Class Field Theory

Xingfeng Lin

- last updated on Feburary 16, 2026

Preface

These notes are a striving-for-conciseness material focusing on class field theory. By the time I started to write the main context, I had already been halfway on learning the course on class field theory (lectured by Ruochuan Liu) in Peking University. Therefore I assume familiarity with Lubin-Tate formal groups, (finite) group cohomology, local class field theory, etc. (roughly based on Yiwen Ding, Sutherland and Neukirch), but still I will mention some fundamental basics of them.

- Apr. 2025

These notes are a continuation of the unfinished notes on class field theory. There is a slight change in writing style, but still I stick to the principle of creativity and freedom of writing. The notes cover material equivalent to a full-semester advanced graduate course on class field theory. Among all the arguments or examples in the main text, while a few of them have their owners explicitly indicated, others are considered standard or well-known in the literature.

- Jan. 2026

Nankai University,
Xingfeng Lin

Contents

1 Abstract Class Field Theory

1.1 Infinite Galois Theory

For two field extensions $L/k, K/k$, we do compositum by assuming that they lie in a same extension of k.

1. Knowing that every Galois group G is a profinite group, it is totally disconnected and compact. If we only want to show G is Hausdorff, there is an easy way.

   Proof. For any two distinct $\sigma, \pi \in G$, they must act differently on some finite subextension, thus falling into disjoint cosets of a normal subgroup of finite index (which are defined to be open). □

2. Every closed subgroup of a profinite group is again a profinite group. Since every open subgroup is closed, every open subgroup is also profinite.

3. Suppose L/k is a Galois extension, K/k an arbitrary extension. Then we have a topological isomorphism:

   $$\begin{aligned} Gal(LK/K) &\longrightarrow Gal(L/L\cap K) \\ \sigma &\longmapsto \sigma|_L \end{aligned}$$

   Proof. Consider finite Galois subextension of $L/L\cap K$. Apply finite Galois theory and view $Gal(L/L\cap K)$ as an inverse limit. □

4. For a family of Galois extension K_i/k, we wonder the relation between $Gal(K/k)$ and $\Pi_i Gal(K_i/k)$, where K is the compositum of K_i. In fact, they are topologically isomorphic if K_i intersects with the compositum of the rest K_j on k, for each i.

5. Suppose G is a profinite group, H a closed normal subgroup. Then G/H is a profinite group.

6. For a profinite group G, abelianization should be defined to be $G/(closure\ of\ [G,G])$. (Note: ker. of a homom. of Hausdorff groups is closed because a point is closed, and the closure of a normal subgroup is still normal.)

For infinite Galois extensions, the 1-1 Galois correspondence fails spectacularly, roughly because there are too many subgroups of a infinite Galois group. For example, $Gal(\overline{F_p}/F_p) \simeq \prod_p \mathbb{Z}_p$ has uncountably many (abstract) subgroups of finite index, but $\overline{F_p}/F_p$ has only countably finite subextensions. Another example is similar. $G := Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ has uncountably many subgroups of index 2 (one can construct a surjective group homomorphism $G \longrightarrow \prod_{[K:\mathbb{Q}]=2} \mathbb{Z}/2$), but $\mathbb{Q}$ has only countably many quadratic extensions. However, given a subextension M/K of an infinite Galois extension L/K, we can always determine a normal subgroup $Gal(L/M)$ of $Gal(L/K)$.

To distinguish such subgroups, we give the Galois group Krull topology, making those subgroups corresponding to a subextension closed. Then we can establish the infinite Galois correspondence between open normal subgroups of the Galois group and Galois subextensions of the Galois extension.

1.2 Projective Limit and Inductive Limit

1. Projective limit (inverse limit): defined as a subset of the product compatible with maps in the projective system.

   Inductive limit (direct limit): defined as a quotient of the disjoint union by identifying those whose germs agree in the inductive system.

2. (UNIVERSAL PROPERTY) (here proj. limit, similar for ind. limit) Suppose there is a family of (continuous) homom. of topological groups $H \longrightarrow G_i$, compatible with the maps in the projective system G_i, then there exists a unique continuous homom. $\phi : H \longrightarrow \varprojlim G_i$ such that $H \longrightarrow G_i$ factors as $\pi_i \circ \phi$, where π_i is the natural projection map $\varprojlim G_i \longrightarrow G_i$.

3. $\varprojlim$ and $\varinjlim$ can be regarded as functors. For example, $\varprojlim$ is a functor from the category of proj. systems (with morphisms) to the category of topological groups (with continuous homoms.). Consider their exactness.

   Actually, $\varinjlim$ is exact, in the sense: given three proj. systems G_i, G_i', G_i'', and exact seqs. $G_i \longrightarrow G_i' \longrightarrow G_i''$, for each i, applying $\varinjlim$ we have the exact seq. $\varinjlim G_i \longrightarrow \varinjlim G_i' \longrightarrow \varinjlim G_i''$. (The proof follows immediately from definitions.)

   $\varprojlim$ is not exact in general, but for compact Hausdorff groups, it is:

   Proof. Say $x \in \varprojlim G_i'$ maps to 1, then x_i maps to $1 \in G_i''$, for each i. So x_i has nonempty closed (thus compact) preimage. With the fact that proj. limit of nonempty compact groups is nonempty compact (in a compact space, if a family of closed subset intersect on nothing, then there is a subfamily intersecting on nothing), the conclusion follows. □

   Remark 1. Similar to groups, you can call a ring a topological ring by giving it a topology such that ring operations are all continuous. Moreover, you can call a topo. ring a profinite ring if it is compact and totally disconnected. However we will restrict our attention to groups for now.

4. Examples of profinite groups (or rings):

   (a) Galois groups, the p-adic integers, a discrete valuation ring (and its subgroups $1 + (\pi)^n$).

   (b) the Prüfer ring ($\hat{\mathbb{Z}}$):

   Compute the kernel of the projection map $\hat{\mathbb{Z}} \longrightarrow \mathbb{Z}/n\mathbb{Z}$, which turns out to be $n\hat{\mathbb{Z}}$. Thus we have an isom.:

   $$\hat{\mathbb{Z}}/n\hat{\mathbb{Z}} \longrightarrow \mathbb{Z}/n\mathbb{Z}.$$

   From this we know that $n\hat{\mathbb{Z}}$ is an open subgroup of $\hat{\mathbb{Z}}$. Actually, for any open subgroup H of $\hat{\mathbb{Z}}$, it is of finite index (say n) because $\hat{\mathbb{Z}}$ is compact. So clearly $n\hat{\mathbb{Z}} \subseteq H$. With $[\hat{\mathbb{Z}} : n\hat{\mathbb{Z}}] = n$, we have $H = n\hat{\mathbb{Z}}$. So $n\hat{\mathbb{Z}}$ are the all open subgroups of $\hat{\mathbb{Z}}$.

   More generally, for a procyclic group G, G^n are all the open subgroups. Procyclic groups are defined to be profinite groups with a dense cyclic subgroup. By the way, to prove G^n is an open subgroup, we first show it is of finite index by noting that the quotient group contains a finite dense subset, and then

show it is open, by noting that multiplication is a closed map in a compact Hausdorff group. Furthermore, you can prove $[G : G^n] = n$. Procyclic groups are generalizations of $\hat{\mathbb{Z}}$ and $\mathbb{Z}_p$, but not a very "essential" generalization. We have:

Proposition 1. Every procyclic group is a quotient of $\hat{\mathbb{Z}}$.

Proof sketch : For a procyclic group $G = \overline{< x >}$, verify the homomorphism $\mathbb{Z}/n\mathbb{Z} \longrightarrow G/G^n,\ 1 \longmapsto x$ is surjective, for any n, yielding a sujection $\hat{\mathbb{Z}} \longrightarrow G$. By Chinese Remainder Theorem, we have an isom.:

$$\hat{\mathbb{Z}} \simeq \varprojlim_{n}(\Pi_{p|n}\mathbb{Z}/p^{v_p}\mathbb{Z}) \simeq_{n \text{ varies over prime powers}} \varprojlim_{p,i}(\Pi_{p,i}\mathbb{Z}/p^i\mathbb{Z}) \simeq \Pi_p\mathbb{Z}_p.$$

So you see that the Prüfer ring is the product of all rings of p-adic integers.

Remark 2. the Prüfer ring (as a group under addition) arises as $G(\overline{\mathbb{F}}/\mathbb{F})$, where $\mathbb{F}$ is a finite field, or as $G(K^{ur}/K)$ where K is a nonarchimedean local field.

(c) The Potryagin dual of an abelian torsion group:
Let A be an abelian torsion group. Put $\chi(A) := Hom(A, \mathbb{Q}/\mathbb{Z})$. Call it the potryagin dual of A. For example, take $A = \mathbb{Q}/\mathbb{Z}$. Let $A_n = \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. So we have $A = \cup_n A_n$, which implies $\chi(A) = \varprojlim_n \chi(A_n)$, where $\chi(A_n) \simeq \mathbb{Z}/n\mathbb{Z}$. Therefore, $\chi(A) \simeq \hat{\mathbb{Z}}$.

5. (EXTEND HOMOMORPHISMS AND DEFINE "POWERS"):

ASK : Is the following statement true?

Let H, G be profinite groups, H_0 a dense subgroup of H. Given any continuous homomorphism $\phi : H_0 \longrightarrow G$, there exists a continuous homomorphism $\Phi : H \longrightarrow G$ extending ϕ.

ANSWER : Yes. First define $\Phi(h), h \in H$, as the unique (G being Hausdorff) limit of $\phi(h_i)$,where h_i converges to h (which exists due to continuity). You can check the definition is independent of the sequence h_i chosen and is clearly a homomophism.

Now look at some explicit cases:

Proposition 2. For a profinite group G, the power map $G \times \mathbb{Z} \longrightarrow G$, $(g, n) \longmapsto g^n$ can be extended to a continuous homomorphism $G \times \hat{\mathbb{Z}} \longrightarrow G$, $(g, a) \longmapsto g^a$ such that $g^{a+b} = g^a g^b$ and $(g^a)^b = g^{ab}$ if G is abelian.

Proof. Note that $G \times \mathbb{Z}$ is dense in $G \times \hat{\mathbb{Z}}$. You can extend the homomorphism continuously. □

6. (SYLOW SUBGROUPS OF PROFINITE GROUPS)

Let G be a profinite group. A closed subgroup H is called a p-Sylow subgroup of G if for every open normal subgroup N, HN/N is a p-Sylow subgroup of G/N.

Example 1. the p-Sylow subgroups of $\mathbb{Z}_p, \mathbb{Z}_p^\times, \hat{\mathbb{Z}}$ are $\mathbb{Z}_p$. (When calculating the p-Sylow subgroup of $\mathbb{Z}_p^\times$, recall: Guass showed that $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if $n = 2, 4, p^k$, or $2p^k$ for odd primes p.)

7. For profinite groups, abelianization commutes with taking inverse limit.

1.3 Abstract Galois Theory

1. *INTRODUCTION* : The idea of abstract Galois theory is to develop Galois theory in the pure group theory, beginning with a profinite group and its closed subgroups. You (will) know that every profinite group is the Galois group of some Galois extension. Terminologies and notations are purely group theoretical. For example, closed subgroups G_K of a profinite group G is indexed by "fields" K; by a *field extension* L/K we mean $G_L \subseteq G_K$; L/K is said to be normal or Galois if G_L is a normal subgroup of G_K. Let k be the "field" indexing G.

2. Define the norm map $N_{L/K} : A_L \longrightarrow A_K$, $a \longmapsto \Pi_{\sigma \in G_L \backslash G_K} a^\sigma$, where σ ranges over right cosets. (Note that a^σ depends only on right cosets of G_L in G_K.)

3. Kummer theory has a purely (abstract) group theoretical formulation.

   Start with a surjective G-homomorphism:

   $$\begin{aligned} \wp : A &\longrightarrow A \\ a &\longmapsto a^\wp, \end{aligned}$$

   which satisfies $\mu_\wp := ker(\wp)$ is finite cyclic of order n (called the exponent of $\wp$), where A is a continuous multiplicative G-module satisfying the AXIOM, analog of Hilbert 90, and G is a profinite group.

   Fix a field K such that $\mu_\wp \subseteq A_K$.

   Theorem 1. *Every Kummer extension (defined as the field indexing the closed subgroup of G_K that fix some preimages of $\wp$) is an abelian extension of exponent n, where n is the exponent of $\wp$. Conversely, every abelian extension of K of exponent n is a Kummer extension (with respect to $\wp$).*

   Remark 3. You see:

   (a) The exponent of a Kummer extension is determined by the map $\wp$.

   (b) The abstract Kummer extensions coincide with our explicit Kummer extensions if you take $\wp$ to be taking n^{th} power.

   The following theorem is the main result of Kummer theory.

   Theorem 2. *There is a one-to-one correspondence between*

   $$\begin{aligned} \{\textit{subgroups } \Delta \textit{ of } A : A_K^\wp \subseteq \Delta \subseteq A_K\} &\longrightarrow \{\textit{abelian extensions } L \textit{ of } K \textit{ of exponent } n\} \\ \Delta &\longmapsto K(\wp^{-1}(\Delta)) \\ A_L^\wp \cap A_K &\longleftarrow L, \end{aligned}$$

   where the n is the exponent of $\wp$.

   EXPLICIT APPLICATION : Let k be an (actual) field, $G := Gal(\bar{k}/k)$, $\wp : a \longmapsto a^n$. Let K/k contain all n^{th} roots of 1 (which is the usual setting of abelian Kummer theory). We obtain the explicit abelian Kummer theory.

4. Hilbert 90:

   Suppose L/K is a finite Galois extension. Put $G := Gal(L/K)$. We have the general version of Hilbert 90:

Theorem 3. $H^1(G,L^\times)=0$.

Proof. Use the linear independence of automorphisms of a field. Pick a 1-cocycle f. For any $\alpha\in L^\times$, put $\beta(\alpha):=\Sigma_{\tau\in G}f(\tau)\tau(\alpha)$. You can find α such that $\beta(\alpha)$ is nonzero. Then you can prove $f(\sigma)=\beta/\sigma(\beta),\forall\sigma\in G$. □

Theorem 3 still holds when L/K is an infinite Galois extension. (See Fact 1.)

When the extension L/K is cyclic with a generator σ, noting that a 1-cocycle f is determined by $\alpha=f(\sigma)$ ($f(\sigma^k)=\alpha\sigma(\alpha)\cdots\sigma^{k-1}(\alpha)$), we have Hilbert 90 (for the cyclic case):

Theorem 4. *Put $N:=N_{L/K}$. If $\alpha\in L^\times$ such that $N(\alpha)=1$, then there exists $\beta\in L^\times$ such that $\alpha=\sigma(\beta)/\beta$.*

Proof. Recall (or by the proof of the Theorem 3) that β should be defined as

$$\beta=\alpha+\sigma(\alpha)\alpha+\cdots+\sigma^{n-1}(\alpha)\cdots\sigma(\alpha)\alpha,$$

where $n=[L:K]$. □

Remark 4. Hilbert 90 is the main basis of Kummer theory. See the proof of the following proposition.

Proposition 3. Suppose L/K is a finite cyclic subextension of degree d of some abelian extension of exponent n. $K^\times$ contains all n^{th} roots of 1 (which corresponds to "$\mu_{\wp}\subseteq A_K$" in the abstract settings). Then, $L=K(\alpha)$ for some $\alpha\in L$ whose n^{th} power is in K.

