free part $U_0 = U/U_{\text{tor}}$ where U_tor is torsion subgroup of U.
2: Choose $\theta \in U_{\text{tor}}/U_{\text{tor}}^2$ and define $(\mathbb{Z}; \mathbb{U}_{\approx \rtimes \setminus}) = U_{tor} \oplus \mathbb{Z}$ with G_v-action $\overline{(0,1)} = (\theta, 1)$.
3: Compute $U_0 = \mathbb{Z}^a \oplus \mathbb{Z}[G_v]^b$ for $a, b \in \mathbb{Z}$ and corresponding basis $\{\bar{x_1}, \dots, \bar{x_a}, \bar{y_1}, \dots, \bar{y_b}\}$ using theorem (74.3) of [Curtis] which we have described in the above remark.
4: Compute the lifts of U_0 as x_i and y_i respectively and find $c \in \mathbb{Z}$ such that $\bar{x_1}, \dots, \bar{x_c} \notin U^{G_v}$ and $x_{c+1}, \dots, x_a \in U^{G_v}$.
5: Apply the **Algorithm** 3 for $\{x_1, \dots, x_c\}$, so that $x_2, \dots, x_c$ are G_v-invariant and $x_1 = \theta_1 \cdot \eta_1$ where $\theta_1 \in U_{tor}$.
6: For $2 \le i \le a$ choose the signs so that $i_v(x_i) \in \mathbb{R}_{>0}$.
7: Compute algebraically independent elements $\gamma_i \in \mathbb{C}$ satisfying $\gamma_i \bar{\gamma_i} = x_i$ and $\prod_{i=2}^{a} \gamma_i^{a_i + b_i \sigma} \in U$ then $a_i = b_i$ for $i = 2, \dots, a$.
8: **Return** the module $W_v = (\mathbb{Z}; U_{\text{tor}}) \oplus \bigoplus_{i=2}^{a} \mathbb{Z}[G_v]\gamma_i \oplus \mathbb{Z}[G_v]^b$.

This algorithm is long but we have managed to compute it. The problem is in the step 7 to find γ_i and then compute the algebra $\mathbb{Z}[G_v]\gamma_i$. But we take the abstract generators instead of γ_i.

From previous section we have finitely generated module $L_v^\times$ which is cohomologically isomorphic to $L_v^\times$ for an y place v of L. In fact, $L_v^f = L_v^\times/\exp(\mathsf{L}_v)$. One can construct the finitely generated module $L_v^f = W_v \subset \mathbb{C}^\times$ for infinite place v of L. Then one can construct a finitely generated approximation to the S-idèle class group of L by fixing a set of G-representatives $S(G)$ in S and corresponding modules $L_v^\times$. We define

$$I_{L,S}^f := \bigoplus_{v \in S(G)} \mathrm{ind}_{G_v}^G L_v^f \text{ and } C_{L,S}^f := I_{L,S}^f/U_{L,S}$$

which are finitely generated module.

Proposition 4.1.11. *$H^i(G, I_{L,S}^f) \simeq H^2(G, I_{L,S})$ and $H^i(G, C_{L,S}^f) \simeq H^2(G, C_{L,S})$.*

Proof. Chinburg prop2.1. □

Let S_f and S_∞ denote set of finite places and infinite places of S respectively. For $v \in S_\infty$ the injection $L_v^f = W_v \hookrightarrow L_v^\times$ induces an isomorphism in G_v-cohomology. Thus for every $v \in S$ we have $H^2(G_v, L_v^\times) \simeq H^2(G_v, L_v^\times)$ and therefore $I_{L,S}^f$ and $I_{L,S}$ are cohomologically isomorphic. Let $S_{\infty,0}$ be a set of representatives for the G-orbits in S_∞. Let W_v be a submodule of $L_v^\times$ as of the Lemma 4.1 for $v \in S_{\infty,0}$. Then define

$$I_0 = \bigoplus\{L_v^f : v \in S_f\} \tag{4.1}$$

$$I_{L,S}^f = I_0 \oplus \bigoplus\{ind_{G_v}^G W_v : v \in S_{\infty,0}\} \tag{4.2}$$

$$I_{L,S}^q = I_0 \oplus \bigoplus\{L_v^\times : v \in S_\infty\} \tag{4.3}$$

Identifying $\{L_v^\times : v \in S_\infty\}$ with $\{ind_{G_v}^G W_v : v \in S_{\infty,0}\}$ induces an injection $I_{L,S}^f \hookrightarrow I_{L,S}^q$ and then Lemma 4.1 induces isomorphisms in cohomology. Since $U_{L,S} \subset W_v$ for $v \in S_{\infty,0}$, we have injections $U_{L,S} \to I_{L,S}^f$ and $U_{L,S} \to I_{L,S}^q$. In this way we have $C_{L,S}^f = I_{L,S}^f/U_{L,S}$ and $C_{L,S}^f = I_{L,S}^q/U_{L,S}$. Let us consider the exact diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & U_{L,S} & \longrightarrow & I^f_{L,S} & \longrightarrow & C^f_{L,S} & \longrightarrow & 0 \\
 & & \| & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & U_{L,S} & \longrightarrow & I^q_{L,S} & \longrightarrow & C^q_{L,S} & \longrightarrow & 0 \\
 & & \| & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & U_{L,S} & \longrightarrow & I_{L,S} & \longrightarrow & C_{L,S} & \longrightarrow & 0.
\end{array}$$

One can find using the consequence of five lemma that $C^f_{L,S}$ and $C_{L,S}$ are cohomologically isomorphic. Using this isomorphism we can compute the cohomology group of $C^f_{L,S}$.

Let L/K be a finite Galois field extension with $G := \mathrm{Gal}(L/K)$ and for any place w of L over place of K with decomposition decomposition group $G_w := \mathrm{Gal}(L_w/K_v)$. Then for every prime v of K we have the invariant map

$$\mathrm{inv}_{L_w/K_v} : H^2(G_v, L_w^\times) \to \frac{1}{[L_w : K_v]}\mathbb{Z}/\mathbb{Z}.$$

we obtain a canonical isomorphism

$$\mathrm{inv}_{L/K}\, H^2(G, I_L) \to \frac{1}{[L : K]}\mathbb{Z}/\mathbb{Z}, \;\; \mathrm{inv}_{L/K}(c) = \sum_{w/v} \mathrm{inv}_{L_w/K_v}(c_w)$$

from the decomposition

$$H^2(G, I_K) \cong \bigoplus_v H^2(G_v, L_w^\times).$$

Algorithm 11 Global Fundamental Class:

Input: A finite Galois extension L/K of number fields with Galois group G.

Output: The global fundamental class $u_{L/K} \in H^2(G, C^f_{L,S})$.

1: Find a cyclic extension L'/K such that $[L' : K] = [L : K]$ and choose a place u_0 of K such that there is only on place v'_0 in L' over u_0.

2: Compute the compositum $N = LL'$ with $\Gamma = \mathrm{Gal}(N/K)$ and S a set of places satisfying $(S1) - (S3)$ for which $Cl_S(K) = Cl_S(L) = Cl_S(N) = 0$.

3: Compute $\mathsf{N}_v \subset \mathcal{O}_{N_v}$ for every $v \in S_f(\Gamma)$.

4: Compute W_v using the algorithm 3.7 of Debeerst for every $v \in S_\infty$.

5: Compute $I^f_{N,S}, C^f_{N,S}$ and find the fixed modules $I^f_{L,S} = (I^f_{N,S})^G$, $C^f_{L,S} = (C^f_{N,S})^G$ where $G \subset \Gamma$ represents the Galois group of L/K.

6: Compute the cohomology group of L/K, $H^2(G, C^f_{L,S})$ and the boundaries $B^2(\Gamma, C^f_{N,S})$ using [Derekholt,Magma].

7: For a fixed precision $k \in \mathbb{N}$, compute the local fundamental class of $L_{v'_0}/K_{u_0}$ using algorithm 2 which represents the global fundamental class $u_{L'/K} \in Z^2(G', I_{L',S})$. Compute its inflation $\inf^{N/K}_{L'/K}(u_{L'/K}) \in C^2(\Gamma, C^f_{N,S})$.

8: **return** a generator g of $H^2(G, C^f_{L,S})$ such that $\inf^{N/K}_{L'/K}(u_{L'/K}) - \inf^{N/K}_{L/K}(g) \in B^2(\Gamma, C^f_{N,S})$.