Proof. Let ζ be the primitive n^{th} root of 1. Note $N_{L/K}(\zeta^{\frac{n}{d}})=(\zeta^{\frac{n}{d}})^d=1$, by Hilbert 90, we know $\zeta^{\frac{n}{d}}=\sigma(\alpha)/\alpha$, for some $\alpha\in L^\times$, where σ is a generator of $Gal(L/K)$. You can verify that $L=K(\alpha)$, completing the proof. □

There is also Hilbert 90 for infinite Galois extension, i.e., $H^1(Gal(L/K),L^\times)=0$ if L/K is (infinite) Galois. This results from the following FACT:

Fact 1. $H^1(G,A)=\varinjlim H^1(G/N,A^N)$, *where G is a profinite group, and N ranges over open normal subgroups of G.*

This fact is almost immediate from the definition of direct limit, noting that the maps in the directed system are inflation maps, and that two representatives have the same germ if and only if they finally agree in $H^1(G,A)$.

5. Suppose K is a field with characteristic p, n a positive integer coprime to p. Let μ_n denotes the group of n^{th} roots of 1 in the separable closure $\bar{K}$ of K. Then we have

$$H^1(G(\bar{K}/K),\mu_n)\simeq K^\times/(K^\times)^n.$$

Proof sketch : define the natural homomorphism from $K^\times$ to the homology group (NOT the group of cocycles), and then calculate the kernel.

1.4 Abstract Valuation Theory

In the abstract formulation, we start with a sujective homomorphism

$$d : G \longrightarrow \hat{\mathbb{Z}},$$

which mimics the homomorphism

$$Gal(\bar{k}/k) \longrightarrow Gal(k^{ur}/k) \longrightarrow \hat{\mathbb{Z}},$$

where k is a p-adic field. We denote by I the ker. of d, I_K the ker. of

$$d|_{G_K} : G_K \longrightarrow \hat{\mathbb{Z}}.$$

Here I_K is (and should be) called the inertia group over K. The notion of (abstract) max. unr. ext. $\tilde{K}$ of K can be drawn from I_K. We denote by d_K the isom.

$$G(\tilde{K}/K) \longrightarrow \hat{\mathbb{Z}},$$

by φ_K the Frobenius over K. With these notations, the terminology of the inertia degree and the ramification index are defined as in the concrete case.

2 Local Class Field Theory

In this section, K denotes a nonarchimedean local field. U_K Denotes the group of units in the valuation ring $\mathcal{O}_K$. The filtration $U_K^i := 1 + \pi^i \mathcal{O}_K$, $i \in \mathbb{Z}_{>0}$, where π denotes a uniformizer.

2.1 Artin Reciprocity

The local class field theory studies abelian extensions over local fields. With the artin reciprocity, we can describe the Galois groups of abelian extensions over K via arithmetic information of K. Suppose L/K is a finite Galois extension that is unramified. Then $G(L/K) \simeq G(l/k)$ is cyclic, where l, k denote the residue field of L, K respectively. Then the canonical generator $[x \mapsto x^{\#k}]$ is pulled back to the unique Frobenius element $Frob_{L/K} \in G(L/K)$. We can construct a homomorphism

$$\psi_{L/K} : K^\times \longrightarrow G(L/K)$$

sending the uniformizer π to $Frob_{L/K}$, the group of units to 1, inducing an isomorphism

$$K^\times / (\pi^{[L:K]\mathbb{Z}} \times U_K) \xrightarrow{\sim} G(L/K).$$

Note that π is also a uniformizer of L since L/K is unramified. We claim that

$$N_{L/K}(L^\times) = \pi^{[L:K]\mathbb{Z}} \times U_K.$$

Proof. Since l/k is a finite extension of finite fields, we know that $N_{l/k} : l^\times \longrightarrow k^\times$ is surjective. Since l/k is finite separable, we know that $Tr_{l/k} : l \longrightarrow k$ is nonzero and thus surjective. Therefore, The norm map $N_{L/K}$ is surjective from U_L/U_L^1 to U_K/U_K^1, surjective from U_L^i/U_L^{i+1} to U_K^i/U_K^{i+1}, $i \in \mathbb{Z}_{>0}$, by the surjectivity of $N_{l/k}, Tr_{l/k}$ respectively. Hence, for any $a \in U_K$, we can find $b_0, b_1, \ldots$ which are in $U_L, U_L^1, \ldots$ respectively, such that $aN_{L/K}(b_0 b_1 \cdots b_{m-1})^{-1} \in U_K^m$. Since the product $\prod_{m=1}^{\infty} b_m$ converges in U_L, this proves that $N_{L/K}(U_L) = U_K$. Therefore $N_{L/K}(L^\times) = N_{L/K}(\pi^{\mathbb{Z}} \times U_L) = \pi^{[L:K]\mathbb{Z}} \times U_K$, completing the proof of the claim. □

Therefore we obtain an isomorphism

$$\psi_{L/K} : K^\times / N_{L/K}(L^\times) \xrightarrow{\sim} G(L/K).$$

This is the local **artin map** that we shall introduce in a more general setting where the extensions L/K are finite abelian. This elementary proof of the artin reciprocity for finite unramified extension attributes to Xingfeng Lin. The local artin reciprocity states that *there is a unique homomorphism*

$$\psi_K : K^\times \longrightarrow Gal(K^{ab}/K)$$

such that for any finite abelian extension L/K, ψ_K induces a surjective homomorphism

$$\psi_{L/K} : K^\times \longrightarrow Gal(L/K)$$

whose kernel is the norm group $N_{L/K}(L^\times)$, and that if L/K is moreover unramified, $\psi_{L/K}$ sends uniformizers of K to $Frob_{L/K}$. A norm group $N(L^\times) \leq K^\times$ is open if and only if it is of finite index since $N(\pi_L^{\mathbb{Z}})$ is always open and of finite index in $\pi_K^{\mathbb{Z}}$ and $\mathcal{O}_K^\times$ is compact. With the artin reciprocity at hand, we can prove some basic properties of norm groups.

1. *Every norm group in $K^\times$ has finite index.*

   Proof. Suppose L is a finite abelian extension over K. Then $K^\times/N_{L/K}(L^\times) \simeq G(L/K)$, thus the norm group $N_{L/K}(L^\times)$ has finite index. □

2. *Every subgroup of $K^\times$ that contains a norm group is a norm group.*

   Proof. Suppose $N_{L/K}(L^\times) \leq H \leq K^\times$, where L/K is a finite abelian extension. Consider the map

   $$\psi_{L/K} : K^\times \longrightarrow G(L/K)$$

   and $\psi_{L/K}(H) \leq G(L/K)$. By Galois theory, $\psi_{L/K}(H) = Gal(L/L^{\psi_{L/K}(H)})$. Put $F = L^{\psi_{L/K}(H)}$, $res^L_F : G(L/K) \longrightarrow G(F/K)$, then $\psi_{F/K} = res^L_F \circ \psi_{L/K}$. Therefore

   $$H = \psi^{-1}_{L/K}(G(L/F)) = \psi^{-1}_{L/K}(res^L_F)^{-1}(1) = Ker(\psi_{F/K}) = N_{F/K}(F^\times),$$

   so that H is a norm group. □

One may ask whether any subgroup of $K^\times$ of finite index is open. If $char(K) = 0$, then this is true. We have the logarithm map from U^1_K to $\pi\mathcal{O}_K$, which is an isomorphism of topological groups. Then, by the decomposition

$$K^\times \simeq \mathbb{Z} \times k^\times \times (1 + \pi\mathcal{O}_K),$$

it suffices to show that any finite-index (additive) subgroup of $\mathcal{O}_K$ is open, which is trivial as an extension of $\mathbb{Z}_p$. If $char(K) > 0$, we know that $K \simeq F_q((t))$ for some prime power $q = p^k$, where F_q is the finite field of cardinality q. Then

$$K^\times \simeq \mathbb{Z} \times F_q^\times \times (1 + tF_q[[t]]).$$

Though the logarithm map is not well defined on U^1_K, it is well defined on U^m_K for large m, and we still have isomorphisms

$$\frac{1 + t^i F_q[[t]]}{1 + t^{i+1} F_q[[t]]} \simeq \frac{t^i F_q[[t]]}{t^{i+1} F_q[[t]]}$$

for $i \in \mathbb{Z}_{>0}$. To find a non-open finite-index subgroup of $K^\times$, it suffices to find such a subgroup of the (additive) group $F_q[[t]]$. For example, consider the linear functional

$$\begin{aligned} f : F_q[[t]] &\longrightarrow F_q \\ t^i &\longmapsto 1, \end{aligned}$$

$i \in \mathbb{Z}_{\geq 0}$. Then $Ker(f)$ is a subgroup not containing $t^j F_q[[t]]$ for any $j \in \mathbb{Z}_{\geq 0}$, thus not open.

To conclude the discussion, note that an open subgroup of $K^\times$ need not have finite index ($K^\times$ not compact, with a infinite discrete summand $\mathbb{Z}$). Among all finite-index subgroups of $K^\times$, those open ones are exactly all norm groups by the local existence theorem. (The **local existence** theorem states that *for every open and finite-index subgroup N of $K^\times$ there exists a unique finite abelian extension L/K satisfying $N = N_{L/K}(L^\times)$.*) Hence the set of norm groups in $K^\times$ forms a topological basis of neighborhoods of $1 \in K^\times$. (This follows from the fact that $\mathcal{O}^\times_K$ is a profinite group.) If K has characteristic 0, then any subgroup of finite index is a norm group by previous arguments.

2.2 Further discussion on K^{ab}

Suppose K is a nonarchimedean local field. For the purpose of describing K^{ab}/K, we assume the knowledge of profinite groups and profinite completion. (See Section 1 and Section 5.) We have an isomorphism of profinite groups

$$\hat{K^\times} \simeq Gal(K^{ab}/K),$$

where $\hat{K^\times}$ denotes the profinite completion of $K^\times$. The artin map ψ_K can be interpreted as the action of $K^\times$ on the maximal abelian extension of K. Since $K^\times = \pi^{\mathbb{Z}} \times \mathcal{O}_K^\times$, we would like to know the action of uniformizers and units in $K^\times$.

In fact, an element $a \in K^\times$ act trivially on the maximal unramified extension K^{unr} if and only if $a \in \mathcal{O}_K^\times$. An element $a \in K^\times$ acts trivially on K^{ab} if and only if $a = 1$ (ψ_K is injective), since $\{N(L^\times)\}_{L/K\ finite\ abelian}$ forms a basis of neighborhoods of 1. Therefore we have a commutative diagram of two short exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & K^\times & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow \sim & & \downarrow \psi_K & & \downarrow & & \\ 1 & \longrightarrow & G(K^{ab}/K^{unr}) & \longrightarrow & G(K^{ab}/K) & \longrightarrow & G(K^{unr}/K) & \longrightarrow & 1 \end{array}.$$

This reveals the action of $K^\times$ on the unramified part K^{unr}.

To discover the action on the (totally) ramified part, note that π acts trivially on a finite abelian extension L/K if and only if $\pi \in N(L^\times)$, if and only if the inertia degree $f(L/K) = 1$. Put

$$K_\pi = (K^{ab})^{\psi_K(\pi)}.$$

Then K_π is the compositum of all totally ramified finite subextensions of K^{ab}/K, and $K_\pi \cap K^{unr} = K$. So, the only thing that remains unknown from the superficial statements of the artin reciprocity theorem is the action of $\mathcal{O}_K^\times$ on K_π. This hides in the construction of the artin map ψ_K, and is exactly where the Lubin-Tate theory is needed.

We will see in Section 4 the formulation of K_π as a compositum L_π of a tower of finite extensions $L_n, n \in \mathbb{Z}_{>0}$, by adjoining roots of some Lubin-Tate polynomial $e^{\circ n}$, and prove that they are totally ramified, much like cyclotomic extensions over $\mathbb{Q}_p$, for example. Using Lubin-Tate theory, we would be able to define the action of $a = u\pi^{v(a)} \in K^\times$ on L_π as the Lubin-Tate action $[u]_e$ (or $[u^{-1}]_e$), where e is any Lubin-Tate series for the uniformizer π of K, so that π acts trivially on L_π. Put this action in the construction of ψ_K (in a cohomological way), completing the local artin reciprocity.

From Lubin-Tate theory, we are able to see that

$$G(L_\pi/K) \simeq \varprojlim_n G(L_n/K) \simeq \varprojlim_n (\mathcal{O}_K/\pi^n)^\times \simeq \mathcal{O}_K^\times,$$

and

$$L_\pi \subseteq K_\pi, \quad K^{unr} = (K^{ab})^{\psi_K(\mathcal{O}_K^\times)},$$

and therefore $K^{ab} = K_\pi K^{unr}$. Since every totally ramified finite extension can be obtained by adjoining roots of a Lubin-Tate polynomial (or an Eisenstein polynomial), we know

that $K_\pi = L_\pi$. Moreover, by taking profinite completion, we have the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & \hat{K}^\times & \longrightarrow & \hat{\mathbb{Z}} & \longrightarrow & 0 \\ & & \downarrow \sim & & \downarrow \hat{\psi}_K & & \downarrow \sim & & \\ 1 & \longrightarrow & G(K^{ab}/K^{unr}) & \longrightarrow & G(K^{ab}/K) & \longrightarrow & G(K^{unr}/K) & \longrightarrow & 1 \end{array} .$$

Since the exact sequence on the first row splits, which says the decomposition on the arithmetic side

$$\hat{K}^\times \simeq \mathcal{O}_K^\times \times \hat{\mathbb{Z}},$$

we have the corresponding decomposition on the Galois side

$$G(K^{ab}/K) \simeq G(K_\pi/K) \times G(K^{unr}/K).$$

This absolutely clarifies the structure of abelian extensions over nonarchimedean local fields.

3 Main Theorems of Global Class Field Theory

Suppose K is a number field.(We can deal with all global fields, but number fields are satisfying for now.)

3.1 Ray Class Fields

The motivation of ray class fields is to study abelian extensions. We wish to prove that every finite abelian extension must be contained in a(the) ray class field for some modulus, as generalization of the Kronecker-Weber theorem.

Given a modulus $\mathfrak{m}$, We have the ray group $\mathscr{R}_K^{\mathfrak{m}}$ and the ray class group $Cl_K^{\mathfrak{m}}$. For an abelian extension L/K such that all primes of K ramifying in L divides $\mathfrak{m}$, we have the artin map $\psi_{L/K}^{\mathfrak{m}} : \mathscr{I}_K^{\mathfrak{m}} \longrightarrow Gal(L/K)$ sending primes not dividing $\mathfrak{m}$ to the corresponding Frobenius.

Definition 1. A ray class field for $\mathfrak{m}$ is a finite abelian extension of K such that the following holds:

1. L/K is unr. at all places not in the support of $\mathfrak{m}$;
2. $Ker(\psi_{L/K}^{\mathfrak{m}}) = \mathscr{R}_K^{\mathfrak{m}}$.

Remark 5. The existence of ray class fields is difficult to prove. Assuming existence, we will prove the uniqueness shortly after. We will also prove that artin maps are surjective. With this fact, by looking at the artin map for the ray class field $K(\mathfrak{m})$ for $\mathfrak{m}$, we can build a 1-1 correspondence between $\{$subextensions of $K(\mathfrak{m})/K\}$ and $\{$quotients of $Cl_k^{\mathfrak{m}}\}$(or "congruence subgroups for $\mathfrak{m}$", which will be defined later).

Here are two examples of ray class fields over $\mathbb{Q}$.
Take $\mathfrak{m} = (5)$. The corresponding ray class field is $\mathbb{Q}(\sqrt{5})$;
Take $\mathfrak{m} = (5)\infty$. The corresponding ray class field is $\mathbb{Q}(\zeta_5)$.
As we care about the class number of a number field, we care about the ray class number of a modulus $\mathfrak{m}$ of K, which refers to $|Cl_K^{\mathfrak{m}}|$. There is a way to compute the ray class number by applying the Snake Lemma to the following commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^{\mathfrak{m},1} & \xrightarrow{f} & K^{\mathfrak{m}} & \longrightarrow & K^{\mathfrak{m}}/K^{\mathfrak{m},1} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle g\circ f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle \pi} & & \\ 1 & \longrightarrow & \mathscr{I}_K^{\mathfrak{m}} & \xrightarrow{\sim} & \mathscr{I}_K^{\mathfrak{m}} & \longrightarrow & 1 & \longrightarrow & 1 \end{array},$$

where

$$K^{\mathfrak{m}} := \{\alpha \in K : v_{\mathfrak{p}}(\alpha) = 0, \forall \mathfrak{p} | \mathfrak{m}_0\},$$

$$K^{\mathfrak{m},1} := \{\alpha \in K : v_{\mathfrak{p}}(\alpha) \geq m(\mathfrak{p})), \forall \mathfrak{p} | \mathfrak{m}_0, \alpha_v > 0, \forall v \in \mathfrak{m}_\infty\},$$

and the maps in the diagram are naturally defined.

Now we use the Polar Density $\rho(S)$ of a set S of primes in K(defined using the Dedekind zeta function $\zeta_{K,S}$) to prove the surjectivity of the artin maps and the uniqueness of the ray class field.

Proposition 4. Suppose L/K is a finite Galois extension of number fields. The set $S := Spl(L/K)$ of all primes in K that splits in L has polar density $\frac{1}{[L:K]}$.

Proof. By definition of the polar density, we consider the Dedekind zeta functions of L, K. Put $T :=$\{primes of L lying over some prime in S\}, easy to prove $\zeta_{L,T} = \zeta_{K,S}^n$. It suffices to show T has polar density 1. Note that $P_L - T \subseteq$\{primes of L ramified over K\}$\cup$\{primes of L with degree$\geq$2 over K\}. The former set is finite, and the latter is contained in \{primes of L with degree$\geq$2 over $\mathbb{Q}$\}, which has polar density 0. □

For any finite extensionL/K, consider the Galois closure M/K of L/K. Then we have $\rho(Spl(L/K)) = \rho(Spl(M/K)) = 1/[M:K]$. With this conclusion, we can use $Spl(L), Spl(M)$ to illustrate the degree of, say, LM, L over K, and then the containment between L, M would be clear. (Here I point out the main technique!) Now we can prove our first two main results.

Theorem 5. *Suppose $\mathfrak{m}$ is a modulus of K, L/K a finite abelian extension where all primes not in the support of $\mathfrak{m}$ are unramified. Then, the artin map $\psi_{L/K}^{\mathfrak{m}}$ is surjective.*

Proof. Let F be the fixed field of $Im(\psi_{L/K}^{\mathfrak{m}})$. It suffices to show $\rho(Spl(F)) = 1$, which is clear from the definition of F: F is fixed by almost all Frobenius(of unramified primes), and thus almost all primes split completely in F. □

Theorem 6. *For any modulus $\mathfrak{m}$ of K, there exists at most one ray class field for $\mathfrak{m}$.*

Proof. Suppose L, L' are ray class fields for $\mathfrak{m}$. Then their artin maps have the same kernel, thus $Spl(L) \sim Spl(L')$, thus $L = L'$. □

3.2 Congruence Subgroups and Ray Class Characters

In preparation for statements of the main theorems of GCFT, we introduce the notion of congruence subgroups and ray class characters, and we pay attention, in particular, to whether their primitivity and conductor coincide. This part of preparation involves numerous details.

Definition 2. A congruence subgroup of mod. $\mathfrak{m}$ is a subgroup of the ideal group of $\mathfrak{m}$ containing the ray group of $\mathfrak{m}$.

Motivation of studying congr. subgroups and some remarks: to realize the Gal. group of an abel ext. as a quot. of some ray class group, we need the kernel of the Artin map to contain the ray group, i.e. we need to find a modulus $\mathfrak{m}$ of K such that the ker. of the Artin map is a congruence subgroup.

For some Artin maps(with modulus $\mathfrak{m}$), the ker. may not be a congr. subgroup of $\mathfrak{m}$. For example, Consider K=$\mathbb{Q}$, L the splitting field of $x^3 - 3x - 1$. Let $\mathfrak{m} = (3)$, whose ray class field is $\mathbb{Q}$, not containing L. Thus, by looking at $Spl(L/\mathbb{Q})$, we see that $ker(\psi_{L/K}^{\mathfrak{m}})$ does NOT contain the ray group of $\mathfrak{m}$, which is $ker(\psi_{K/K}^{\mathfrak{m}})$, i.e. not a congruence subgroup of $\mathfrak{m}$.

There is a problem to think of: Is every congr. subgroup the kernel of some Artin map? The answer is "roughly yes", known as the EXISTENCE THEOREM.

Note that for moduli $\mathfrak{m}, \mathfrak{n}$, there are some obvious relations between the corresponding artin maps and ray groups. For example, if $\mathfrak{m}_0 = \mathfrak{n}_0$, then the corresponding artin maps are the same, but the ray groups may differ; if $\mathfrak{m}$ divides $\mathfrak{n}$, then the ray group of $\mathfrak{m}$ contains that of $\mathfrak{n}$.

Thus, we define an equiv. relation among congr. subgroups for various $\mathfrak{m}$.

Definition 3. Suppose C_1, C_2 are congr. subgroups of moduli $\mathfrak{m}_1, \mathfrak{m}_2$ resp.. Say $C_1 \sim C_2$ if they have the same part in the intersection of ideal groups of $\mathfrak{m}_1, \mathfrak{m}_2$.

It turns out (as many parts of number theory would) that if C_1 and C_2 are equiv., then there is a congr. subgroup C_0 of modulus $gcd(\mathfrak{m}_1, \mathfrak{m}_2)$ that is equiv. to $C_1 \sim C_2$. It follows that for any congr. subgroup C, say of mod. $\mathfrak{m}$, there is a unique minimal mod. $\mathfrak{c}$ admitting a congr. subgroup C' equiv. to C. We call $\mathfrak{c}$ the **conductor** of C, and call a congr. subgroup **primitive** if it is a congr. subgroup of its conductor.

Another problem to think of: Given a modulus m, when is $\mathfrak{m}$ a conductor? It is fairly easy to prove the following proposition.

Proposition 5. $\mathfrak{m}$ is a conductor if and only if $\mathfrak{m}$ is the conductor of the ray group of $\mathfrak{m}$.

Here is an example of a mod. $\mathfrak{m}$ NOT a conductor: $K = \mathbb{Q}, \mathfrak{m} = (2)$. Then the conductor of the ray group of $\mathfrak{m}$ is (1), not (2). Thus (2) is not a conductor of any congr. subgroup.

Now the congr. subgroups and relations among them are well understood, we study ray class characters to dig into the arithmetic properties of the ray class groups. (As we study Dirichlet characters to explore the arithmetic properties of $\mathbb{Z}$ modulo a positive integer.)

Definition 4. A ray class character of modulus $\mathfrak{m}$ is a group homomorphism from the ray class group of $\mathfrak{m}$ to $\mathbb{C}^*$ with finite image, which can always be extended by 0 to a (nonzero) character of the ideal group of $\mathfrak{m}$, whose kernel contains the ray group of $\mathfrak{m}$.

For $\mathfrak{m}|\mathfrak{n}$, we have a natural homom. from the ray class group of $\mathfrak{n}$ to the ray class group of $\mathfrak{m}$, which leads to ray class chars. of $\mathfrak{m}$ inducing ray class chars. of $\mathfrak{n}$. Given a ray class char. χ, one can find a minimal modulus $\mathfrak{c}$ such that there is a unique ray class char. of modulus $\mathfrak{c}$ inducing χ. This $\mathfrak{c}$ is called the **conductor** of χ, and χ is called **primitive** if its modulus is its conductor. (Intuitively you may view chars. induced from a same primitive char. as one char., since they do not differ after extended by 0 to chars. of the ideal group of K.)

Two notions of "conductor" for χ and $Ker(\chi)$ resp., both defined to be minimal in the natural inducing order, coincide. The proof is natural and direct if you follow the definition of the inducing process.

Proposition 6. Suppose χ is a ray class character of modulus $\mathfrak{m}$, then the conductor $\mathfrak{c}(\chi)$ of χ equals to the conductor $\mathfrak{c}(Ker(\chi))$ of $Ker(\chi)$.

Remark 6. Alternatively, you can use Proposition 5 as the definition of the conductor of a ray class character χ, and verify that it is the minimal modulus with a (unique) ray class character inducing χ.

Like Dirichlet characters, each ray class character has an associated L-function.

Definition 5. The Weber L-function $L(s,\chi)$ of a ray class character χ is a complex-valued function defined as

$$L(s,\chi) := \prod_{\mathfrak{p}} (1 - \chi(\mathfrak{p}) N(\mathfrak{p})^{-s})^{-1}.$$

$L(s,\chi)$ is holomorphic on $Re(s) > 1$, by the absolute and uniform convergence on $Re(s) \geq 1 + \varepsilon, \forall \varepsilon > 0$.

Similar to the Dedekind L-function of a number field. We have the follwing extension of the Weber L-functions.

Proposition 7. Suppose χ is a ray class character of modulus $\mathfrak{m}$ of a number field K, with $[K : \mathbb{Q}] = n$. Then $L(s,\chi)$ can be extended to a meromorphic function on $Re(s) > 1 - 1/n$, with at most a simple pole at $s = 1$. If χ is not principal (i.e. not induced by the trivial character $\mathbf{1}$), then $L(s,\chi)$ is holomorphic on $Re(s) > 1 - 1/n$.

Recall that one can prove the non-vanishing property of the Dirichlet L-function of non-principal Dirichlet characters of modulus m at $s=1$, by writing the Dedekind zeta function of $Q(\zeta_m)$ (note $\left(Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = (\mathbb{Z}/m)^\times\right)$) as the product of Dirichlet L-functions of Dirichlet characters of modulus m. Similarly, we can prove that $L(1,\chi) \neq 0$ if the ray class character χ is non-principal. However, the proof of this non-vanishing property shall use the existence of the ray class fields.

Without assuming the existence of ray class fields, we can prove a weaker result.

Proposition 8. Suppose C is a congruence subgroup, put $d(C) := d(\{\mathfrak{p} \in C\})$. Then there exist at most one non-vanishing ray class character whose kernel containing C such that $L(1,\chi) = 0$. and

$$d(C) = \begin{cases} 1/n, & L(1,\chi) \neq 0, \forall non-pricinpal \chi \in X(C) \\ 0, & otherwise \end{cases}$$

Here $X(C)$ denotes the set of primitive ray class characters whose kernel contains C (say of modulus $\mathfrak{m}$). This is a subgroup of $X(\mathfrak{m})$, the proof of which is interesting: one needs to compare the conductor $\mathfrak{c}$ of a character whose ker. containing C with the modulus $gcd(\mathfrak{m},\mathfrak{c})$.

Proposition 8 finds its origin in Sutherland [3], and is revised by Xingfeng Lin. The proof of Proposition 8 use the help of the indicator in character theory and is based on the analytic property of Weber L-functions desribed in Proposition 7.

In order to state the (ideal-theoretic version of) main theorems of GCFT, we need to define another notion of conductors for an abelian extension.

Definition 6. Suppose L/K is a finite abelian extension of local fields. Define the (local) conductor $\mathfrak{c}(L/K)$ of L/K to be

$$\mathfrak{c}(L/K) = \begin{cases} 1, & L = \mathbb{C}, K = \mathbb{R} \\ 0, & L = K, archimedean \\ min\{n : 1 + \mathfrak{p}^n \subseteq N(L^\times)\}, & nonarchimedean \end{cases}$$

The existence of $\mathfrak{c}(L/K)$ in the nonarchimedean case is based on the fact that $N(L^\times)$ is open. It is natural and almost immediate to prove that this fact is equivalent to the fact that $N(L^\times)$ has finite index in $K^\times$, and to the fact that $N(L^\times)$ contains a neighborhood of 1.

Definition 7. Suppose L/K is a finite abelian extension of global fields. Define the (global) conductor $\mathfrak{c}(L/K)$ to be the modulus

$$\mathfrak{m} : M_K \longrightarrow \mathbb{Z}$$

by sending the place v to $\mathfrak{c}(L_w/K_v)$, where w is any place of L lying over v (note that L/K is Galois).

By Hilbert 90, we can prove that for global L/K, the support of $\mathfrak{c}(L/K)$ is precisely the set of ramified primes in K. Moreover, we have the following proposition.

Proposition 9. Suppose L/K is a finite abelian extension of global fields or local fields. Then

$$v_{\mathfrak{p}}(\mathfrak{c}(L/K)) \begin{cases} = 0, & \mathfrak{p}\, unramified \\ = 1, & \mathfrak{p}\, tamely\, ramified \\ \geq 2, & \mathfrak{p}\, wildly\, ramified \end{cases}$$

Now we state the main theorems of GCFT for number fields. Suppose L/K is a finite abelian extension of number fields. Then

1. For any modulus $\mathfrak{m}$ of K, the ray class field $K(\mathfrak{m})$ exists. (EXISTENCE)

2. If L/K is a finite abelian extension, $\mathfrak{m}$ is a modulus of K, then $L \subseteq K(\mathfrak{m})$ if and only if $\mathfrak{c}(L/K)|\mathfrak{m}$. (COMPLETENESS)

3. Suppose L/K is a finite abelian extension in $K(\mathfrak{m})$. Then $Ker\psi^{\mathfrak{m}}_{L/K}$ (which clearly contains $\mathcal{R}^{\mathfrak{m}}_K$) is the **norm group** (Takagi group) $T^{\mathfrak{m}}_{L/K} := \mathcal{R}^{\mathfrak{m}}_K N_{L/K}(\mathcal{J}^{\mathfrak{m}}_L)$, where $\mathcal{J}^{\mathfrak{m}}_L$ is generated by primes lying over those primes of K not in the support of $\mathfrak{m}$. Moreover, we have a canonical isomorphism

$$\mathcal{J}^{\mathfrak{m}}_K / T^{\mathfrak{m}}_{L/K} \longrightarrow Gal(L/K).$$

   This enables us to build a 1-1 correspondence between subextensions of a ray class field to norm groups of the modulus (or quotients of the ray class group of the modulus). (ARTIN RECIPROCITY)

In particular, consider the ray class field H of the trivial modulus. By COMPLETENESS, we know that the conductor of $H = K((1))$ must be trivial, and it is the largest among all finite unramified abelian extensions.

Definition 8. Suppose K is a number field, we call the compositum H of all finite unramified abelian extensions of K the Hilbert class field of K.

Thus we have shown that Hilbert class field H of K is finite over K, and equals to $K((1))$. By ARTIN RECIPROCITY, we know $[H : K] = h_K$, the class number of K.