The computation of S-units is expensive. Because of this the modules $I_{N,S}$ and $C_{N,S}$ become large and consumes much time when the field is of high degree and S contains many places. Since we can not reduce the degree of the field N but we can minimise the number of places in S satisfying all required conditions. We try to find the small primes in S which are unramified and satisfies the condition $S4$. We can see this in the example presented below.

1. Not needed to make all the class group to be trivial for all the subfields.
2. we use our norm equation to compute the LFC.
3. **Try to find the small primes which are unramified and which make class group to be trivial and this is possible**.

Example 4.1.1.

```
>K:=NumberField(CyclotomicPolynomial(23));
>S := [x[1]: x in Factorisation(Discriminant(MaximalOrder(K)))];
>S;
[ 23 ]
>trivialSClassNumberPrimes(K:primes:=S);
[ 23, 47 ]
> S:=[23,2];
> trivialSClassNumberPrimes(K:primes:=S);
[ 2, 23 ]
>S:=[23,3];
```

```
>trivialSClassNumberPrimes(K:primes:=S);
[ 3, 23 ]
```

The above example shows that the set of primes $[23, 47]$ makes the class group trivial for every subfields of K. We also see that set $[2, 23]$ also makes $Cl_S(F) = 0$ for all subfields F of K. To compute the global fundamental class for number field K we have to compute the local field K_v for each $v \in S$ and have to work on it. Computation of p-adic field for big prime p consumes much time and so on the functions applied on it. Therefore, it will be good to search for small prime numbers which satisfy our conditions. Also we know that the computation of local fundamental class is fast in unramified extension so we can also look for small unramified primes which make the class group trivial.

```
Aslamali@CTM-Supports-MacBook-Pro ~ % magma
Magma V2.24-5     Mon Mar 16 2020 22:41:56 on CTM-Supports-MacBook-Pro
[Seed = 2946368287]
Type ? for help.  Type <Ctrl>-D to quit.
> x:=PolynomialRing(Integers()).1;
> f := x^3 - 4*x + 1;
> AttachSpec("/Users/AslamAli/Desktop/Debeerst/magma/alispec");
> L:=SplittingField(f);
> g:=x^6-x^5-95*x^4+530*x^3-925*x^2+367*x+187;
> L1:=NumberField(g);
> time CohL,f1CL,gfc,rec := gfcCompositumcl(L,L1);
Time: 255.100
> gfc;
(1)
```

Let $N = LL1$ be the composite filed of L and $L1$ of from example. We optimised the algorithm and computed the suitable set of primes S for N so that it consumes only 255 seconds to compute the global fundamental class for L. In this computation we take S as a set of places of N lying above the places $\{11, 229, \infty\}$ of $\mathbb{Q}$ which satisfies the conditions required to implement the algorithm 5. Let US be the S-unit group of N. The place $\mathfrak{p}_1$ of $L1$ over the place of 229 of $\mathbb{Q}$ is undecomposed prime. We can compute the local fundamental class $L1_{\mathfrak{p}_1}/\mathbb{Q}_{229}$ effectively and use it. Note that working on extension of $\mathbb{Q}_{229}$ is always expensive but in our case we rather choose undecomposed place over 229 of $\mathbb{Q}$ because we target to minimize then number of places in S. Since N is totally real number field so we have $W_v = US$ the module for infinite place v of N and $G_v = \{id\}$. The S-units have 27-generators so the induced module $\mathrm{ind}_{G_v}^{\Gamma} W_v$ is generated by $27 * 18 = 486$ elements $26 * 18 = 468$ free generators. Once we reduce the number of generators then we can optimise the time of the computation global fundamental class. Debeerst takes 22 minutes to compute it.

4.1.2 gfc in relative number fields extension

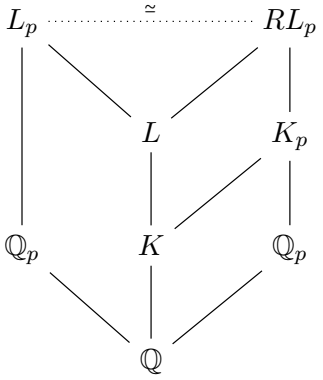
We are also able to compute the global fundamental class for relative number field extensions L/K. If we can find the exact place of w of L over v of K then one can compute easily the completion L_w over K_v. We present an algorithm to compute such completion in relative extension of number fields.

Algorithm 4.1.1. Input: L/K be a finite Galois extension of number fields and Suppose f be the polynomial defining L over K and $\mathbb{Q} < K \leq L$.
Output : Compute $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ for $\mathfrak{P}$ over $\mathfrak{p}$ in K.

1. Compute the completion $K_{\mathfrak{p}}$.
2. Convert the polynomial f as f_p over $K_{\mathfrak{p}}$.
3. Compute $K_{\mathfrak{p}}/f_p$.
4. Using RamifiedRepresentaion Command one can find the $L_{\mathfrak{P}}$.

Since we have applied all our algorithm in MAGMA and it has the function "Local Field" which will compute the step 3. Then using another function "RamifiedRepresentaion" we can convert in to p-adic field extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}/\mathbb{Q}_p$.

```
Magma V2.25-5     Thu Jun  4 2020 14:54:58 on nenepapa [Seed = 2921864985]
Type ? for help.  Type <Ctrl>-D to quit.
> x:=PolynomialRing(Integers()).1;
> K:=NumberField(x^2+5);
> y:=PolynomialRing(K).1;
> L:=NumberField(y^2+1);
> Lp,mLp :=Completion(l,Factorisation(2*MaximalOrder(l))[1,1]);
> ChangePrecision(Lp,20);
Totally ramified extension defined by a map over Unramified extension defined by
a map over 2-adic field mod 2^10
> RLp, mRLp:= Lrelative_completion_check(l,L,K,2,20);
> RLp;
Unramified extension defined by the polynomial x^2 + x + 1
 over Totally ramified extension defined by a map over 2-adic field mod 2^10
Mapping from: FldNum: l to Unramified extension defined by the polynomial x^2 +
    x + 1
 over Totally ramified extension defined by a map over pAdicField(2, 10) given
by a rule
```



In the above example we see that L_p is totally ramified over unramified extension but while computing the relative completion we have obtained unramified over ramified. But both completions L_p and RL_phave the same defining polynomials over completion $\mathbb{Q}_p$.

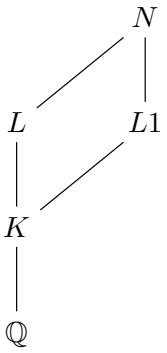
Actually while computing the global fundamental class for relative number fields we have to work in many place for absolute fields. Because of this the computation time does not decrease for the small degree fields extension.

Using this algorithm one can set up for the computation of the global fundamental class for relative field extensions.

```
Magma V2.23-11    Mon Apr 15 2019 12:05:43 on nenepapa [Seed = 3109138953]
Type ? for help.  Type <Ctrl>-D to quit.
> x:=PolynomialRing(Integers()).1;
> K:=NumberField(PolynomialWithGaloisGroup(6,2));
> s:=Subfields(K,2)[1,1];
//Below its computed RayClassGroup(37^2*ZZ);
> l1:=NumberField(x^6+x^5-15*x^4-28*x^3+15*x^2+38*x-1);
> IsCyclic(l1);
true
> L:=RelativeField(s,K);
> IsSubfield(s,l1);
true Mapping from: FldNum: s to FldNum: l1
> L1:=RelativeField(s,l1);
> Attach("ComplexModule.m");
> AttachSpec("spec");
>  time CohL,f1CL,gfc,comp,Req :=gfcCompositumcl(K,l1);
Time: 172.560
> gfc;
(1)
> time CohL,f1CL,gfc,comp :=gfcCompositum_relative_check_update(L,L1);
Time: 265.570
> gfc;
(1)
> [x: x in CohomologyGroup(CohL,2)];
[
    (0),
    (1),
```

```
    (2)
]
```

To compute global fundamental class of relative number fields extension L/K, we have to find first the cyclic extension $L1$ over K such that $[L : K] = [L1 : K]$. Once $K = \mathbb{Q}$ then finding $L1$, working on the compositum N of L and $L1$ is an easier task than computing the case when when $K \neq \mathbb{Q}$.



From above figure we see even if the degree of number fields extension L/K is very small, the computation time of $u_{L/K} \in H^2(\mathrm{Gal}(L/K), C^f_{L,S})$ depends up on the absolute degree of L/K because in many places we have to use the absolute fields. To apply the algorithm of global fundamental class one needs to find suitable S for which we must compute the class group of number fields. In MAGMA class group can be computed only for absolute field. If we can compute the class group of relative field then we can minimize some time of computations.