Some problems concerning Hilbert extensions are in order. One can build a tower of Hilbert class fields starting from some number field K and ask questions like:

1. Will the tower be finite?

2. Taking compositum of the ascending sequence of Hilbert class fields, it must be solvable, but is it abelian?

3. Such towers are unramified and solvable. Is there an infinite unramified extension that is not solvable?

These questions already have considerably satisfying answers.

4 Lubin-Tate Theory

One of the main purposes of Lubin-Tate theory is to construct cyclotomic theory on any local field.

4.1 Formal Groups and Lubin-Tate Extensions

Suppose K is a local field, π a uniformizer of K. With the notion of formal groups, we can define the notion of Lubin-Tate module over $\mathcal{O}_K$ for π. Use a crucial technical property of the existence and uniqueness of 'formal power series satisfying some requirements' (concerning Lubin-Tate series), we can determine all Lubin-Tate modules.

Theorem 7. *The Lubin-Tate modules for π are precisely the series $F_e(X,Y)$, with the formal $\mathcal{O}_K$-module structure given by*

$$\mathcal{O}_K \longrightarrow End_{\mathcal{O}_K}(F_e),\ a \longmapsto [a]_e(X),$$

where F_e is defined to be the unique power series in $\mathcal{O}_K[[X,Y]]$ satisfying

$$F_e(X,Y) \equiv X+Y \ mod\ deg\ 2$$

$$e(F_e(X,Y)) = F_e(e(X),e(Y)),$$

$[a]_e$ defined to be the unique power series in $\mathcal{O}_K[[X]]$ satisfying

$$[a]_e(X) \equiv aX \ mod\ deg\ 2$$

$$e \circ [a]_e = [a]_e \circ e.$$

The proof of this result is an easy application of the crucial technical property mentioned above (especially the uniqueness argument).

The Lubin-Tate theory furnishes a generalization of the notion of p^n-th roots of unity, and provide an explicit version of the local reciprocity law in the corresponding extensions.

Our first goal would be to define 'Lubin-Tate Extensions', the analogue of cyclotomic extensions over an arbitrary local field K. To do this, we use the formal Lubin-Tate module to define an explicit module, where we shall find the elements that are expected to be involved in the Lubin-Tate extensions.

Definition 9. Suppose $\overline{K}$ is an algebraic closure of K, with the unique prime ideal $\overline{\mathcal{P}}$. Suppose F is a Lubin-Tate module for a prime element π of $\mathcal{O}_K$. Then, $\overline{\mathcal{P}}$ becomes an $\mathcal{O}_K$-module under the addition given by F and the ring action given by $[\cdot]_F$, denoted by $\overline{\mathcal{P}_F}$.

In the definition above, the Lubin-Tate module F can be replaced by any formal $\mathcal{O}_K$-module, but we need F to be Lubin-Tate in the following definition. We define the analogue of 'p^n-th roots of 1'.

Definition 10. The group $F(n)$ of π^n-division points is defined to be

$$F(n) := \{\lambda \in \overline{\mathcal{P}_F} : [\pi^n]_F(\lambda) = 0\}$$

Here you may wish to verify the usual 0 in $\overline{\mathfrak{p}}$ is the zero under $+_F$, which follows from the fact that a formal group F must be of the form $F(X,Y) = X + Y + XYG(X,Y)$, for some $G \in \mathcal{O}_K[[X,Y]]$.

One can verify that $F(n)$ is really a subgroup of $\overline{\mathfrak{p}_F}$ by definition. Moreover, $F(n)$ is an $\mathcal{O}_K/\pi^n$-module.

Proposition 10. *$F(n)$ is a free $\mathcal{O}_K/\pi^n$-module of rank 1.*

Proof. The proof is based of the following fact:

Fact 2. *With $F_e, F_{\overline{e}}$ defined in Theorem 7 respectively for any Lubin-Tate series $e, \overline{e}$ for the prime element π of K, for $a \in \mathcal{O}_K$, let $[a]_{e,\overline{e}} \in \mathcal{O}_K$ be the unique power series satisfying*

$$[a]_{e,\overline{e}}(X) \equiv aX \ mod \ deg \ 2$$

$$[a]_{e,\overline{e}} \circ \overline{e} = e \circ [a]_{e,\overline{e}}.$$

Then $[a]_{e,\overline{e}}$ is a homomorphism from $F_{\overline{e}}$ to F_e, which is a isomorphism if $a \in \mathcal{O}_K^\times$.

We can verify that if two Lubin-Tate modules F, G are isomorphic (say via $f \in \mathcal{O}_K[[X]]$), then $F(n), G(n)$ are isomorphic via f. Fact 2 shows that all F_e are isomorphic. Thus, it suffices to show that $F_e(n)$ is a free $\mathcal{O}_K$-module of rank 1, where $e(X) = X^q + \pi X$, $q = |\mathcal{O}_K/\pi|$. Then by checking that $e^{\circ n}$ is a separable polynomial, with all roots in $\overline{\mathfrak{p}_F}$, we get that $F_e(n)$ consists of exactly q^n zeroes of $e^{\circ n}$. Now pick $\lambda_n \in F_e(n) - F_e(n-1)$ (which turns out later to be the analogue of primitive p^n-th root of 1), we can define an isomorphism from $\mathcal{O}_K/\pi^n$ to $F_e(n)$ by letting every $a \in \mathcal{O}_K$ act on λ_n. The proof is complete. □

Now we can define the Lubin-Tate extensions.

Definition 11. Define the field L_n of π^n-division points to be $K(F(n))$. By checking that $F(n) \subseteq F(n+1), \forall n \in \mathbb{Z}_{>0}$, we obtain a tower

$$L_1 \subseteq L_2 \subseteq \cdots \subseteq L_\pi := \cup_n L_n$$

of **Lubin-Tate extensions**.

It should be mentioned that L_n is independent of the Lubin-Tate module F. (Any two Lubin-Tate modules F, G for π are isomorphic, say via an invertible power series f, then f would be an isomorphism between $F(n), G(n)$. Note that f has coefficients in $\mathcal{O}_K$, fixed by $Gal(L_n/K)$.)

We can see that cyclotomic extensions are really a special case of Lubin-Tate extensions from the following example:

Example 2. Let $K = \mathbb{Q}_p$, F the Lubin-Tate module $\mathbb{G}_m$. Then the Lubin-Tate extension $K(F(n)) = \mathbb{Q}_p(\zeta_{p^n})$.

A key feature of cyclotomic extensions by adjoining p^n-th roots is their Galois groups, which are isomorphic to the group of units of $\mathbb{Z}_p/p^n$. Another key feature is that they are totally ramified. For Lubin-Tate extensions, we have the following similar result:

Theorem 8. *L_n/K (defined as in Definition 11) is a totally ramified abelian extension of degree $q^{n-1}(q-1)$ with Galois group*

$$Gal(L_n/K) = Aut_{\mathcal{O}_K}(F(n)).$$

Furthermore, Let $F = F_e$, where e is a Lubin-Tate polynomial for π. Pick $\lambda_n \in F(n) - F(n-1)$. Then $L_n = K(\lambda_n)$ and the minimal polynomial of λ_n over K is

$$\phi_n(X) := \frac{e^{\circ n}(X)}{e^{\circ(n-1)}(X)} = X^{q^{n-1}(q-1)} + \cdots + \pi \in \mathcal{O}_K[X].$$

Remark 7. The first statement of Theorem 8 implies that every $\sigma \in G(L_n/K)$ is a Lubin-Tate action of a unit in $\mathcal{O}_K$. (By Proposition 10, $Aut_{\mathcal{O}_K}(F(n))$ is isomorphic to the group of units in $End_{\mathcal{O}_K}(\mathcal{O}_K/\pi^n) = \mathcal{O}_K/\pi^n$.) The second statement says that elements in $F(n) - F(n-1)$ are analogue of the primitive p^n-th roots of 1 over $\mathbb{Q}_p$.

The proof of Theorem 8 is easy if you recall that forming a totally ramified extension over a local field is equivalent to adjoining a root of a Eisenstein polynomial.

Remark 8. Let me put some results we have not proved yet to help readers (hopefully) understand the Lubin-Tate theory. (We did this in Subsection 2 of Section 2.) By the local artin reciprocity map, we obtain actions of $K^\times$ on the maximal abelian extension $K^{ab} = K^{unr}L_\pi$. Here L_π can be viewed as the totally ramified part of the maximal abelian extension, built by adjoining roots of some Lubin-Tate polynomials, and is proved by Lubin-Tate theory to be independent of the Lubin-Tate polynomials chosen (thus depending only on π). Then the (Artin) action behaves as the following:

1. The action of units is trivial on the unramified part: by definition of the local artin map, uniformizers are sent to Frobs., and units are sent into the inertia subgroup of $G(L/K)$, which is trivial if L/K is unramified.

2. The action of π is trivial on the totally ramified part: Fix a Lubin-Tate module F for π. The (Artin) action of $a = u\pi^{v_\pi(a)}$ is determined by the Lubin-Tate action of u^{-1} on $F(n)$.

5 Cohomology

5.1 Profinite Groups

Definition 12. A profinite group is defined to be an inverse limit of finite groups, given the product topology, or equivalently, a compact totally disconnected topological group. For any topological group G, we define the profinite completion of G to be $\varprojlim_N G/N$, where N runs over all open normal subgroups of finite index. For any group G, by giving it the profinite topology (with topological bases cosets of subgroups of finite index), we define the separated completion of G to be $\varprojlim_N G/N$, where N runs over all normal subgroups of finite index.

One can verify that, for a profinite group G, G is isomorphic to its separated completion $\hat{G}^{sep}$ if and only if every subgroup of G of finite index is open, and that any homomorphism $G \longrightarrow H$ of profinite groups factors through the natural inclusion map $G \longrightarrow \hat{G}^{sep}$. The second property is referred to as the universal property of separated completion.

As an application in number theory, Recall the local artin map ψ_K for a nonarchimedean local field K, which induces isomorphisms

$$\psi_{L/K} : K^\times/N(L^\times) \xrightarrow{\sim} G(L/K)$$

for finite abelian extensions L/K. Let $\hat{K^\times}$ denote the profinite completion of $K^\times$. By local existence theorem we have

$$\hat{K^\times} \simeq \varprojlim_L (K^\times/N(L^\times)),$$

where L ranges over all finite abelian extensions of K. Therefore, after taking profinite completions, the artin map ψ_K becomes an isomorphism

$$\hat{\psi_K} : \hat{K^\times} \xrightarrow{\sim} G(K^{ab}/K).$$

Here are examples of profinite groups:

Example 3. 1. A compact analytic group G over $\mathbb{Q}_p$ is a profinite group. First look at the following argument:

Suppose U is an open neighborhood of 1 homeomorphic to an open subset V of $\mathbb{Q}_p^n$ (say via a homeomorphism ϕ), where n is the dimension of G as a manifold. By shifting V, we can assume $0 \in V$ and $\phi(1) = 0$. Pick an open subgroup G_0 contained in V. Pulling G_0 back on G, we obtain an open profinite subgroup G_1 of G. Cosets of G_1 cover G disjointly, forcing G to be totally disconnected.

This argument is FALSE, because nothing ensures that $\phi^{-1}(G_0)$ is still a group (ϕ not compatible with group structure). Here is a true argument:

We claim that a p-adic manifold M is always totally disconnected. In fact, for any two distinct points $x, y \in M$, there are disjoint open neighborhoods U, V of x, y respectively, with U, V homeomorphic to some open subset of $\mathbb{Q}_p^n$. Thus there is a compact open neighborhood K of x contained in U. Since M is Hausdorff (like any manifold), K must be closed in M. Therefore we have found a closed and open neighborhood of x not containing y.

2. If M is a torsion abelian group, its Pontryagin dual $M^* := Hom(M, \mathbb{Q}/\mathbb{Z})$ is a profinite group, given the weak* topology. (The weak* topology is the same as the restriction of product topology.)

   Furthermore, by Pontryagin duality theorem, we obtain an anti-equivalence between the category of torsion abelian groups and the category of abelian profinite groups. (Noting that a profinite group G is compact, one can check that G^* is indeed torsion.)

Proposition 11. Every closed subgroup H of a profinite group G is profinite. Moreover, the homogeneous space G/H is compact and totally disconnected.

Proof. The first statement is trivial. For the second statement, G/H is clearly compact. It suffices to show totally disconnectedness. For any $xH \neq H$, there is an open and closed set $U \subseteq G$ such that $H \subseteq U, xH \subseteq G - U$, for H being compact. We claim that H is contained in some open subgroup $H' \subseteq U$. Thus, H'/H is an open and closed subset of G/H such that $H \in H'/H, xH \in G/H - H'/H$. □

Thus, if H is a closed normal subgroup of G, we obtained a natural projection of profinite groups, forming a bundle over a profinite group. The following proposition ensures the existence of continuous sections of profinite bundles.

Proposition 12. If $K \subseteq H$ are two closed subgroups of the profinite group G, there exists a continuous section $s : G/H \longrightarrow G/K$.

Proof. For the first step we prove the case where K is open in H. Since K has finite index in H, one can find an open normal subgroup U of G such that $U \cap H \subseteq K$, using the fact that open subgroups form a base at 1. This leads to a injective map (say ϕ) from UK/K to G/H, resulting a continuous section (on an open subset of G/H, noting that projections of topological groups are open maps) backwards. Since U is a subgroup of G, we can extend this section to G/H by putting the same map on cosets of U.

For the general case, we may assume $K = 1$. Put $\Sigma := \{(S, s) : S$ a closed subgroup of H, $s : G/H \longrightarrow G/S$ a continuous section$\}$, which is nonempty since $(H, id) \in \Sigma$, equipped with the natural order defined by containment of subgroups and pull back of sections. For a chain $\{(S_i, s_i)\}$ in Σ, it is easy to prove $(\cap S_i, \prod s_i)$ is an upper bound. Thus, by Zorn's lemma, one obtains a maximal element (S, s) in Σ. If $S \neq 1$, then one can find an nontrivial open subgroup S' of S. By our first step, there exists a continuous section from G/S to G/S', making S', along with a section, a larger element than (S, s). Therefore, $S = 1$, completing the proof. □

For a profinite group G and its closed subgroups, we can define profinite index by taking the least common multiple of finite indices in finite quotients of G. The usual properties of indices still hold. In addition, it is almost trivial to prove:

Proposition 13. Suppose H_i are closed subgroups of G, $H := \cap H_i$. Then we have $(G : H) = lcm(G : H_i)$.

Proof. Write down the definitions, and switch the lcm. over i and normal open subgroups of G. Note that, for a closed subgroup K of G, open subgroups of G intersecting K are cofinal with all open subgroups of K. □

Here we state a well-known result (have not been proved in this note yet) to further motivate our study of profinite groups. Every profinite group is isomorphic to the Galois

group $Gal(L/K)$ of some Galois extension L over K, given the Krull topology. Consider the maximal cyclotomic extension $L = \cup_n \mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$. We have

$$G(L/\mathbb{Q}) = \varprojlim (\mathbb{Z}/n)^\times = \hat{\mathbb{Z}}^\times.$$

Calculated another way, we note that

$$G(L/\mathbb{Q}) = \varprojlim (\mathbb{Z}/n)^\times = \prod_p \mathbb{Z}_p \times \prod_p \mathbb{Z}/(p-1) = \hat{\mathbb{Z}} \times \prod_p \mathbb{Z}/(p-1).$$

Here $\mathbb{Z}_p$ is a **pro-p-group**, a projective limit of p-groups. Thus, some quotient of $G(L/\mathbb{Q})$ is a pro-p-group, i.e. some cyclotomic extension over $\mathbb{Q}$ is a pro-p-group.