Restricting For $L/M/K$ be a tower of Galois field extensions. Once we have the cohomology module C for the extension L/K then we can restrict this module to for any subgroups of the Galois Group of L/K. In fact one can find the subgroup H for the relative extensions L/M and the we can restrict C for this group H by the command $Restriction(C, H)$ of $MAGMA$. And then we can compute the cohomology group and find the corresponding fundamental class for L/M by restriction map because we know that $u_{L/M} = res_{L/M}(u_{L/K})$.

Definition 4.1.12. Cup Product::::::——¿¿¿¿¿¿¿¿

Using the fundamental class $u_{L/K}$ we have the cup product which is an isomorphism

$$H^r(G(L/K), \mathbb{Z}) \xrightarrow{\sim} H^{r+2}(G(L/K), C_L),$$

for $r \in \mathbb{Z}$. Also for $L/K'/K$ be a tower of field extensions such that L/K is Galois then the diagrams

$$\begin{array}{ccc} H^r(G,\mathbb{Z}) & \xrightarrow{\sim} & H^{r+2}(G,C_L) \\ \downarrow{\scriptstyle \text{res}} & & \downarrow{\scriptstyle \text{res}} \\ H^r(G',\mathbb{Z}) & \xrightarrow{\sim} & H^{r+2}(G',C_L) \end{array} \quad \text{and} \quad \begin{array}{ccc} H^r(G,\mathbb{Z}) & \xrightarrow{\sim} & H^{r+2}(G,C_L) \\ \uparrow{\scriptstyle cor} & & \uparrow{\scriptstyle cor} \\ H^r(G',\mathbb{Z}) & \xrightarrow{\sim} & H^{r+2}(G',C_L) \end{array}$$

are commutative where $G = \mathrm{Gal}(L/K)$ and $G' = \mathrm{Gal}(L/K')$.
Note: For $r = -2$, we obtain a canonical isomorphism

$$H^{-2}(G,\mathbb{Z}) \cong G(L/K)^{ab} \to C_K/N_{L/K}C_L,$$

which is an inverse of the Artin map.

4.1.3 gfc for complex field written above few

Already written in Global Fundamental—- Let U,mU be the S-unit group of a complex number field K. Let $U_0 = U/U_t$ be the torsion free $Z[G]$ module where G is the automorphism group of number field. Since we have the order of decomposition group of infinite places of K is cyclic of order 2. In this case we use the remark 3.6 of Debeerst or Chinburg paper to create a Module for such infinite place. We have $Gv := \sigma, id$ for infinite place v. $H^{-1}(Gv, U) = 0$ so is $H^{-1}(Gv, U_0) = 0$. But $H^{-1}(Gv, U_t) \neq 0$ because $-1 \notin I_G(U_t)$.

Let $M = U_0, G := G_v$. Then $N_G(M) = k = Ker(\sigma + 1) = Z^n$. and $I_G(M) = (\sigma - 1)M = Z^n$ because $H^{-1}(Gv, U_0) = 0$ that is they are equal.
There exists another $Z[G]$ module X such that $M = k + X$ reason ???
or one can also check that the intersection is trivial or their generators generate the module M.
$(\sigma - 1)k \subset (\sigma - 1)M \subset k$. we get the factor group as $Q = (\sigma - 1)M/(\sigma - 1)k \simeq (Z/2Z)^r$ an images b_i^* of b_i generate Q.

Define the surjective homomorphism $\phi : X \to Q$ such that $x \mapsto (\sigma - 1)x + (\sigma - 1)M$. Let $< a_i^{'} >$be basis of X. Then $k > r(see)$. Let $A := (a_{ij})_{k\times r}$ be the representation matrix for ϕ such that $\phi(a_i^{'}) = \sum_1^r a_{i,j} b_j^*$.

By diagonalizing A over $Z/2Z$ by Echelon form we can find that$\overline{V} \in Gl_k(Z/2Z)$ and then corresponds to a lift $v \in Gl_k(Z)$ such that $a_i = \sum_1^k v_{i,j} a_j^{'}$ and $\phi(a_i) = c_i b_i^*$ for $1 < i \leq e$ and $\phi(a_i) = 0$ for $r + 1 \leq i \leq k$ where $c_i \in Z \setminus 2Z$.

Chapter 5

Applications

5.1 Applications

Suppose $E/L/K$ be tower of Galois field extensions then for every field we have exact sequences as:

$$0 \to K^* \to J_K \to C_K.$$

Since $H^1(L/K, C_L) = 0$ we obtain cohomology long exact sequence from using above exact sequence as:

$$0 \to H^2(L/K, L^*) \to H^2(L/K, J_L) \to H^2(L/K, J_L) \to H^3(L/K, L^*) \to \dots$$

We have similar results for the extension E/K and E/L and using these exact sequences we form an exact commutative diagram:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & H^2(L/K, L^*) & \longrightarrow & H^2(L/K, J_L) & \longrightarrow & H^2(L/K, C_L) \\
 & & \downarrow{\scriptstyle \inf} & & \downarrow{\scriptstyle \inf} & & \downarrow{\scriptstyle \inf} \\
0 & \longrightarrow & H^2(E/K, E^*) & \longrightarrow & H^2(E/K, J_E) & \longrightarrow & H^2(E/K, C_E) \\
 & & \downarrow{\scriptstyle \text{res}} & & \downarrow{\scriptstyle \text{res}} & & \downarrow{\scriptstyle \text{res}} \\
0 & \longrightarrow & H^2(E/L, E^*) & \longrightarrow & H^2(E/L, J_E) & \longrightarrow & H^2(E/L, C_E)
\end{array}$$

Let us suppose $\overline{K}$ be the algebraic closure of K and $E \to \overline{K}$ then one can also obtain commutative diagram:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & H^2(L/K, L^*) & \xrightarrow{\gamma_1} & H^2(L/K, J_L) & \xrightarrow{\epsilon_1} & H^2(L/K, C_L) \\
 & & \downarrow{\scriptstyle \inf} & & \downarrow{\scriptstyle \inf} & & \downarrow{\scriptstyle \inf} \\
0 & \longrightarrow & H^2(\overline{K}/K, \overline{K}^*) & \xrightarrow{\gamma_2} & H^2(\overline{K}/K, J_{\overline{K}}) & \xrightarrow{\epsilon_2} & H^2(\overline{K}/K, C_{\overline{K}}) \\
 & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} \\
0 & \longrightarrow & H^2(\overline{K}/L, \overline{K}^*) & \xrightarrow{\gamma_3} & H^2(\overline{K}/L, J_{\overline{K}}) & \xrightarrow{\epsilon_3} & H^2(\overline{K}/L, C_{\overline{K}})
\end{array}$$

Define $\mathrm{inv}_1 = \sum_v \mathrm{inv}_v : H^2(L/K, J_L) \to \mathbb{Q}/\mathbb{Z}$ then the sequence

$$0 \longrightarrow H^2(L/K, L^*) \xrightarrow{\gamma_1} H^2(L/K, J_L) \xrightarrow{\mathrm{inv}_1} \mathbb{Q}/\mathbb{Z}$$

is a complex form [**?**] and the following sequence

$$0 \longrightarrow H^2(L/K, L^*) \xrightarrow{\gamma_1} H^2(L/K, J_L) \xrightarrow{\mathrm{inv}_{L/K}} \tfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}.$$

By the axiom of class formation we have $\mathrm{inv}_w(\mathrm{res}(\alpha))[L_w : K_v]\,\mathrm{inv}_v(\alpha)$ where $\alpha \in H^2(\overline{K}/K, J_{\overline{K}})$ and w is a place of L over v of K. Let us define map $\mathrm{inv}_3 = \sum_v \mathrm{inv}_v : H^2(\overline{K}/L, J_{\overline{K}}) \to \mathbb{Q}/\mathbb{Z}$ so we obtain another commutative diagram

$$\begin{array}{ccc}
H^2(\overline{K}/K, J_{\overline{K}}) & \xrightarrow{\mathrm{inv}_2} & \mathbb{Q}/\mathbb{Z} \\
\downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle [L:K]} \\
H^2(\overline{K}/L, J_{\overline{K}}) & \xrightarrow{\mathrm{inv}_3} & \mathbb{Q}/\mathbb{Z}
\end{array}$$

where for every place v of K we have $\sum_{w/v}[L_w : K_v] = [L : K]$.