Let $L_p := \cup_n \mathbb{Q}(\zeta_{p^n})$ be the maximal p-cyclotomic extension over $\mathbb{Q}$. Then,

$$G(L_p/\mathbb{Q}) = \varprojlim (\mathbb{Z}/p^n)^\times = \mathbb{Z}_p^\times = \mathbb{Z}_p \times \mathbb{Z}/(p-1),$$

if p is odd. If $p = 2$, then

$$G(L_2/\mathbb{Q}) = \mathbb{Z}_2^\times = \mathbb{Z}_2 \times \mathbb{Z}/2.$$

Note that $\mathbb{Z}_p$ is the (obviously unique) **Sylow p-subgroup** (a pro-p-subgroup with index coprime to p) of $\hat{\mathbb{Z}}$. We have established the rough insight that $L_p/\mathbb{Q}$ is the p-component, whatever this means, of $L/\mathbb{Q}$ both in the field extension sense and in the group theoretical sense. This observation is given by Xingfeng Lin.

For a profinite group G, the existence and conjugacy of Sylow subgroups can be almost trivially verified (based on the finite case) once you note that a projective limit of nonempty finite set is still nonempty.

Definition 13. Let I be a set, $\{x_i\}_{i\in I}$ a set of indeterminates indexed by I. Define the **free pro-p-group** generated by x_i as $\varprojlim_M L(I)/M$, where $L(I)$ is the discrete free group $F(I)$ generated by x_i, and M runs over normal subgruops containing all but finitely many x_i such that $L(I)/M$ is a p-group.

Being "free" is justified by the following property:

Proposition 14. Suppose G is any pro-p-group. Then there is a 1-1 correspondence between $\{$morphisms from $F(I)$ to $G\}$ and $\{\{g_i\}_{i\in I} : g_i$ converges to 0 along the filter made of complements of finite subsets of $I\}$.

Proof. Given a morphism $\phi : F(I) = \varprojlim_M L(I)/M \longrightarrow G$, consider $\{\phi(x_i)\}_i$, which converges to zero due to the assumptions that M contains almost all x_i. Conversely, given such $\{g_i\}_i$, one can well define a morphism sending x_i to g_i, due to G being pro-p. □

Remark 9. One may want to compare $F_s(I)$, defined to be the p-completion of $L(I)$, to the free pro-p-group $F(I)$.

1. Similar to Proposition 14, given a pro-p-group G, morphisms from $F_s(I)$ to G are in 1-1 correspondence with elements of G^I.

2. There is a natural projection $F_s(I) \longrightarrow F(I)$. Actually, $F_s(I)$ must be isomorphic to some $F(J)$. So, we know that the p-completion of any free discrete group is a free pro-p-group.

3. Another easy fact that deserves our attention is that $F(I) = F_s(I)$ if I is finite.

Is it possible that we make the structure of a free pro-p-group explicit? The following proposition due to Lazard gives a positive answer for **free pro-p-groups $F(n)$ of finite rank**, i.e. generated by finitely many indeterminates.

Proposition 15. There is a continuous isomorphism α (of $\mathbb{Z}_p$-algebras) from $\mathbb{Z}_p[[F(n)]]$ to $A(n)$, the Magnus algebra over $\mathbb{Z}_p$, equipped with the weak* topology (in other words, the topology of coefficient-wise convergence) such that

$$\begin{aligned} \alpha : \mathbb{Z}_p[[F(n)]] &\longrightarrow A(n) \\ x_i &\longmapsto 1+t_i. \end{aligned}$$

Proof. The proof is short and elegant if you understand Inverse Limit, so that you really understand the Iwasawa algebra $\mathbb{Z}_p[[F(n)]]$ generated by the group $F(n)$ over $\mathbb{Z}_p$. It can be interpreted as the completion of $\mathbb{Z}_p[F(n)]$ under the usual topology given by the inverse limit.

α is clear to be well defined by freedom of x_i. To define the inverse, we wish the map

$$\begin{aligned} \beta : A(n) &\longrightarrow \mathbb{Z}_p[[F(n)]] \\ t_i &\longmapsto x_i - 1 \end{aligned}$$

is continuous (clearly well defined). It suffices to show the powers of the augmentation ideal I of $\mathbb{Z}_p[[F(n)]]$ tend to 0. This is a consequence of the following trivial fact: for any normal open subgroup U of $F(n)$, any $r \in \mathbb{Z}_{>0}$, $I^k = 0$ in $(\mathbb{Z}/p^r)[F(n)/U]$. Therefore the inverse β of α is verified to exist. □

Corollary 1. The free pro-p-group $F(n)$ of rank n is isomorphic to the multiplicative subgruop of $A(n)$ generated by $1+t_1, ..., 1+t_n$.

Proof. By restricting α to $F(n)$, one obtains an injective morphism θ from $F(n)$ to U, the (closed) multiplicative subgroup of A(n) consisting of (noncommutative) formal series with degree zero term 1. □

Exercise 1. One can verify directly that U (defined in the proof of Corollary 1) is a pro-p-group. (Hint: Recall that $\{1+p^k\mathbb{Z}_p\}_k$ forms a base of 1 in $\mathbb{Z}_p$. Similarly, find a base of 1 of consisting of open subgroups in $A(n)$, with index a power of p.)

The following Exercise 2 is given by Serre and the author, the proof by the author.

Exercise 2. (Structure of Divisible Abelian Groups) Every divisible abelian group M is isomorphic to a direct sum of $\mathbb{Q}$ and the Prüfers $\mathbb{Z}(p^\infty) \simeq \mathbb{Q}_p/\mathbb{Z}_p$.

Every torsion-free abelian profinite group G is isomorphic to a product of $\mathbb{Z}_p$.

Prove or disprove the following statement: every abelian profinite group is isomorphic to a product of $\mathbb{Z}_p$ and the finite Adele $\mathbb{A}_f := \prod_p' \mathbb{Q}_p$.

Proof. For the first statement, $Tor(M)$ is a divisible (thus injective) subgroup of M, thus a direct summand of M. So, we have $M \simeq Tor(M) \oplus M/Tor(M)$. $M/Tor(M)$ is torsion-free and divisible, thus a vector space over $\mathbb{Q}$. For every p, pick a maximal $\mathbb{Z}$-independent family $\{x_i\}_{i\in I}$ in $(Tor(M))_p$, the p-primary component of $Tor(M)$. Existence of such a family is justified by the Zorn's lemma. By divisibility and independence of x_i, we have $(Tor(M))_p \simeq \oplus_{i\in I}\mathbb{Z}(p^\infty)$.

The second statement follows from the first. Since G is compact abelian, its Pontryagin dual G^* is torsion abelian, and divisible since G is torsion-free. Thus G^* is isomorphic to a

direct sum of $\mathbb{Z}(p^\infty)$. Therefore, by Pontryagin duality, $G \simeq Hom(G^*, \mathbb{Q}/\mathbb{Z})$ is isomorphic to a product of $Hom(\mathbb{Z}(p^\infty), \mathbb{Q}/\mathbb{Z})$. Note that

$$Hom(\mathbb{Z}(p^\infty), \mathbb{Q}/\mathbb{Z}) = Hom(\cup_n (Z/p^n), \mathbb{Q}/\mathbb{Z}) \simeq \varprojlim_n \mathbb{Z}/p^n \simeq \mathbb{Z}_p.$$

Therefore, G is isomorphic to a product of $\mathbb{Z}_p$.

The last statement is false. Otherwise, every abelian profinite group must be torsion free, thus isomorphic to a product of $\mathbb{Z}_p$, which is absolutely absurd. □

Exercise 3. Suppose G is a profinite group. Prove or disprove that elements in the Iwasawa algebra $\mathbb{Z}_p[[G]]$ can be expressed as a formal sum $\sum_{g\in G} a_g g$, where $a_g \in \mathbb{Z}_p$, such that for any open normal subgroup U of G, any coset $\tau \in F(n)/U$, $\sum_{g\in\tau} a_g$ converges in $\mathbb{Z}_p$.

Remark 10. How is the last statement in the Exercise 2 formulated? If you pretend the Pontryagin dual of an abelian profinite group G is divisible, and apply the structure theorem and Pontryagin duality, you will calculate and find that

$$Hom(\mathbb{Q}, \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Q} \otimes_{\mathbb{Z}} \prod_p \mathbb{Z}_p \simeq \mathbb{A}_f.$$

The statement is completely nonsense of course, but it illustrates two points:

1. From the view of Pontryagin duality, the structure of divisible torsion abelian groups corresponds to the structure of torsion-free abelian profinite groups.

2. One of the reasons why $\mathbb{A}_f$ is introduced. ($Hom(\mathbb{Q}, \mathbb{Q}/\mathbb{Z})$)

We end this subsection with an example of Iwasawa algebras.

Example 4. Let $n = 1$. Then the free pro-p-group of rank 1 is the p-completion $\mathbb{Z}_p$ of $\mathbb{Z}$. The Iwasawa algebra $\mathbb{Z}_p[[\mathbb{Z}_p]]$ is isomorphic to the Magnus algebra $A(1)$ of rank 1 over $\mathbb{Z}_p$, i.e. the ring $\mathbb{Z}_p[[X]]$ of formal power series of rank 1 over $\mathbb{Z}_p$.

5.2 Cohomology of profinite groups

We are going to define cohomology on discrete G-modules, for a profinite group G. Recall what a discrete G-module is:

Proposition 16. Suppose A is a discrete abelian group, G a profinite group acting on A. The following three statements are equivalent:

1. the action is continuous;

2. the stabilizer of every element of A is an open subgroup of G;

3. $A = \cup_U A^U$, where U runs over open subgroups of G.

Suppose A is a discrete G-module. Define the cohomology groups $H^n(G,A), n \geq 0$, from the cochain complex $C^*(G,A)$

$$0 \longrightarrow C^0(G,A) \longrightarrow C^1(G,A) \longrightarrow \cdots,$$

where $C^n(G,A)$ denotes the group of continuous maps from G^n to A (i.e. locally constant maps). By definition, we know that $\prod_{i\in I} H^n(G,A_i) \simeq H^n(G, \prod_{i\in I} A_i)$ if $\{A_i\}_{i\in I}$ is a family of discrete G-modules. We relate the cohomology of profinite groups to the cohomology of finite groups by taking limits.

Proposition 17. Suppose $\{G_i\},\{A_i\}$ are projective system and inductive system respectively, indexed by the same directed set I, where A_i is a discrete G_i-module and the inductive maps $A_i \longrightarrow A_j$ are compatible with $G_j \longrightarrow G_i$, for $i \leq j$. Then we have a canonical isomorphism

$$H^n(\varprojlim_i G_i, \varinjlim A_i) \simeq \varinjlim H^n(G_i, A_i).$$

Proof. Put $G := \varprojlim_i G_i, A := \varinjlim_i A_i$. One can check that there is a canonical isomorphism $\varinjlim C^*(G_i,A_i) \longrightarrow C^*(G,A)$. Then pass to isomorphism of cohomology by noting that direct limit behaves well with quotients. □

Corollary 2. Recall that $H^n(G,A), n \in \mathbb{Z}_{>0}$, is annihilated by $|G|$ if G is finite (a fact proved by dimension shifting and the trivial fact that $A^G/N_G A$ is annihilated by $|G|$). For a profinite group G, a discrete G-module A, the higher cohomologies are torsion.

Remark 11. Here I remark on what can be discussed about cohomology being torsion.

1. In the general setting of cohomology/ homology, torsion often means "no infinite algebraic/topological invariants" and "periodicity".

2. If a cohomology group $H^n(G,A)$ is torsion abelian, one may guess its Pontryagin dual is $H^n(G,A^*)$, where A^* is the Pontryagin dual of A. This is true in a more general setting where G is replaced by a compact space and consider the Čech (co)homology.

Example 5. Suppose K is a non-archimedean local field. Then the Brauer group $Br(K) := H^2(G_K, \overline{K}^\times)$ of K is isomorphic to $\mathbb{Q}/\mathbb{Z}$, where G_K is the absolute Galois group of K. The Brauer group provides a fundamental link between local and global class field theory, and offers new ways to understand the structure of number fields. Thus the Pontryagin dual $(H^2(G_K, \overline{K}^\times))^*$ of the Brauer group is isomorphic to $\hat{\mathbb{Z}}$. One can verify that this coincides with $H^2(G_K, Hom(\overline{K}^\times, \mathbb{Q}/\mathbb{Z}))$ (see Problem 1 for details).

Problem 1. *Suppose K is a non-archimedean local field. Then $Hom(\overline{K}^\times, \mathbb{Q}/\mathbb{Z})$ becomes a G_K-module. Calculate $H^2(G_K, Hom(\overline{K}^\times, \mathbb{Q}/\mathbb{Z}))$ by considering finite Galois subextensions of $\overline{K}/K$.*

With Proposition 17, usual properties of cohomology of finite groups can be translated to the profinite case.

Proposition 18. Suppose G is a profinite group, A is a discrete G-module. Then

1. the higher cohomologies $H^n(G,A), n > 0$, vanish when A is injective in the category C_G of discrete G-modules;

2. The functor $H^*(G,-)$ is a derived functor of the functor $A \longmapsto A^G$.

Proof. For the first statement, since A is an injective G-module, for any open normal subgroup U of G, A^U is an injective G/U-module. Therefore, we have

$$H^n(G/U, A^U) = Ext^n_{\mathbb{Z}[G/U]}(\mathbb{Z}, A^U) = 0, \forall n \geq 1.$$

By Proposition 17, $H^n(G,A) = \varinjlim H^n(G/U,A) = 0, \forall n \geq 1$.

For the second statement, Given any exact sequence of discrete G-modules

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0,$$

we have a short exact sequence of cochain complexes by applying $Hom_{\mathbb{Z}[G]}(-,A)$, $Hom_{\mathbb{Z}[G]}(-,B)$, $Hom_{\mathbb{Z}[G]}(-,C)$ (continuous homomorphisms) to the standard free resolution of $\mathbb{Z}$ by $\mathbb{Z}[G^n]$. From the short exact sequence of cochain complexes we derive the long exact sequence

$$\begin{aligned} 0 \longrightarrow H^0(G,A) &\longrightarrow H^0(G,B) \longrightarrow H^0(G,C) \\ &\longrightarrow H^1(G,A) \longrightarrow \cdots, \end{aligned}$$

where $H^0(G,A) = \varinjlim_U H^0(G/U, A^U) = \varinjlim_U A^G = A^G$. □

Exercise 4. One may check whether $H^*(G,-)$ is a cohomological universal δ-functor, as in the case G being discrete.

5.3 Cohomology of Discrete Groups and Tate Cohomology

In this subsection, all groups mentioned are discrete. Let G be a group, A an abelian group.

Definition 14. Suppose H is a subgroup of G, A an H-module. Define the coinduced G-module associated to A to be

$$CoInd_H^G(A) = Hom_{\mathbb{Z}[H]}(\mathbb{Z}[G], A),$$

with the group action $(g\phi)(z) = \phi(zg), z \in \mathbb{Z}[G]$, for $g \in G, \phi \in CoInd_H^G(A)$. Define the induced G-module associated to A to be

$$Ind_H^G(A) = \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A,$$

with the group G acting on the left of the tensor. Denote $CoInd_H^G\,(Ind_H^G)$ by $CoInd^G\,(Ind^G)$ if $H = 1$.