Proposition 5.1.1. *Let L/K be a finite Galois field extensions with Galois group G, v a place in K and w_0 be a place of L over v. Then there are mutually inverse isomorphisms*

$$H^r(G, \textstyle\prod_{w/v} L_w^\times) \underset{j_{w_0}\cdot \mathrm{res}}{\overset{\mathrm{cor}\cdot i_{w_0}}{\rightleftarrows}} H^r(G_{w_0}, L_{w_0}^\times).$$

Also for unit group U_w of L_w we have

$$H^r(G, \prod_{w/v} U_w) \underset{j_{w_0}\cdot \mathrm{res}}{\overset{\mathrm{cor}\cdot i_{w_0}}{\rightleftarrows}} H^r(G_{w_0}, U_{w_0}^{\times}).$$

Proof. [**?**],Cassels, Proposition 7.2. □

5.1.1 Ray Class Group

[FHS19].
As we have seen earlier the idèle class group of K is $C_K = I_K/K^{\times}$. Let K, $\mathcal{O}_K$ and $\mathfrak{p}_K$ be as earlier. Then a modulus $\mathfrak{m}$ of K is a formal product $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{m_p} = \mathfrak{m}_f \cdot \mathfrak{m}_\infty$ where $m_{\mathfrak{p}} = 0$ for almost all $\mathfrak{p}$, $\mathfrak{p} = v_{\mathfrak{p}}(\mathfrak{m}) \geq 0$ and $\mathfrak{m}_\infty$ a set of real embeddings of K.

Definition 5.1.2. Let K be a global field, $\mathfrak{m}$ be a modulus of K and $I_{\mathfrak{m}}$ be the group of fractional ideals prime to $\mathfrak{m}_f$ which is isomorphic to the free abelian group

$$\bigoplus_{\mathfrak{p}\nmid \mathfrak{m}_f, \mathfrak{p}\ finite} \mathbb{Z}\cdot\mathfrak{p}.$$

Also suppose

$$R_{\mathfrak{m}} = \{(a) \mid a \equiv 1 \mod \mathfrak{m}\} \subset I_{\mathfrak{m}},$$

then the quotient $I_{\mathfrak{m}}/R_{\mathfrak{m}}$ is known as the ray class group and denoted by $Cl_{\mathfrak{m}}$.

In fact when $\mathfrak{m} = 1$ then $\mathfrak{m}_{\mathfrak{p}} = 0$ for all $\mathfrak{p}$ then we obtain $Cl_1 = I_1/R_1 = Cl(\mathcal{O}_K)$.
Let us suppose that $\mathfrak{p}$ be a prime ideal of K which is unramified in the abelian field extension L/K. Then $L_{\mathfrak{p}}/K_{\mathfrak{p}}$ is unramified local field extension. So, there exists a unique Frobenius automorphism $\mathrm{Frob}_{\mathfrak{p},L/K} \in \mathrm{Gal}(L/K)$ with $\mathrm{Frob}_{\mathfrak{p},L/K}(x) \equiv x^{N(\mathfrak{p})} \mod \mathfrak{p}\mathcal{O}_L$ for all $x \in \mathcal{O}_L$. Let $\mathfrak{m}$ be a modulus which is only divisible ramified prime ideals of L/K then one can define the Artin map $\psi_{L/K} : I_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ such that $\psi_{L/K}(\mathfrak{p}) = \mathrm{Frob}_{\mathfrak{p},L/K}$ for all $\mathfrak{p}$ not dividing $\mathfrak{m}_f$.

Theorem 5.1.3. *Let L/K be a finite abelian extension of number fields and suppose $\mathfrak{m}$ be a modulus for K divisible by all ramified primes. Then the Artin map $\psi_{L/K} : I_{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ is surjective.*

Proof. Lecturenotes 21 pdf. □

From above theorem we obtain an exact sequence:

$$1 \to \ker(\psi_{L/K}) \to I_{\mathfrak{m}} \to \mathrm{Gal}(L/K) \to 1.$$

Thus we find $R_{\mathfrak{m}} \subset \ker(\psi_{L/K})$ for a modulus $\mathfrak{m}$ of K. This shows that Artin map induces an isomorphism from quotient $Cl_{\mathfrak{m}} = I_{\mathfrak{m}}/R_{\mathfrak{m}}$ to $\mathrm{Gal}(L/K)$. But when $R_{\mathfrak{m}} = \ker(\psi_{L/K})$ then $Cl_{\mathfrak{m}} \simeq \mathrm{Gal}(L/K)$ and the field L is called the **ray class field**.
Let $\mathfrak{p}$ be a prime ideal of K, $n \in \mathbb{Z}_{\geq 0}$ and define $U_{\mathfrak{p}}^n$ as

$$U_{\mathfrak{p}}^n = \begin{cases} \mathcal{O}_{K_{\mathfrak{p}}}^{\times}, & \mathfrak{p} \text{ finite }, n = 0, \\ 1 + \pi_{\mathcal{O}_{K_{\mathfrak{p}}}}^n \mathcal{O}_{K_{\mathfrak{p}}} & \mathfrak{p} \text{ finite }, n > 0, \\ K_{\mathfrak{p}}^{\times} & \mathfrak{p} \text{ real and } n = 0, \text{ or } \mathfrak{p} \text{ complex}, \\ K_{\mathfrak{p}}^{\times,+} & \mathfrak{p} \text{ real}, n > 0. \end{cases}$$

Let a modulus $\mathfrak{m}$ of K, then $U_{K,\mathfrak{m}} = \prod_{\mathfrak{p}} U_{\mathfrak{p}}^{\mathfrak{m}_{\mathfrak{p}}}$ forms an open subgroup of K because $U_{\mathfrak{p}}^{\mathfrak{m}_{\mathfrak{p}}} \subset K_{\mathfrak{p}}^{\times}$ is open for all $\mathfrak{p}$ and equals $\mathcal{O}_{K_{\mathfrak{p}}}^{\times}$ for almost all $\mathfrak{p}$.

Proposition 5.1.4. *Any open subgroup of J_K contains some $U_{K,\mathfrak{m}}$, and the quotient $|J_K/K^{\times}U_{K,\mathfrak{m}}| < \infty$.*

Proof. Proposition 9.2, Note of M. Flach Ray Class group. □

Note: For a modulus $\mathfrak{m}$ of K we have $Cl_{\mathfrak{m}} = J_K/K^{\times}U_{K,\mathfrak{m}}$.

Proposition 5.1.5. *Let K be a number field and $\mathfrak{m}$ be a modulus of K. Suppose $\overline{U}_{K,\mathfrak{m}}$ be the image of $U_{K,\mathfrak{m}}$ in C_K then we have*

$$C_K/\overline{U}_{K,\mathfrak{m}} = I_K/K^{\times}.U_{K,\mathfrak{m}} \xrightarrow{\sim} I_{\mathfrak{m}}/R_{\mathfrak{m}} = Cl_{\mathfrak{m}}$$

and

$$C_K/N_{L/K}(C_L) = J_K/K^{\times} \cdot N_{L/K}(J_L^{\times}) \cong I_{K,\mathfrak{m}}/R_{\mathfrak{m}} \cdot N_{L/K} I_{L,\mathfrak{m}}.$$

Proof. See note by M Flach , Prospostion 3.2. □

Proposition 5.1.6. *Let L/K be a normal extension of number fields and $\mathfrak{m}$ be a modulus of L which is invariant under the $G = \mathrm{Gal}(L/K)$. Then for every subgroup H of ray class group $Cl_{\mathfrak{m}}$ which is invariant under the action of G there exists an abelian extension E/L such that E/K is normal.*

Proof. [FHS19], Proposition 15. □

Let L/K be a normal extension of the fields. Compute an abelian extension E/L using [FHS19] so that E/K is normal.

Definition 5.1.7. Let L/K be a finite abelian field extension. A modulus $\mathfrak{m}$ of K is said to be admissible for an abelian extension L/K if and only if (almost) all primes $\mathfrak{p} \in \mathfrak{R}_{\mathfrak{m}}$ of K totally split in L.
OR
There exist a modulus $\mathfrak{m}$ such that $\mathrm{Gal}(L/K) \cong Cl_{\mathfrak{m}}$.

Let L/K be a finite Galois field extension, $\Delta_{L/K}$ be the discriminant of the extension L/K and $I_K(\Delta_{L/K})$ be the group of fractional $\mathbb{Z}_K$-ideals generated by the primes $\mathfrak{p}$ of $\mathcal{O}_K$ that do not divide $\Delta_{L/K}\mathcal{O}_K$. The Artin map for L/K is defined as the homomorphism

$$\psi_{L/K} : I_K(\Delta_{L/K}) \to \mathrm{Gal}(L/K), \mathfrak{p} \mapsto \mathrm{Frob}_{\mathfrak{p}}\,.$$

Theorem 5.1.8 (Kronecker-Weber)**.** *Let $L/\mathbb{Q}$ be an abelian extension then there exists an integer $m \in \mathbb{Z}_{\geq 0}$ such that the kernel of the Artin map $\psi_{L/\mathbb{Q}}$ consists of all $\mathbb{Z}-$ ideals $x\mathbb{Z}$ with $x > 0$ and $x \equiv 1 \bmod m$.*

Theorem 5.1.9 (Artin's Reciprocity)**.** *Let L/K be an abelian extension then there a nonzero ideal $\mathfrak{m}_0\mathbb{Z}_K$ such that the kernel of the Artin map defined as*

$$\psi_{L/K} : I_{\mathfrak{m}_0} \to \mathrm{Gal}(L/K), \mathfrak{p} \mapsto \mathrm{Frob}_{\mathfrak{p}}$$

consists of all principal $\mathbb{Z}_K-$ ideals $x\mathbb{Z}_K$ with x totally positive and $x \equiv 1$ mod $\mathfrak{m}_0$.

Let $P_{\mathfrak{m}}$ be the principal ideals in $I_{\mathfrak{m}}$ of K then the ray group $R_{\mathfrak{m}}$ is contained in $P_{\mathfrak{m}}$ and from [CS08] $I_{\mathfrak{m}}/P_{\mathfrak{m}} \cong Cl(K)$ for all modulus $\mathfrak{m}$. Because of the relations $R_{\mathfrak{m}} \subset P_{\mathfrak{m}} \subset I_{\mathfrak{m}}$ it is clear that $Cl_{\mathfrak{m}}$ is an extension of Cl_K by a finite abelian group $P_{\mathfrak{m}}/R_{\mathfrak{m}}$. We have an exact sequence

$$\mathcal{O}_K^{\times} \to (\mathcal{O}_K/\mathfrak{m})^{\times} \to Cl_{\mathfrak{m}} \to Cl_K \to 0.$$

where $(\mathcal{O}_K/\mathfrak{m})^{\times} = (\mathcal{O}_K/\mathfrak{m}_0)^{\times} \times \prod_{\mathfrak{p}|\mathfrak{m}_\infty} \langle -1 \rangle$ and $x \in \mathcal{O}_K$ coprime to $\mathfrak{m}_0$ is mapped in the finite group $(\mathcal{O}_K/\mathfrak{m}_0)^{\times}$ as of its residue class modulo and the signs of its images under the real primes $\mathfrak{p} \mid \mathfrak{m}_\infty$. Then the quotient $(\mathcal{O}_K/\mathfrak{m}_0)^{\times}/\mathrm{Im}[\mathcal{O}_K^{\times}]$ is isomorphic to $\mathrm{Gal}(H_{\mathfrak{m}}/H_1)$ given by Artin map where $H_{\mathfrak{m}}$ denotes the ray class field associated to modulus $\mathfrak{m}$.

```
> x := PolynomialRing(Integers()).1;
> K := NumberField(x^2+5);
> O := MaximalOrder(K);
> m := 5*O;
```

```
> r,mr := RayClassGroup(m);
> R,mR := RayResidueRing(m);
> U,mU := UnitGroup(o);
> f := hom<U->R|x:-> x@mU@@mR>;
> q,mq := quo<R|Image(f)>;
> Hm :=AbsoluteField(NumberField(RayClassField(m)));
> H1 :=AbsoluteField(HilbertClassField(K));
> IsSubfield(H1,Hm);
true Mapping from: FldNum: H1 to FldNum: Hm
```

Let $\mathfrak{m}$ be an admissible modulus for an abelian extension L/K then the Artin map induces an isomorphism

$$\psi_{L/K} : Cl_{\mathfrak{m}} \to \mathrm{Gal}(L/K), \qquad [\mathfrak{p}] \mapsto \mathrm{Frob}_{\mathfrak{p}}\,.$$

In fact this map is surjective because of the triviality of extensions in which all primes totally split[CS08].

Let $\mathfrak{q}$ be the prime of L over the prime $\mathfrak{p}$ of K then the order of $\mathrm{Frob}_{\mathfrak{p}}$ equal $[F_{L_{\mathfrak{q}}} : F_{K_{\mathfrak{p}}}] = f_{\mathfrak{p}}$ where $F_{K_{\mathfrak{p}}}$ and $F_{L_{\mathfrak{q}}}$ are the residue class fields of $K_{\mathfrak{p}}$ and $L_{\mathfrak{q}}$ respectively. For every prime ideal $\mathfrak{q} \in \mathcal{O}_L$ coprime to $\mathfrak{m}$ 1, the norm $N_{L/K}(\mathfrak{q}) = \mathfrak{p}^{f_{\mathfrak{p}}}$ is contained in the kernel of the Artin map.

Let the ideal group $A_{\mathfrak{m}} \subset I_{\mathfrak{m}}$ which corresponds to L so that $\ker(\psi_{L/K}) = A_{\mathfrak{m}}/P_{\mathfrak{m}}$ then $A_{\mathfrak{m}} = N_{L/K}(I_{\mathfrak{m}\mathbb{Z}_L}) \cdot P_{\mathfrak{m}}$.

Let us suppose $E/L/K$ be tower of global field extensions such that E/L is abelian and L/K is normal. Suppose $\mathrm{Gal}(L/K) = G, \mathrm{Gal}(E/K) = \Sigma$ and $\mathrm{Gal}(E/L) = A$. So we have an exact sequence of Galois groups:

$$1 \to A \to \Sigma \to G \to 1.$$

In fact by $A \simeq C_L/N_{E/L}(C_E)$ by Artin isomorphism.

```
K:=NumberField(x^2-5);
> o :=MaximalOrder(K);
> m :=8*o;
> r,mr :=RayClassGroup(m,[1..2]);
> A :=AbelianExtension(mr);
> L :=NumberField(A);
> G,_,psi :=AutomorphismGroup(A);
> ar :=ArtinMap(A);
> f :=hom<r->G|x:-> x@mr@ar@Inverse(psi)>;
> Kernel(f);
Abelian Group of order 1
> IsSurjective(f);
> R,mR :=RayResidueRing(m,[1..2]);
> f :=hom<R->G|x:-> x@mR@ar@Inverse(psi)>;
> q,mq :=quo<R|Kernel(f)>;
> quo< r|[q.i @@mq@mR@@mr : i in [1..Ngens(q)]]> ;
Abelian Group of order 1
Mapping from: GrpAb: r to Abelian Group of order 1
```

The following theorem is of main interest to find information of Σ:

Theorem 5.1.10. *Let $E/L/K$ be as above and so as Galois groups A, Σ, G then*

1. *Let $\gamma \in \Sigma$ have image $\overline{\gamma} \in G$. suppose $x \in C_L$ and $\psi : C_L \to A$ be the Artin map then $\psi(\overline{\gamma}x) = \gamma\psi(x)\gamma^{-1}$.*
2. *Let $v \in H^2(G, A)$ be the class of the group extension Σ, $u_{L/K} \in H^2(G, C_L)$ be the fundamental class for L/K and $\psi_* : H^2(G, C_L) \to H^2(G, A)$ is induced by the Artin map ψ then $v = \psi_*(u_{L/K})$.*

Proof. [**?**]. □

5.1.2 Shafarevich-Weil theorem

Let L/K be local or global fields extension, then Shafarevich–Weil theorem relates the fundamental class $u_{L/K}$ to an extension of Galois groups $\mathrm{Gal}(L, K)$.