Lemma 1. *$CoInd^G(A)$ is acyclic, and $H^0(G, CoInd^G A) \simeq A$.*

Proof. By the standard free resolution of $\mathbb{Z}$

$$\cdots \longrightarrow \mathbb{Z}[G^2] \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0,$$

and isomorphisms $Hom_{\mathbb{Z}[G]}(\mathbb{Z}[G^n], Hom_{\mathbb{Z}}(\mathbb{Z}[G], A)) \simeq Hom_{\mathbb{Z}}(\mathbb{Z}[G^n], A)$, we obtain an isomorphism of cochain complexes between

$$0 \longrightarrow Hom_{\mathbb{Z}[G]}(\mathbb{Z}[G], CoInd^G A) \longrightarrow Hom_{\mathbb{Z}[G]}(\mathbb{Z}[G^2], CoInd^G A) \longrightarrow \cdots$$

and

$$0 \longrightarrow Hom_{\mathbb{Z}}(\mathbb{Z}[G], A) \longrightarrow Hom_{\mathbb{Z}}(\mathbb{Z}[G^2], A) \longrightarrow \cdots.$$

Therefore, we obtain $H^n(G, CoInd^G A) \simeq H^n(\{1\}, A)$. Consider the free resolution of $\mathbb{Z}$ by $\{1\}$-modules

$$\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow 0.$$

We have

$$H^n(\{1\}, A) = \begin{cases} A, & n = 0 \\ 0, & n > 0. \end{cases}$$

□

Our first goal would be to define Tate cohomology. To do this, we define homology $H_*(G,A)$ by the *Tor* functor in a usual way (If G has a non-discrete topology, homology cannot be defined in this usual manner). Similar to Lemma 1, we have

Lemma 2.

$$H_n(G,Ind^G A) = \begin{cases} A, & n=0 \\ 0, & n>0. \end{cases}$$

Proof. By the same argument in the proof of Lemma 1, we have

$$H_n(G,IndA) = Tor_n^{\mathbb{Z}[G]}(\mathbb{Z},Ind^G A) \simeq Tor_n^{\mathbb{Z}}(\mathbb{Z},A) = H_n(\{1\},A).$$

□

For a G-module A, we denote $H_0(G,A) \simeq \mathbb{Z} \otimes_{\mathbb{Z}[G]} A$ by A_G, called the **G-coinvariants** of A. A^G is the largest trivial G-submodule of A, and A_G is the largest trivial G-module quotient of A.

For more general induced modules, we have the following fundamental lemma of Shapiro, proved in exactly the same way as in Lemma 1 and Lemma 2, using *Ext* and *Tor*.

Lemma 3. *Let $H \leq G$, A be an H-module. Then we have canonical isomorphisms*

$$H^n(G,CoInd_H^G A) \simeq H^n(H,A)$$
$$H_n(G,Ind_H^G A) \simeq H_n(H,A),$$

for $n \geq 0$. In particular, if $(G:H) < \infty$, then $H_n(G,CoInd_H^G A) \simeq H_n(H,A)$ since $Ind_H^G A \simeq CoInd_H^G A$.

Proof. Note that

$$Hom_{\mathbb{Z}[G]}(\mathbb{Z}[G^n],CoInd_H^G A) \simeq Hom_{\mathbb{Z}[H]}(\mathbb{Z}[G^n],A),$$

and that

$$\mathbb{Z}[G^n] \otimes_{\mathbb{Z}[G]} Ind_H^G A \simeq \mathbb{Z}[G^n] \otimes_{\mathbb{Z}[H]} A.$$

□

From now on till the end of this subsection, G denotes a finite group unless stated otherwise. For any abelian group A, we have an isomorphism $CoInd^G A \simeq Ind^G A$.

Example 6. Suppose L/K is a finite Galois extension. Then $H^n(Gal(L/K),L) = 0, n > 0$.

Proof. Since L/K is Galois, it is a splitting field of some polynomial with coefficients in K. Hence there exists $\alpha \in L$ such that $\{\sigma(\alpha)\}_{\sigma \in G}$ forms a basis of L/K, where G denotes $Gal(L/K)$. Therefore $L \simeq \mathbb{Z}[G] \otimes_{\mathbb{Z}} K \simeq CoInd^G K$ is an acyclic G-module. □

Definition 15. Let $N_G := \sum_{g \in G} g$. Suppose A is a G-module. Let $\hat{N}_G^A$ (abbreviated as $\hat{N}_G$ if no confusion arises) denote the map $A_G \longrightarrow A^G$ induced by multiplication by N_G. Define Tate cohomology groups of G with coefficients in A to be

$$H_T^n(G,A) = \begin{cases} H^n(G,A), & n > 0 \\ Coker\hat{N}_G, & n = 0 \\ Ker\hat{N}_G, & n = -1 \\ H_{-n-1}(G,A), & n < -1. \end{cases}$$

Any G-module homomorphism $f : A \longrightarrow B$ induces maps

$$Coker\hat{N}_G^A = A^G/N_GA \longrightarrow B^G/N_GB = Coker\hat{N}_G^B$$

and

$$Ker\hat{N}_G^A = ann_A(N_G)/I_GA \longrightarrow ann_B(N_G)/I_GB = Ker\hat{N}_G^B,$$

where I_G denotes the augmentation ideal of $\mathbb{Z}[G]$. Therefore one can verify that $H_T^n(G,-)$ is a covariant functor from the category of G-modules to the category of abelian groups, for all $n \in \mathbb{Z}$.

Exercise 5. Prove that $\{H_T^n(G,-)\}_{n\in\mathbb{Z}}$ is a cohomological δ-functor.

Proof. Given a short exact sequence of G-modules

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0,$$

what needs proof is the existence and naturality of the map

$$H_T^{-1}(G,C) \longrightarrow H_T^0(G,A).$$

Since the category of G-modules is an abelian category, this follows immediately from applying the snake lemma to the following commutative diagram

$$\begin{array}{ccccccc} & & A_G & \longrightarrow & B_G & \longrightarrow & C_G & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \hat{N}_G^A} & & \downarrow{\scriptstyle \hat{N}_G^B} & & \downarrow{\scriptstyle \hat{N}_G^C} & & \\ 0 & \longrightarrow & A^G & \longrightarrow & B^G & \longrightarrow & C^G & & \end{array} .$$

□

The definition of cohomology leads us to calculate H_T^0, H_T^{-1} for some specific examples.

Example 7. Suppose G is abelian, $A = \mathbb{Z}[G]$. Let $aug : \mathbb{Z}[G] \longrightarrow \mathbb{Z}$ denote the augmentation map. Note that $N_Gz = aug(z)N_G, \forall z \in \mathbb{Z}[G]$, we have $ann(N_G) = I_G$, thus, $H_T^{-1}(G,A) = 0$. Since $\mathbb{Z}[G]^G = \mathbb{Z}N_G = N_GA$, we have $H_T^0(G,A) = 0$.

This example is not alone, noting that $\mathbb{Z}[G]$ is induced from $\mathbb{Z}$. More generally, we have

Proposition 19. Suppose A is an abelian group. Then $H_T^n(G, Ind^GA) = 0, \forall n \in \mathbb{Z}$.

Proof. It suffices to prove $H_T^0, H_T^{-1} = 0$. A similar argument as in Example 6 works directly, but here is another perspective. We have $H_T^n(G, Ind^GA) \simeq H_T^n(\{1\}, A)$, and

$$H_T^0(\{1\},A) = A^{\{1\}}/A = 0$$
$$H_T^{-1}(\{1\},A) = ann(1)/0 = 0$$

□

Corollary 3. Suppose A is a free $\mathbb{Z}[G]$-module. Then Tate cohomology of A vanishes.

Proof. Let S be a $\mathbb{Z}[G]$-basis of A, B the free $\mathbb{Z}$-module with basis S. Then we have $A \simeq Ind^GB$. Apply Proposition 19. □

Tate cohomology is a crucial tool for studying Galois extensions, as we would discuss in the future. To serve this purpose, we need to look at the case where G is finite cyclic, to (hopefully) work on extensions like unramified extensions of local fields, and subsequently global fields. For finite cyclic groups, we show that one can easily determine $H_T^n, \forall n \in \mathbb{Z}$, once H_T^0, H_T^{-1} are known.

Proposition 20. Suppose $G =< g >$ is finite cyclic, with g the generator. Let A be a G-module. Then we have

$$H_T^{2n}(G,A) = H_T^0(G,A)$$
$$H_T^{2n-1}(G,A) = H_T^{-1}(G,A),$$

for all $n \in \mathbb{Z}$.

Proof. We have the following free resolution of $\mathbb{Z}$ by $\mathbb{Z}[G]$-modules

$$\cdots \longrightarrow \mathbb{Z}[G] \xrightarrow{g-1} \mathbb{Z}[G] \xrightarrow{N_G} \mathbb{Z}[G] \xrightarrow{g-1} \mathbb{Z}[G] \xrightarrow{aug} \mathbb{Z} \longrightarrow 0$$

Apply $Hom_{\mathbb{Z}[G]}(-,A)$ and $-\otimes_{\mathbb{Z}[G]} A$. Calculate the cohomologies and homologies of the cochain complex and the chain complex respectively, completing the proof. □

We introduce a cohomological invariant that will directly appear in number theory.

Definition 16. Suppose G is finite cyclic, A a G-module. If $h^0(A) := \#H_T^0(G,A), h^{-1}(A) := \#H_T^{-1}(G,A) < \infty$, we define the Herbrand quotient $h(A) = h^0(A)/h^{-1}(A)$.

Suppose L/K is a finite Galois extension of nonarchimedean local fields. Then $L^\times$ is naturally a $Gal(L/K)$-module. Then we have $H_T^0(Gal(L/K), L^\times) \simeq K^\times / N_{L/K}(L^\times)$. By Hilbert 90 (Theorem 3), we have

$$H_T^1(Gal(L/K), L^\times) = 0.$$

If L/K is cyclic, then $h(L^\times) = |K^\times / N_{L/K}(L^\times)|$. The fact that $N_{L/K}(L^\times)$ has finite index is a consequence of local reciprocity.

Proposition 21. Suppose G is finite cyclic. For any short exact sequence of G-modules

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0,$$

if any two of $h(A), h(B), h(C)$ are defined, so is the third and $h(B) = h(A)h(C)$.

Proof. By the periodicity of cohomology groups of G, and the fact that $H_T^*(G,-)$ is a cohomological δ-functor, we have the following commutative diagram

$$\begin{array}{ccccc} H_T^0(G,A) & \longrightarrow & H_T^0(G,B) & \longrightarrow & H_T^0(G,C) \\ \uparrow & & & & \downarrow \\ H_T^{-1}(G,C) & \longleftarrow & H_T^{-1}(G,B) & \longleftarrow & H_T^{-1}(G,A) \end{array},$$

and the conclusion follows. □

Proposition 22. Suppose $G =< g >$ is finite cyclic, A a G-module, finitely generated as an abelian group. Then $h(A)$ is well-defined. If moreover G acts on A trivially, then $h(A) = |G|^r$, where $r = rankA$.

Proof. Note that both $H_T^0(G,A) = A^G/N_G A$ and $H_T^{-1}(G,A) = ann(N_G)/(g-1)A$ are finitely generated abelian groups and annihilated by $|G|$, therefore finite, so that $h(A)$ is well-defined.

If moreover A is a trivial G-module, decompose $A = \mathbb{Z}^r \oplus A_t$ into its free part and its torsion part, which are indeed G-submodules. It suffices to show $h(\mathbb{Z}) = |G|$ and $h(A_t) = 1$. For $\mathbb{Z}$, The norm map becomes

$$\begin{aligned} \hat{N}_G^{\mathbb{Z}} : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ a &\longmapsto |G|a. \end{aligned}$$

Hence we have $h(\mathbb{Z}) = \frac{\#(\mathbb{Z}/|G|\mathbb{Z})}{\#ann_{\mathbb{Z}}(|G|)} = |G|$. The fact that $h(A_t) = 1$ is proved in the following lemma. □

Proposition 23. If A is a G-module with $\#A < \infty$, $G =< g >$ finite cyclic, then $h(A) = 1$.

Proof. Consider the exact sequence

$$0 \longrightarrow A^G \longrightarrow A \longrightarrow A \longrightarrow A_G \longrightarrow 0,$$

where the middle map is given by multiplication by $g-1$. Since $\#A < \infty$, we can prove that $\#A^G = \#A_G < \infty$. Therefore

$$\#Coker(\hat{N}_G) = \#A^G/\#Im(\hat{N}_G) = \#A_G/\#Im(\hat{N}_G) = \#Ker(\hat{N}_G),$$

which implies $h(A) = 1$. □

In explicit settings, we would use Tate cohomology to construct isomorphisms $K^\times/N_{L/K}(L^\times) \simeq Gal(L/K)$, where K is a nonarchimedean local field, L/K a finite abelian extension, as isomorphisms between cohomology groups. From this construction we induce the homomorphism $K^\times \longrightarrow Gal(K^{ab}/K)$ by taking inverse limit, establishing local reciprocity.

Recall that we defined (co)induced G-module associated to any abelian group A. If A is already a G-module, we still can define the (co)induced G-module for A.

Definition 17. Suppose G is a group (not necessarily finite), H a subgroup of G. A is a G-module. Define

$$CoInd_H^G A = Hom_{\mathbb{Z}[H]}(\mathbb{Z}[G], A)$$

with the action of G by $(g\phi)(z) := g\phi(g^{-1}z), \forall z \in \mathbb{Z}[G]$, for $\phi \in CoInd^G A$,

$$Ind_H^G A = \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A$$

with the action of G by $g(z \otimes a) := gz \otimes ga$, for $z \otimes a \in Ind_H^G A$.

Definition 17 enables us to view A as a quotient module of $Ind_H^G A$, and as a submodule of $CoInd_H^G A$, by paying attention to the quotient map $\mathbb{Z}[G] \longrightarrow \mathbb{Z}[H]$. Denote the forgetful functor from the category of G-modules to the category of abelian groups by $\mathscr{F}$. Then we have G-module isomorphisms

$$\begin{aligned} CoInd^G(A) &\longrightarrow CoInd^G\mathscr{F}(A) \\ \phi &\longmapsto [g \longmapsto g\phi(g^{-1})], \\ Ind^G A &\longrightarrow Ind^G\mathscr{F}(A) \\ g \otimes a &\longmapsto g \otimes g^{-1}a. \end{aligned}$$

Hence, we can still appeal to facts developed (in Lemma 1, 2, 3, for example) if we replace $CoInd^G\mathscr{F}(A)$ by $CoInd^GA$, $Ind^G\mathscr{F}(A)$ by Ind^GA. This allows us to build a connection of (co)homology groups of different dimensions by looking at the exact sequences

$$0 \longrightarrow A \longrightarrow CoInd^GA \longrightarrow Hom_{\mathbb{Z}}(I_G,A) \longrightarrow 0,$$
$$0 \longrightarrow I_G \otimes_{\mathbb{Z}} A \longrightarrow Ind^GA \longrightarrow A \longrightarrow 0.$$

Let H be a subgroup of G. By the property of (co)homological δ-functor, and noting that $CoInd^GA = CoInd^HCoInd^G_HA, Ind^GA = Ind^HInd^G_HA$, we have isomorphisms

$$H^{n+1}(H,A) \simeq H^n(H,Hom_{\mathbb{Z}}(I_G,A))$$
$$H_{n+1}(H,A) \simeq H_n(H,I_G \otimes_{\mathbb{Z}} A)$$

for all $n \geq 1$. If G is moreover finite, then these isomorphisms yield

$$H^{n+1}_T(H,A) \simeq H^n_T(H,Hom_{\mathbb{Z}}(I_G,A))$$

for all $n \in \mathbb{Z}$. By this technique of dimension shifting, some basic properties of Tate cohomology groups can be proved.

Proposition 24. Let G be a finite group, A a G-module. Then $exp(H^n_T(G,A))|\#G, \forall n \in \mathbb{Z}$.

Proof. By dimension shifting, it suffices to show $exp(H^0_T(G,A))|\#G$, which is the fact that A^G/N_GA is annihilated by $\#G$. □

Proposition 25. Let G be a finite group, A a finitely generated G-module. Then $\#H^n_T(G,A) < \infty, \forall n \in \mathbb{Z}$.

Proof. By Proposition 24, $H^n_T(G,A)$ is torsion. A being finitely generated leads $H^n_T(G,A)$ to be a finitely generated abelian group, completing the proof.

Alternatively, one can argue directly using dimension shifting by verifying that $Hom_{\mathbb{Z}}(I_G,A)$, A^G/N_GA are finitely generated if A is finitely generated. □

Remark 12. By Proposition 25, if A is finitely generated (To say A finitely generated as a $\mathbb{Z}$-module is equivalent to say it finitely generated as a G-module), then the Herbrand quotient $h(A)$ is well-defined, generalizing the first statement of Proposition 22.

Using the idea of dimension shifting, we can develop a fundamental tool concerning the restriction maps and the inflation maps.

Definition 18. Suppose G is a group (not necessarily finite), H a normal subgroup of G. Let A be a G-module. Define the restriction maps to be

$$res : H^i(G,A) \longrightarrow H^i(H,A)$$

for $i \geq 0$, induced by the inclusion $H \longrightarrow G$. Define the inflation maps to be

$$inf : H^i(G/H,A^H) \longrightarrow H^i(G,A)$$

for $i \geq 0$, induced by $G \longrightarrow G/H$ and $A^H \longrightarrow A$.

Exercise 6. With settings as in Definition 18, define the **corestriction** maps to be

$$cor : H^i(H,A) \longrightarrow H^i(G,A)$$

for $n \geq 0$, induced by $CoInd^G_HA \simeq Ind^G_HA \longrightarrow A$ and $H^i(H,A) \simeq H^i(G,CoInd^G_HA)$ (Shapiro's lemma). Assume that $(G:H) < \infty$. Prove that $cor \circ res$ is multiplication by $(G:H)$ on $H^i(G,A)$. Deduce that $H^n(G,A) = 0, \forall n > 0$ if $\#G, \#A < \infty$ and satisfy $gcd(\#G,\#A) = 1$.

Proof. For any cohomology class $f \in H^i(G,A)$, $res(f)$ stays essentially the same. By identifying $H^i(H,A)$ with $H^i(G,CoInd_H^G A)$, f is identified with $(G:H)$ copies of f. Since $Ind_H^G A \longrightarrow A$ sums over cosets of H, $cor(res(f))$ is the sum of these copies of f, which is to say $cor \circ res$ is multiplication by $(G:H)$.

Since $gcd(\#G,\#A) = 1$, we have an isomorphism

$$\begin{aligned} A &\longrightarrow A \\ a &\longmapsto (\#G)a, \end{aligned}$$

which induces an automorphism on $H^i(G,A), i \geq 0$, multiplication by $\#G$, the same as $cor^G_{\{1\}} \circ res^G_{\{1\}}$. Note that $H^n(\{1\},A) = 0, \forall n > 0$. The conclusion follows. □

One should note that (co)restriction maps are still well-defined for arbitrary subgroups of G (not necessarily finite).

Similarly one can define (co)restriction maps and **coinflation** maps on homology groups. Suppose A is a G-module, H a subgroup of G. Define

$$\begin{aligned} cor &: H_*(G,A) \longrightarrow H_*(G,Ind_H^G A) \xrightarrow{\sim} H_*(H,A) \\ res &: H_*(H,A) \longrightarrow H_*(G,A) \end{aligned}$$

and, if H is a normal subgroup,

$$coinf : H_*(G,A) \longrightarrow H_*(G/H,A) \longrightarrow H_*(G/H,A_H).$$

Therefore, if G is finite, we have the definition of (co)restriction on Tate cohomology groups.

$$\begin{aligned} res &: H_T^*(G,A) \longrightarrow H_T^*(H,A) \\ cor &: H_T^*(H,A) \longrightarrow H_T^*(G,A). \end{aligned}$$

The following lemma would be a useful tool for the later study of cohomological properties of the Galois world (such as Brauer groups and artin reciprocity).

Lemma 4. *With settings as in Definition 18, we have an exact sequence*

$$0 \to H^1(G/H,A^H) \xrightarrow{inf} H^1(G,A) \xrightarrow{res} H^1(H,A).$$

For $i \geq 2$, if $H^1(H,A) = \cdots H^{i-1}(H,A) = 0$, then we have an exact sequence

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

Proof. The first exact sequence can be justified by definition of res, inf and H^1. We prove the rest by induction on i. Consider the short exact sequence

$$0 \longrightarrow A \longrightarrow CoInd^G A \longrightarrow Hom_{\mathbb{Z}}(I_G,A) \longrightarrow 0,$$

which induces the commutative diagram of short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A^H & \longrightarrow & (CoInd^G A)^H & \longrightarrow & (Hom_{\mathbb{Z}}(I_G,A))^H & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A & \longrightarrow & CoInd^G A & \longrightarrow & Hom_{\mathbb{Z}}(I_G,A) & \longrightarrow & 0 \end{array}.$$

Denote $Hom_{\mathbb{Z}}(I_G, A)$ by B. Apply $H^*(H,-)$ to the second line of the above diagram. We can prove that $H^1(H,B) = \cdots = H^{i-2}(H,B) = 0$ if $i \geq 3$, resulting in the exacteness of

$$0 \longrightarrow H^{i-1}(G/H,B) \longrightarrow H^{i-1}(G,B) \longrightarrow H^{i-1}(H,B)$$

for $i \geq 2$, by the induction hypothesis (the case $i = 2$ was independently verified), and (dimension shifting) $H^{i-1}(H,B) = H^i(H,A)$. Together with applying $H^*(G,-), H^*(G/H,-)$ to the second, first line of the diagram respectively, we have the commutativity of dimension shifting with inflation and restriction:

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^{i-1}(G/H, B^H) & \longrightarrow & H^{i-1}(G,B) & \longrightarrow & H^{i-1}(H,B) \\ & & \downarrow & & \downarrow & & \downarrow \\ & & H^i(G/H, A^H) & \longrightarrow & H^i(G,A) & \longrightarrow & H^i(H,A) \end{array},$$

completing the proof. □

Remark 13. Conclusions of Lemma 4 are often referred to as the inflation-restriction sequence, a special case of Hochschild-Serre spectral sequence, which is beyond the scope of this material.

For later usage in the explicit study of class field theory, We relate the abelianization of a group to the first-order homology.

Example 8. Suppose G is a group (not necessarily finite). We have a canonical isomorphism

$$H_1(G,\mathbb{Z}) \simeq G^{ab}.$$

In fact, this is again an application of the technique of dimension shifting by considering

$$0 \longrightarrow I_G \longrightarrow Ind^G\mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow 0,$$

and note the isomorphism

$$\begin{aligned} G^{ab} &\longrightarrow I_G/I_G^2 \simeq H_0(G, I_G) \\ g &\longmapsto g-1. \end{aligned}$$

Moreover, if H is a subgroup of G, the corestrction map

$$cor : H_1(H,\mathbb{Z}) \longrightarrow H_1(G,\mathbb{Z})$$

coincides with $H^{ab} \longrightarrow G^{ab}$ induced by the inclusion $H \longrightarrow G$. If H is of finite index (so that the transfer map is defined), The restriction map

$$res : H_1(G,\mathbb{Z}) \longrightarrow H_1(H,\mathbb{Z})$$

coincides with the transfer map $G^{ab} \longrightarrow H^{ab}$. If H is normal, the coinflation map

$$coinf : H_1(G,\mathbb{Z}) \longrightarrow H_1(G/H,\mathbb{Z})$$

coincides with the quotient map $G^{ab} = G/G' \longrightarrow G/G'H = (G/H)^{ab}$.

5.4 Tate's Vanishing Theorem

The following result traces back to John Tate [12], 1952.
Suppose G is a finite group, A a G module. If

$$H^1(H,A) = H^2(H,A) = 0$$

for all subgroups H of G, then we have

$$H_T^i(G,A) = 0, \quad \forall i \in \mathbb{Z}.$$

Proof. If G is cyclic, this follows from Tate periodicity. Suppose G is solvable for now. We do induction on $\#G$. Let H be a normal subgroup of G such that G/H is cyclic. Then by induction hypothesis we have $H_T^i(H,A) = 0, \forall i \in \mathbb{Z}$. Therefore, considering inflation-restriction sequence, we have exact sequences

$$0 \longrightarrow H^n(G/H, A^H) \longrightarrow H^n(G,A) \longrightarrow 0$$

for $n \geq 1$. Since $H^1(G,A) = H^2(G,A) = 0$, we know $H^1(G/H,A^H) = H^2(G/H,A^H) = 0$, and thus $H_T^i(G/H,A^H) = 0, \forall i \in \mathbb{Z}$. Again by the above sequence, we have $H^i(G,A) = 0$, for $i \geq 1$. Verify $H_T^0(G,A) = 0$ and, by dimension shifting, we successively obtain $H_T^{-1}(G,A) = H_T^{-2}(G,A) = \cdots = 0$.

For an arbitraty finite group G, for any prime integer p, denote its Sylow p-subgroup by G_p. Then we have $H_T^i(G_p,A) = 0, \forall i \in \mathbb{Z}$. For any $i \in \mathbb{Z}$, consider the map

$$H_T^i(G,A) \xrightarrow{res} H_T^i(G_p,A) \xrightarrow{cor} H_T^i(G,A),$$

which is multiplication by $(G : G_p)$, and is a zero map since the middle object is zero. Since p is coprime to $(G : G_p)$, the p-primary component of $H_T^i(G,A)$ is zero. Letting p range over all prime integers completes the proof. □

5.5 Construction of Cohomology Classes

The notion of cup product relates homology groups of different orders, giving a calculation similar to taking product, which provides a way of constructing cohomology classes. For example, we can construct a Brauer class in H^2 by taking cup product of classes in H^1. See Example 9 below.

Throughout this subsection, G denotes a group.

Definition 19. Suppose A, B are G-modules define the cup products $\cup$ on cohomology groups to be

$$H^i(G,A) \otimes_{\mathbb{Z}} H^j(G,B) \xrightarrow{\cup} H^{i+j}(G, A \otimes_{\mathbb{Z}} B),$$

for $i, j \in \mathbb{Z}_{\geq 0}$, which is induced by

$$\begin{aligned} C^i(G,A) \otimes_{\mathbb{Z}} C^j(G,B) &\xrightarrow{\cup} C^{i+j}(G, A \otimes_{\mathbb{Z}} B) \\ f \otimes f' &\mapsto [(g_1, \ldots, g_{i+j}) \mapsto f(g_1, \ldots, g_i) \otimes g_1 \cdots g_i f'(g_{i+1}, \ldots, g_{i+j})]. \end{aligned}$$

Example 9. Recall the definition of Brauer groups and the Hilbert symbol. The **Brauer group** $Br(K)$ of a field K is defined to be $H^2(Gal(K_{sep}/K), K_{sep}^{\times})$. If L/K is a finite Galois extension, then the corresponding Brauer group $Br(L/K)$ is defined to be $H^2(G(L/K), L^{\times})$.

The Hilbert symbol $(\ ,\ )_n$ is defined as follows. Suppose K is a local field containing the group $\mu(n)$ of n-th roots of 1, where n is a positive integer not divided by $char(K)$ if $char(K) > 0$. Let $L_n = K((K^\times)^{1/n})$ be the maximal abelian extension of K of exponent n, with Galois group G_n. Since we are in the Kummer case, the homomorphism

$$\begin{aligned} K^\times &\longrightarrow Hom(G_n, \mu(n)) \\ a &\longmapsto [\chi_a : \sigma \mapsto \frac{\sigma(a^{1/n})}{a^{1/n}}] \end{aligned}$$

is well defined, inducing the isomorphism

$$K^\times/(K^\times)^n \simeq Hom(G_n, \mu(n)).$$

Suppose K is moreover nonarchimedean. Since

$$K^\times \simeq O_K^\times \times \pi^{\mathbb{Z}} \simeq (1+\pi O_K) \times (O_K/\pi)^\times \times \pi^{\mathbb{Z}},$$

we know that $K^\times/(K^\times)^n$ is a finite group, and that L_n/K is therefore finite. Assuming local artin reciprocity, since $K^\times/N(L_n^\times) \simeq G_n$ has exponent n, we have $(K^\times)^n \subseteq N(L_n^\times)$, and thus $(K^\times)^n = N(L_n^\times)$ since they have the same index in $K^\times$. We have an isomorphism

$$\psi_{L/K} : K^\times/(K^\times)^n \xrightarrow{\sim} G_n.$$

Therefore the pairing

$$\begin{aligned} G_n \times Hom(G_n, \mu(n)) &\longrightarrow \mu(n) \\ (\sigma, \chi) &\longmapsto \chi(\sigma) \end{aligned}$$

can be written as

$$\begin{aligned} (\ ,\ )_n : K^\times/(K^\times)^n \times K^\times/(K^\times)^n &\longrightarrow \mu(n) \\ (a,b) &\longmapsto (a,b)_n = \frac{\psi_{L_n/K}(a)(b^{1/n})}{b^{1/n}} \end{aligned}$$

We call the pairing $(\ ,\ )_n$ the **Hilbert symbol with exponent** n. Since G_n acts trivially on $\mu(n)$, we have $H^1(G_n, \mu(n)) \simeq Hom(G_n, \mu(n)) \simeq K^\times/(K^\times)^n$. Embed $\mu(n) \simeq \mathbb{Z}/n$ into $Br(L_n/K) \simeq \mathbb{Z}/[L_n : K]$ (L_n/K being finite Galois). Then the Hilbert symbol $(\ ,\ )_n$ induces a unique map on $H^1(G_n, \mu(n)) \otimes_{\mathbb{Z}} H^1(G_n, \mu(n))$ by the universal property of tensor product, which is exactly the cup product

$$H^1(G_n, \mu(n)) \otimes_{\mathbb{Z}} H^1(G_n, \mu(n)) \xrightarrow{\cup} H^2(G_n, \mu(n)) \to H^2(G_n, L_n^\times) = Br(L_n/K).$$

This argument of realizing the Hilbert symbol as a map on cohomological groups is given by Xingfeng Lin. We will discuss Brauer groups further in the next section.