Let us suppose $E/L/K$ be tower of global field extensions such that E/L is abelian and L/K is normal. $\mathrm{Gal}(E/K)$ is an extension of $\mathrm{Gal}(L/K)$ by the abelian group $\mathrm{Gal}(E/L)$ and this extension corresponds to an element of cohomology group $H^2(\mathrm{Gal}(L/K), \mathrm{Gal}(E/L))$. Let $\psi : I_L \to \mathrm{Gal}(E/L)$ be the reciprocity map and $u_{E/L} \in H^2(\mathrm{Gal}(L/K), I_L)$ be the fundamental class. Shafarevich–Weil theorem states that class of the $\mathrm{Gal}(E/K)$ is the image of fundamental class under the homomorphism of cohomology groups induced by the reciprocity law map (Artin-Tate 2009). **Note:**

1. S contains all archimedean primes,
2. S contains all prime divisors of n,
3. $J_K = K^\times J_{K,S}$
4. S contains all factors of the numerator and denominator of a_i.

Condition 4 states that all a_i are S-units that is $a_i \in K_S = K \cap J_{K,S}$.

For a number field K suppose C_K be the idèle class group of K. Suppose H be the subgroup of C_K such that $[C_K : H] < \infty$ then there exists a finite abelian extension L of K such that norm group of C_L is H. In this case H is called normic subgroup of C_K. Let $\psi : C_K \to \mathrm{Gal}(K^{ab}/K)$ be the Artin map then each normic subgroup of C_K is the inverse image of open subgroup of $\mathrm{Gal}(K^{ab}/K)$.

Let H be a normic subgroup of C_K and it corresponds to an abelian extension L over K. Suppose that $H \leq H_1$ then $H_1$is also normic so we have another abelian extension L_1/K such that $L1 \leq L$. In this case

$$N_{L/K}(C_L) = N_{L_1/K}(N_{L/L_1}(C_L)) \leq N_{L_1/K}(C_{L_1}).$$

Hasse Norm Theorem: Let L/K is a cyclic extension of number fields, then Hasse norm theorem states that if $a \in K^\times$ is a local norm everywhere, then it is a global norm. Here to be a global norm means to be an element a of K such that there is an element $b \in L$ with $\mathrm{Norm}_{L/K}(b) = a$
The theorem is no longer true in general if the extension is abelian but not cyclic. Hasse gave the counterexample that 3 is a local norm everywhere for the extension $\mathbb{Q}(\sqrt{-3}, \sqrt{13})/\mathbb{Q}$ but is not a global norm. Serre and Tate showed that another counterexample is given by the field $\mathbb{Q}(\sqrt{13}, \sqrt{17})/\mathbb{Q}$ where every rational square is a local norm everywhere but 5^2 is not a global norm.
Cassel Fröhllich page-186 for norm and page-199 for group extension:

5.2 epsilon function

reduced norm

Let G be a finite group as earlier and $E/\mathbb{Q}$ be the splitting filed of every subgroup of G. Suppose that E contains the mth roots of unity where m is the exponent of G. Let us write $R(G$ as group of all (virtual) characters and $Irr(G$ for a set of irreducible characters of G. Using Brauers's induction theorem every χ of $R(G)$ can be expressed as

$$\chi = \sum_{(H,\phi)} c_{(H,\phi)} \, \mathrm{ind}_H^G(\phi)$$

where (H, ϕ) runs through all pairs of consisting of a subgroup H of G and one dimensional characters ϕ of H, $\mathrm{ind}_H^G(\phi)$ is the induction of the character and $c_{H,\phi} \in \mathbb{Z}$. One can find the ways to compute $c_(H, \phi)$ in [BB08]
For every character χ of G , define $\mathrm{Det}_\chi(a) \in E^\times$ as $\mathrm{Det}(a) = \det(T_\chi(a))$ where $T_\chi : G \to GL_{\chi(1)}(E)$ is a representation with character χ.

Let $E[G] = \prod_{\chi \in \mathrm{Irr}(G)} A_\chi$ be the Weddeburn decomposition of $E[G]$ and $a = (a_\chi)_{\chi \in \mathrm{Irr}(G)} \in E[G]^\times$ then the reduced norm denoted by $nr(a)$ is defines as

$$nr(a) = (nr_{A_\chi/E}(a_\chi))_{\chi \in \mathrm{Irr}(G)}$$

where $nr_{A_\chi/E}(a_\chi) \in E^\times$ is the reduced is the reduced norm of (a_χ) in the central simple E-algebra A_χ. In fact from [BB08] we have

$$nr_{A_\chi/E}(a_\chi) = \mathrm{Det}_\chi(a) = \prod_{(H,\phi)} \mathrm{Det}_{\mathrm{ind}_H^G}(a)^{c_(H,\phi)}.$$

One can find more details of reduced norm in [BB08].
By Wedderburn's theorem one can decompose center of the group ring$\mathbb{C}[G]$ as:

$$Z(\mathbb{C}[G]) \simeq \bigoplus_{\chi \in \mathrm{Irr}_{\mathbb{C}(G)}} \mathbb{C}.$$

Let $L \leq \mathbb{C}$ be a subfield then the image of $Z(L[G])$ in $Z(\mathbb{C}[G])$ has following types of tuples $(a_\chi)_\chi$ for which we have $a_{\sigma\circ\chi} = \sigma(a_\chi)\ \forall \sigma \in \mathrm{Aut}(\mathbb{C}/L)$.

Lemma 5.2.1. *Let G be a finite group, $\mathbb{Q} \leq L \leq \mathbb{C}$ and $(a_\chi)_{\chi\in\mathrm{Irr}(G)} \in \prod_{\chi\in\mathrm{Irr}_{\mathbb{C}}(G)} \mathbb{C}$. Then one obtains*

$$(a_\chi)_{\chi\in\mathrm{Irr}_{\mathbb{C}}(G)} \in Z(L[G]) \Leftrightarrow (a_{\sigma\circ\chi})_{\chi\in\mathrm{Irr}_{\mathbb{C}}(G)} = (\sigma(a_\chi))_{\chi\in\mathrm{Irr}_{\mathbb{C}}(G)}$$

for all $\sigma \in \mathrm{Aut}(\mathbb{C}/L)$.

Proof. [Ble11, Lemma 2.9] □

Projective Modules

For any Ring A, we denote $\mathfrak{m}(A)$ as the class of all finitely generated A-modules and $\mathfrak{P}(R)$ as the class of all finitely generated projective A-modules.
Let $J = \mathrm{rad}(A)$ be the Jacobson radical of A and for $Q \in \mathfrak{m}(A)$ we denote $\overline{Q} = Q/J \cdot Q$ as the reduction modulo J. Suppose $P \in \mathfrak{P}(R)$ and $f \in \mathrm{Hom}_A(Q, P)$ then from [Lam06] f is an isomorphism if $\overline{f} : \overline{Q} \to \overline{P}$ is an isomorphism. From [Lam06, Corollary 1.7], we also have for $x_1, \ldots, x_r \in P$, $\langle x_1, \ldots, x_r\rangle_A = P \Leftrightarrow \langle\overline{x_1}, \ldots, \overline{x_r}\rangle_{\overline{A}} = \overline{P}$.

Definition 5.2.2. A right A-module M is said to be A-flat if $M \otimes -$ is an exact functor from left A-modules to abelian groups. That is, if $M_1 \to M_2 \to M_3$ is exact then

$$M \otimes M_1 \to M \otimes M_2 \to M \otimes M_3 \text{ is exact.}$$

We say M is $A-$ faithfully flat if the above is true for converse also.

Definition 5.2.3. A left $A-$module M is said to be finitely presented if there exists an exact sequence $A^m \to A_n \to M \to 0$ for suitable $m, n \in \mathbb{N}$.

In fact every $P \in \mathfrak{P}(A)$ is finitely presented.

Proposition 5.2.4. *Let A' be a faithfully flat extension of a subring A in the center of A'. Then for any left A-module M we have*

$$M \in \mathfrak{P}(A) \iff A' \otimes_A M \in \mathfrak{P}(A').$$

Proof. [Lam06, Proposition 2.15]. □

Let us denote (P) as the isomorphism class of $P \in \mathfrak{P}(A)$ then the Grothendieck group $K_0(A)$ is an additive abelian group generated by (P) with certain following relations:
G = free abelian group generated by $(P) : P \in \mathfrak{P}(A)$,
$H = \{(P \oplus Q) - (P) - (Q) : P, Q \in \mathfrak{P}(A)\} \leq G$,
$K_0(A) = G/H$ and
$[P]$ = image of (P) in $K_0(A)$. In fact $[P \oplus Q] = [P] + [Q] \in K_0(A)$ whenever $P.Q \in \mathfrak{P}(A)$. In general element of $K_0(A)$ is of the following type:

$$x = [P_1] + \cdots + [P_m] - [Q_1] - \cdots - [Q_n] = [P] - [Q],$$

where $P = P_1 \oplus \cdots \oplus P_m$ and $Q = Q_1 \oplus \cdots \oplus Q_n$.

Proposition 5.2.5. *For $P, Q \in \mathfrak{P}(A)$, the following are equivalent:*

1. $[P] = [Q] \in K_0(A)$;
2. $\exists M \in \mathfrak{P}(A)$ *such that* $P \oplus M \cong Q \oplus M$ *(in this case P and Q are said to be stably isomorphic);*
3. $\exists m \in \mathbb{N}$ *such that* $P \oplus A^m \cong Q \oplus A^m$.

Proof. [Lam06, Proposition 6.1]. □

Let $E_n(A)$ be the group $n \times n$ elementary matrices over A. For every matrix $M \in GL_n(A)$, one can embed this into $GL_{n+1}(A)$ by

$$M = \begin{bmatrix} A & 0 \\ 0 & 1 \end{bmatrix}$$

. Under such an identification clearly we have $E_n(A) \subset E_{n+1}(A)$. In such cases one can form an ascending unions

$$GL(A) := \bigcup_{n \geq 1} GL_n(A), \text{ and } E(A) := \bigcup_{n \geq 1} E_n(A).$$

In fact we have $E(A) = [GL(A), GL(A)]$ from [Lam06, Theorem 7.4] .

Definition 5.2.6. The Whitehead group $K_1(A)$ is defined as an abelianization of the infinite general linear group $GL(A)$. That is

$$K_1(A) = GL(A)^{ab} = GL(A)/[GL(A), GL(A)].$$

One can write the element of $K_1(A)$ by isomorphism classes of pairs (P, f) where f is an isomorphism of a projective A-module P.
Let $\phi : A \to B$ be a ring homomorphism then the relative K-group denoted by $K_0(A, \phi)$ consists of elements of type $[P, f, Q]$ where $P, Q \in \mathfrak{P}(A)$ and an isomorphism $f : B \otimes_A P \to B \otimes_A Q$ of B-modules.
Suppose R be a ring and $E/Quot(R)$ be a finite extension and G a group. The group

Let $\phi : R[G] \to E[G]$ be a ring homomorphism induced by $R \subset E$ then the relative group $K_0(R[G], \phi)$ corresponding to ϕ also denoted by $K_0(R[G], E)$ satisfies the exact sequences:

$$K_1(R[G]) \longrightarrow K_1(E[G]) \xrightarrow{\partial^1_{G,E}} K_0(R[G], E) \xrightarrow{\partial^0_{G,E}} K_0(R[G]) \longrightarrow K_0(E[G]).$$

For $j = 0, 1$, the maps $K_j(R[G]) \to K_j(E[G])$ are induced by the operator/functor(check) $E[G] \otimes_{R[G]} -$ and $\partial^1_{G,E}((E[G]^n, f)) = [R[G]^n, f, R[G]^n]$ and $\partial^0_{G,E}([P, f, Q]) = [P] - [Q]$.

For semi-simple K-algebras A one obtains $A \simeq \oplus_{i=1}^r A_i$ by Wedderburn's decomposition which induces $Z(A) \simeq \oplus_{i=1}^r Z(A_i)$ and $K_1(A) \simeq \oplus_{i=1}^r K_1(A_i)$ from [Deb11]. One can define the reduced norm map as:

$$nr : K_1(A) \to Z(A)^\times \simeq \bigoplus_{i=1}^r Z(A_i)^\times.$$

Let $E/\mathbb{Q}$ be a finite extension such that $\zeta_m \in E$ where m is exponent of G. Then fro a group ring $E[G]$ we have $\mathrm{Irr}_E(G) = \mathrm{Irr}_{\mathbb{C}}(G)$. Since $E(G)$ is a semi-simple algebra we obtain the reduced norm map

$$\mathrm{nr} : K_1(E[G]) \to Z(E[G])^\times \simeq \bigoplus_{\chi \in \mathrm{Irr}_E(G)} E^\times.$$

In fact this map nr is injective and map $\widehat{\partial}^1_{R[G],E} = \partial^1_{R[G],E} \circ \mathrm{nr}^{-1} : \mathrm{Im}(nr) \to K_0(R[G], E)$ is called boundary homomorphism.
In this we are interested in the case of $R = \mathbb{Z}_p$ and $E/\mathbb{Q}_p$ where the reduce norm map is an isomorphism[?].

$$\begin{array}{ccc} Z(E[G])^\times & & \\ \uparrow{\scriptstyle \simeq} & \searrow^{\widehat{\partial}^1_{G,E}} & \\ K_1(E[G]) & \xrightarrow{\partial^1_{\mathbb{Z}_p[G],E}} & K_0(\mathbb{Z}_p[G], E) \end{array} \quad \mathrm{nr}$$

So, we obtain the boundary homomorphism $\widehat{\partial}^1_{G,E} := \widehat{\partial}^1_{\mathbb{Z}_p[G],E} = \partial^1_{\mathbb{Z}_p[G],E} \circ \mathrm{nr}^{-1}$ from $Z(E[G])^\times$ to $K_0(\mathbb{Z}_p[G], E)$.

Let P be a complex of $R[G]$-modules and for simplicity we write $P_E := E[G] \otimes_{R[G]} P$ which is the complex of $E[G]$-modules obtained from P applying the functor $E[G] \otimes_{R[G]} -$. Let $H^+(P_E)$ and $H^-(P_E)$ denote the sum of cohomology groups of even and odd degree respectively. Then the isomorphism $t : H^+(P_E) \xrightarrow{\simeq} H^-(P_E)$ is called a trivialization.

Suppose P be a bounded complex of finitely generated projective $R[G]$-modules then applying the functor $E[G] \otimes_{R[G]}$ to the short exact sequences

$$0 \to B^i(P) \to Z^i(P) \to H^i(P) \to 0 \text{ and } 0 \to Z^i(P) \to P^i \to B^{i+1}(P) \to 0,$$

we obtain the exact sequences as

$$0 \to B^i(E[G] \otimes_{R[G]} P) \to Z^i(E[G] \otimes_{R[G]} P) \to H^i(E[G] \otimes_{R[G]} P) \to 0$$

$$\text{and} \quad 0 \to Z^i(E[G] \otimes_{R[G]} P) \to E[G] \otimes_{R[G]} P^i \to B^{i+1}(E[G] \otimes_{R[G]} P) \to 0.$$

From above exact sequences one gets isomorphisms $Z^i(P_E) = Z^i(E[G] \otimes_{R[G]} P) \simeq B^i(E[G] \otimes_{R[G]} P) \oplus H^i(E[G] \otimes_{R[G]} P)$ and $P^i_E = E[G] \otimes_{R[G]} P^i \simeq Z^i(E[G] \otimes_{R[G]} P) \oplus B^{i+1}(E[G] \otimes_{R[G]} P)$. Using these decompositions we have

$$\begin{aligned}
P^+_E &:= \bigoplus_{i \text{ even}} P^i_E \simeq \bigoplus_{i \text{ even}} (Z^i(p_E) \oplus B^{i+1}(P_E)) \\
&\simeq \bigoplus_{i \text{ even}} (B^i(P_E) \oplus H^i(P_E) \oplus B^{i+1}(P_E)) \\
&= \bigoplus_{i \text{ even}} H^i(P_E) \oplus \bigoplus_i B^i(P_E) \\
&\xrightarrow{t} \bigoplus_{i \text{ odd}} H^i(P_E) \oplus \bigoplus_i B^i(P_E) \\
&= \bigoplus_{i \text{ odd}} (B^i(P_E) \oplus H^i(P_E)) \oplus \bigoplus_{i \text{ odd}} B^{i+1}(P_E) \\
&= \bigoplus_{i \text{ odd}} (Z^i(p_E) \oplus B^{i+1}(P_E)) := P^-_E.
\end{aligned}$$

Thus, we obatin an isomorphism $t_* : P^+_E \to P^-_E$ induced from trivialization map t.

Let L/K be a finite Galois extension of number fields with Group $\mathrm{Gal}(L/K) = G$ and suppose w be a place of L over the place v of K.

Definition 5.2.7. Let the χ be a character of G_w which corresponds to the Galois representation $\rho : G_w \to GL(V_\chi)$. Then the Local Artin L- function is defined as

$$L_{L_w}(\chi, s) = \det(1 - \phi_w \,\mathrm{Norm}_{K_v/\mathbb{Q}_p}\, \mathfrak{p}^{-s}_{K_v} \mid V_\chi^{I_\mathfrak{P}})^{-1}$$

where $\mathfrak{p}_{K_v}$ is the prime ideal of K_v, ϕ_w is a lift of Frobenius automorphism in G_w/I_w and the characteristic polynomial of $\rho(\phi_w) \in GL(V_\chi^{I_\mathfrak{P}})$ is evaluated at $\mathrm{Norm}_{K_v/\mathbb{Q}_p}\mathfrak{p}_{K_v}^{-s}$.

For infinite place w let us suppose $n = \dim_{\mathbb{C}}(V)$, $n^+ = \dim_{\mathbb{C}}(V_{G_w})$ and $n^- = n - n^+$ and define the Artin L- function

$$L_{L_w}(\chi, s) = \begin{cases} (\pi^{-s/2}\Gamma(s/2))^{n^+}(\pi^{-(s+1)/2}\Gamma((s+1)/2))^{n^-}), & \text{for } K_v = \mathbb{R}, \\ (2(2\pi)^{-s}\Gamma(s))^n & \text{for } K_v = \mathbb{C}. \end{cases}$$

Let us suppose that $\overline{\chi}$ denotes the complex conjugate of χ, $W(\chi)$ the Artin root number and $\mathfrak{f}(\chi)$ the conductor of χ as defined in Fröhlich **which we define later on**. Now we define the ϵ-function and the Galois Gauss sum as follows:

Definition 5.2.8. Let χ be any character of decomposition group G_w then we define the ϵ-function as:

$$\epsilon_{L_w/K_v}(\chi, s) = \begin{cases} W_{\mathbb{Q}_p}(i_{K_v}^{\mathbb{Q}_p}\overline{\chi})(\mathrm{Norm}_{K_v/\mathbb{Q}_p}(d_{K_v})^{\chi(1)}\,\mathrm{Norm}_{K_v/\mathbb{Q}_p}(\mathfrak{f}(\chi)))^{\frac{1}{2}-s} & \text{for } K_v/\mathbb{Q}_p, \\ W_{\mathbb{R}}(i_{K_v}^{\mathbb{R}}\overline{\chi}) & \text{for } K_v = \mathbb{R}. \end{cases}$$

where d_{K_v} denotes the absolute discriminant of K_v. The local Galois Gauss sum is defined as

$$\tau_{L_w/K_v}(\chi) = W_{K_v}(\overline{\chi})\sqrt{\mathrm{Norm}_{K_v/\mathbb{Q}_p}\mathfrak{f}(\chi)} \in \mathbb{C}.$$

For every place w of L we have the decomposition group G_w and for any character χ of G we can restrict it to G_w and obtain a local character χ_w to G_w.

Definition 5.2.9. Let L/K be a finite Galois field extension of global fields, S be a set of all places K and S_f be the set of all finite places of K. Then the completed Artin L-function, the global ε-function and the global Galois Gauss sum are defined as follows:

$$\begin{aligned} \Lambda_{L/K}(\chi, s) &= \prod_{v\in S} L_{L_w/K_v}(\chi_w, s), \\ \varepsilon_{L/K}(\chi, s) &= \prod_{v\in S} \varepsilon_{L_w/K_v}(\chi_w, s) \quad \text{and} \\ \tau_{L/K}(\chi) &= \prod_{v\in S_f} \varepsilon_{L_w/K_v}(\chi). \end{aligned}$$

In case if S is a finite set of places of K then we define the S-truncated Artin L-function of a character as

$$L_{L/K,S}(\chi, s) = \prod_{v\notin S} L_{L_w/K_v}(\chi, s).$$

We denote the leading term of $L_{L/K,S}(\chi, s)$ at $s = s_0$ by $L^*_{L/K,S}(\chi, s_0)$.

5.3 Creating Normal Extension

```
> K:=NumberField(PolynomialWithGaloisGroup(6,2));
> r,mr:=RayClassGroup(9*MaximalOrder(K),[1..6]);
>  A:=AbelianExtension(mr);
> L:=NumberField(A);
> q,mq:=quo<r|SylowSubgroup(r,3)>;
> A1:=AbelianExtension(Inverse(mq)*mr);
> A1;
FldAb, defined by (<[9, 0, 0, 0, 0, 0]>, [1     2       3       4       5
6])
of structure: Z/2 + Z/2

> l:=NumberField(A1);
> AbsoluteField(l);
Number Field with defining polynomial $.1^24 - 90*$.1^22 + 2357*$.1^20 -
    11830*$.1^18 - 41070*$.1^16 - 581010*$.1^14 + 47630645*$.1^12 -
    509985570*$.1^10 + 5533389010*$.1^8 - 43273483590*$.1^6 + 387605577333*$.1^4
    - 1533431619050*$.1^2 + 11681842172641 over the Rational Field
> IsNormal($1);
true
> q,mq:=quo<r|SylowSubgroup(r,2)>;
> A1:=AbelianExtension(Inverse(mq)*mr);
> A1;
FldAb, defined by (<[9, 0, 0, 0, 0, 0]>, [1     2       3       4       5
6])
of structure: Z/3

> l:=NumberField(A1);
> AbsoluteField(l);
Number Field with defining polynomial $.1^18 - 9*$.1^17 + 3*$.1^16 + 174*$.1^15
    - 357*$.1^14 - 1083*$.1^13 + 3463*$.1^12 + 2001*$.1^11 - 13218*$.1^10 +
    3150*$.1^9 + 22479*$.1^8 - 14883*$.1^7 - 15063*$.1^6 + 16155*$.1^5 +
    741*$.1^4 - 5073*$.1^3 + 1557*$.1^2 - 37 over the Rational Field
> IsNormal($1);
true
> r,mr:=RayClassGroup(9*MaximalOrder(K),[1..5]);// not invariant subgroup in
   infinite place
> r;
Abelian Group isomorphic to Z/6
Defined on 2 generators
Relations:
    3*r.1 = 0
    2*r.2 = 0
> time IsNormal(AbsoluteField(NumberField(AbelianExtension(mr))));
false
Time: 0.840
```

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

[BB08] Werner Bley and Manuel Breuning. Exact algorithms for p-adic fields and epsilon constant conjectures. *Illinois J. Math.*, 52(3):773–797, 2008.

[Ble03] W. Bley. Numerical evidence for a conjectural generalization of Hilbert's Theorem 132. *LMS J. Comput. Math.*, 6:68–88, 2003. With an appendix by D. Kusnezow.

[Ble11] Werner Bley. Numerical evidence for the equivariant Birch and Swinnerton-Dyer conjecture. *Exp. Math.*, 20(4):426–456, 2011.

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

[CS08] Henri Cohen and Peter Stevenhagen. Computational class field theory. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 497–534. Cambridge Univ. Press, Cambridge, 2008.

[Deb11] R. Debeerst. *Algorithms for Tamagawa Number Conjectures*. Ph. D. thesis. URL http://kobra.bibliothek.uni-kassel.de/handle/urn:nbn:de:hebis: 34-2011060937825, 2011.

[Dok08] T. Dokchitser. Local fields. *Lecture notes*, 2008.

[FHS19] Claus Fieker, Tommy Hofmann, and Carlo Sircana. On the construction of class fields. In *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*, volume 2 of *Open Book Ser.*, pages 239–255. Math. Sci. Publ., Berkeley, CA, 2019.

[Fie09] Claus Fieker. Minimizing representations over number fields. II. Computations in the Brauer group. *J. Algebra*, 322(3):752–765, 2009.

[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.

[FZ16] Claus Fieker and Yinan Zhang. An application of the p-adic analytic class number formula. *LMS J. Comput. Math.*, 19(1):217–228, 2016.

[Gir99] Kurt Girstmair. An algorithm for the construction of a normal basis. *J. Number Theory*, 78(1):36–45, 1999.

[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.

[Lam06] T. Y. Lam. *Serre's problem on projective modules*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2006.

[Led05] Arne Ledet. *Brauer type embedding problems*, volume 21 of *Fields Institute Monographs*. American Mathematical Society, Providence, RI, 2005.

[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.

[Neu99] 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.

[Neu13] Jürgen Neukirch. *Class field theory*. Springer, Heidelberg, 2013. The Bonn lectures, edited and with a foreword by Alexander Schmidt, Translated from the 1967 German original by F. Lemmermeyer and W. Snyder, Language editor: A. Rosenschon.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[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.