The cup products are functorial with the connecting homomorphism δ. The collection of maps

$$\{H^i(G,A) \otimes_{\mathbb{Z}} H^j(G,B) \xrightarrow{\cup} H^{i+j}(G, A \otimes_{\mathbb{Z}} B)\}_{\substack{i,j \in \mathbb{Z}_{\geq 0} \\ A,B \in Mod_G}}$$

is actually the unique one satisfying:

1. if $i = j = 0$, the cup product $H^0(G,A) \otimes_{\mathbb{Z}} H^0(G,B) \xrightarrow{\cup} H^0(G, A \otimes_{\mathbb{Z}} B)$ is induced by the identity map $A^G \otimes_{\mathbb{Z}} B^G \to (A \otimes_{\mathbb{Z}} B)^G$;

2. if

$$0 \to A_1 \to A \to A_2 \to 0$$
$$0 \to A_1 \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B \to A_2 \otimes_{\mathbb{Z}} B \to 0$$

   are exact, then

$$\delta(\alpha_2) \cup \beta = \delta(\alpha_2 \cup \beta)$$

   $(\in H^{i+j+1}(G, A_1 \otimes_{\mathbb{Z}} B))$, for $\alpha_2 \in H^i(G,A_2), \beta \in H^j(G,N)$;

3. if

$$0 \to B_1 \to B \to B_2 \to 0$$
$$0 \to A \otimes_{\mathbb{Z}} B_1 \to A \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B_2 \to 0$$

   are exact, then

$$\alpha \cup \delta(\beta_2) = (-1)^i \delta(\alpha \cup \beta_2)$$

   $(\in H^{i+j+1}(G, A \otimes_{\mathbb{Z}} B_1))$, for $\alpha \in H^i(G,A), \beta_2 \in H^j(G,B_2)$.

We can also define cup product for Tate cohomology groups by considering cap products on homology groups. Suppose G is finite. Then there exists a unique collection of maps

$$\{H_T^i(G,A) \otimes_{\mathbb{Z}} H_T^j(G,B) \xrightarrow{\cup} H_T^{i+j}(G, A \otimes_{\mathbb{Z}} B)\}_{\substack{i,j \in \mathbb{Z} \\ A,B \in Mod_G}}$$

satisfying the functoriality with δ, and that $H_T^0(G,A) \otimes_{\mathbb{Z}} H_T^0(G,B) \xrightarrow{\cup} H_T^0(G, A \otimes_{\mathbb{Z}} B)$ is induced by the identity map on $(A \otimes_{\mathbb{Z}} B)^G$.

6 Brauer Groups

We restate the definition of Brauer groups for completeness.

Definition 20. For a field K, define the Brauer group of K to be $H^2(Gal(K_{sep}/K), K_{sep}^\times)$. Suppose L/K is a Galois extension, then the Brauer group $Br(L/K)$ of L/K is defined to be $H^2(Gal(L/K), L^\times)$.

6.1 Brauer groups of local fields

In this subsection, K is a nonarchimedean local field, π a uniformizer of K.

Proposition 26. Suppose L/K is a finite unramified extension. Then we have

$$H_T^{2n}(G(L/K), L^\times) \simeq \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z},$$

and in particular, $H_T^0(G(L/K), L^\times)$ is generated by π.

Proof. This proposition is a generalization of the first result proved in Subection 1 of Section 2, since we have

$$H_T^0(G(L/K), L^\times) \simeq K^\times / N(L^\times)$$

by definition. Here is the usual proof in terms of cohomology, but the fact that $N(\mathcal{O}_L^\times) = \mathcal{O}_K^\times$ (which is to say $H_T^0(G(L/K), \mathcal{O}_L^\times) = 0$) is still needed, being the essence of this Proposition.

Consider the exact sequence

$$1 \longrightarrow \mathcal{O}_L^\times \longrightarrow L^\times \longrightarrow \mathbb{Z} \longrightarrow 0. \tag{1}$$

Since L/K is unramified, we have

$$H_T^1(G(L/K), \mathcal{O}_L^\times) = 0$$

by Hilbert 90. By Tate periodicity of cyclic groups, we know that $H_T^i(G(L/K), \mathcal{O}_L^\times) = 0, \forall i \in \mathbb{Z}$. By the long exact sequence induced from (1), we have

$$H_T^{2n}(G(L/K), L^\times) \xrightarrow{\sim} H_T^{2n}(G(L/K), \mathbb{Z}) = H_T^0(G(L/K), \mathbb{Z}) \xrightarrow{\sim} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}.$$

□

Let G denotes the Galois group $G(L/K)$ if L/K is a finite Galois extension and L is clear from the context. When L/K is unramified, we have proved an isomorphism $Br(L/K) \simeq \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$.

Proposition 27. Suppose L/K is a finite cyclic extension. Then we have

$$\#H^2(G, L^\times) = [L:K].$$

Proof. There exists an open subgroup W of $\mathcal{O}_L^\times$, stable under G, such that

$$H^i(G,W)=0$$

for any $i\in\mathbb{Z}_{>0}$. In fact, Suppose $L=\oplus_{\sigma\in G}K\sigma(\alpha)$, where $\alpha\in\pi_L^m\mathcal{O}_L$ and m is a large positive integer such that the expnential map

$$exp:\pi_L^m\mathcal{O}_L\longrightarrow U_L^m$$

is well defined, which becomes an isomorphism of G-modules. Put $M=\oplus_{\sigma\in G}\mathcal{O}_K\sigma(\alpha), W=exp(M)$. We have $W\simeq M\simeq Ind^G(\mathcal{O}_K)$ and therefore

$$H^i(G,W)=0 \tag{2}$$

for any $i\in\mathbb{Z}_{>0}$. Since M contains $\pi_L^n\mathcal{O}_L$ for some large n, we know W is indeed open in $\mathcal{O}_L^\times$.

Hence, we have

$$h(\mathcal{O}_L^\times)=h(W)h(\mathcal{O}_L^\times/W)=1,$$

since $\#(\mathcal{O}_L^\times/W)<\infty$ and $h(W)=1$ by (2). Therefore,

$$h(L^\times)=h(\mathbb{Z})=[L:K]$$

and

$$\#H^2(G,L^\times)=[L:K]$$

by Hilbert 90. □

Proposition 28. Suppose L/K is a finite Galois extension. Then we have

$$\#H^2(G,L^\times)\leq[L:K].$$

Proof. By ramfication theory, we know that G is solvable. Decompose L as $K=K_0\subseteq K_1\subseteq\cdots\subseteq K_n=L$, with the corresponding filtration of subgroups $G=G_0\supseteq\cdots\supseteq G_n=1$, such that K_{i+1}/K_i is cyclic, $0\leq i<n$, so that we can apply Proposition 27. For any $0\leq i<n$, since $H^1(G_{i+1},L^\times)=0$, we have the exactness of restriction-inflation sequences

$$0\to H^2(G_i/G_{i+1},(L^\times)^{G_{i+1}})\xrightarrow{inf}H^2(G_i,L^\times)\xrightarrow{res}H^2(G_{i+1}/L^\times).$$

Since $\#H^2(G_i/G_{i+1},(L^\times)^{G_{i+1}})=[K_{i+1}:K_i], 0\leq i<n$, we have

$$\#H^2(G,L^\times)=\prod_{i=0}^{n-1}\frac{\#H^2(G_i,L^\times)}{\#H^2(G_{i+1},L^\times)}\leq\prod_{i=0}^{n-1}\#H^2(G_i/G_{i+1},(L^\times)^{G_{i+1}})=[L:K].$$

□

Finally we achieve

Theorem 9. *Suppose L/K is a finite Galois extension. Then we have an isomorphism*

$$Br(L/K)\simeq\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}.$$

Proof. Let M be the unique unramified extension over K of degree $d = [L : K]$. Put $U = L \cap M$. Then L/U must be totally ramified. Hilbert 90 gives us exactness of the following sequences

$$0 \to H^2(G(L/K), L^\times) \xrightarrow{inf_L} H^2(G(LM/K), (LM)^\times) \xrightarrow{res_L} H^2(G(LM/L), (LM)^\times)$$
$$0 \to H^2(G(M/K), M^\times) \xrightarrow{inf_M} H^2(G(LM/K), (LM)^\times) \xrightarrow{res_M} H^2(G(LM/M), (LM)^\times).$$

Since

$$\#H^2(G(L/K), L^\times) \le d, \quad H^2(G(M/K), M^\times) \simeq \frac{1}{d}\mathbb{Z}/\mathbb{Z},$$

it suffices to show $res_L \circ inf_M = 0$, which is equivalent to

$$H^2(G(M/K), M^\times) \xrightarrow{res} H^2(G(M/U), M^\times) \to H^2(G(LM/L), (LM)^\times)$$

being the zero map. By Tate periodicity for cyclic groups, and the commutative diagram

$$\begin{array}{ccccc} H^0_T(G(M/K), M^\times) & \xrightarrow{res} & H^0_T(G(M/U), M^\times) & \longrightarrow & H^0_T(G(LM/L), (LM)^\times) \\ \downarrow\sim & & \downarrow\sim & & \downarrow\sim \\ H^2_T(G(M/K), M^\times) & \xrightarrow{res} & H^2_T(G(M/U), M^\times) & \longrightarrow & H^2_T(G(LM/L), (LM)^\times) \end{array},$$

we only need to show that the map $K^\times/N_{M/K}(M^\times) \to L^\times/N_{LM/L}((LM)^\times)$ is trivial. In fact, this is because $\pi_K = \pi_L^{e(L/K)}\alpha$ for some $\alpha \in \mathcal{O}_L^\times$, and we note that π_K generates $K^\times/N_{M/K}(M^\times)$ and that π_L generates $L^\times/N_{LM/L}((LM)^\times)$ with order $[LM : L] = [M : U] = \frac{d}{[U:K]} = e(L/K)$. □

To study $Br(K)$, we need to build the compatibility of isomorphisms $Br(L/K) \simeq \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ for various L. The following lemma is purely cohomological.

Lemma 5. *Suppose G is a finite group. Then there are (canonical) isomorphisms $\delta : H^i(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^{i+1}(G, \mathbb{Z}), i \in \mathbb{Z}_{>0}$.*

Proof. It suffices to show $H^i(G, \mathbb{Q}) = 0, \forall i \in \mathbb{Z}_{>0}$. In fact, multiplication by $\#G$ on $H^i(G, \mathbb{Q})$ is an isomorphism (induced by multiplication by $\#G$ on $\mathbb{Q}$), which factors as $cor^G \circ res^G$. The image of res^G is contained in $H^i(\{1\}, \mathbb{Q})$, which is trivial if $i \in \mathbb{Z}_{>0}$. Therefore $H^i(G, \mathbb{Q}) = 0, \forall i \in \mathbb{Z}_{>0}$. □

We can make isomorphisms $Br(L/K) \simeq \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$, L/K unramified, compatible with inflation maps by defining $inv_{L/K}$ as

$$inv_{L/K} : H^2(G(L/K), L^\times) \xrightarrow{\sim} H^2(G(L/K), \mathbb{Z}) \xrightarrow[\delta^{-1}]{\sim} H^1(G(L/K), \mathbb{Q}/\mathbb{Z}) \xrightarrow{\iota_{\sigma_K}} \mathbb{Q}/\mathbb{Z},$$

where σ_K is the arithmetic Frobenius over K and the injection

$$\begin{aligned} \iota_{\sigma_K} : Hom(G(L/K), \mathbb{Q}/\mathbb{Z}) &\longrightarrow \mathbb{Q}/\mathbb{Z} \\ \chi &\longmapsto \chi(\sigma_K) \end{aligned}$$

is the double dual of σ_K. (If σ_K is replaced by the geometric Frobenius σ_K^{-1}, then the inclusion map should be replaced by $1 \mapsto -1$, otherwise you obtain $-inv_{L/K}$ (which actually does no harm). It is okay that you choose σ_K^{-1} in your definition of invariant maps,

but since we are not in algebraic geometry, there is no natural reason of doing so.) To fit in the compatibility with inflation maps, for L/K finite Galois, with notations inf_L, M, inf_M as in the proof of Theorem 9, we define the invariant maps $inv_{L/K}$ to be

$$inv_{L/K} := inv_{M/K} \circ inf_M^{-1} \circ inf_L : Br(L/K) \to \mathbb{Q}/\mathbb{Z},$$

where inf_M^{-1} denotes the inverse of inf_M defined on the image of inf_M, which is the same as the image of inf_L.

Now suppose $L/M/K$ is a tower of finite unramified extensions. Then we have the commutative diagram

$$\begin{array}{ccccccc} H^2(G(L/K),L^\times) & \xrightarrow{\sim} & H^2(G(L/K),\mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G(L/K),\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\iota_{\sigma_K}} & \mathbb{Q}/\mathbb{Z} \\ {\scriptstyle inf_{L/M}}\uparrow & & {\scriptstyle inf_{L/M}(\mathbb{Z})}\uparrow & & {\scriptstyle inf_{L/M}(\mathbb{Q}/\mathbb{Z})}\uparrow & & \\ H^2(G(M/K),M^\times) & \xrightarrow{\sim} & H^2(G(M/K),\mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G(M/K),\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\iota_{\sigma_K}} & \mathbb{Q}/\mathbb{Z} \end{array},$$

where $inf_{L/M}, inf_{L/M}(\mathbb{Z}), inf_{L/M}(\mathbb{Q}/\mathbb{Z})$ are injective due to Hilbert 90, $H^1(G(M/K),\mathbb{Z}) = 0$, the left exactness of $Hom(-,\mathbb{Q}/\mathbb{Z})$, respectively. This proves the compatibility of invariant maps for all finite Galois extensions. That is to say, if $L/M/K$ is a tower of finite Galois extensions, then the following diagram commutes.

$$\begin{array}{ccc} H^2(G(L/K),L^\times) & \xrightarrow{inv_{L/K}} & \mathbb{Q}/\mathbb{Z} \\ {\scriptstyle inf_{L/M}}\uparrow & \nearrow_{inv_{M/K}} & \\ H^2(G(M/K),M^\times) & & \end{array}$$

By Proposition 17, we can define the total invariant map inv_K as

$$inv_K : Br(K) = H^2(\varprojlim_L G(L/K), \varinjlim_L L^\times) \simeq \varinjlim_L H^2(G(L/K),L^\times) \xrightarrow[\varinjlim_L inv_{L/K}]{\sim} \mathbb{Q}/\mathbb{Z}.$$

Up to now we have proved

Theorem 10. *We have canonical isomorphisms $inv_K : Br(K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ and*

$$inv_{L/K} : Br(L/K) \xrightarrow{\sim} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z},$$

where L/K runs over finite Galois extensions, that are compatible under inflation maps

$$inf_{L'/L} : H^2(G(L/K),L^\times) \to H^2(G(L'/K),L'^\times)$$

where $L'/L/K$ denotes any tower of finite Galois extensions.

Remark 14. The invariant map inv_K depends only on the Frobenius $\sigma_K \in G(K^{unr}/K)$, which is always chosen to be the arithmetic one in this material.

Furthermore, letting K vary, we can study the compatibility among inv_K. Suppose $L/K'/K$ is a tower of finite unramified extensions. We have the following commutative diagram

$$\begin{array}{ccccccc} inv_{L/K} : H^2(G(L/K),L^\times) & \xrightarrow{\sim} & H^2(G(L/K),\mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G(L/K),\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\iota_{\sigma_K}} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle res} & & \downarrow{\scriptstyle res} & & \downarrow{\scriptstyle res} & & \downarrow{\scriptstyle q} \\ inv_{L/K'} : H^2(G(L/K'),L^\times) & \xrightarrow{\sim} & H^2(G(L/K'),\mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G(L/K'),\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\iota_{\sigma_{K'}}} & \mathbb{Q}/\mathbb{Z} \end{array}$$

where $\sigma_{K'}, \sigma_K$ denote arithmetic Frobenius over K', K respectively, with $\sigma_{K'} = \sigma_K^{[K':K]}$ in $Gal(L/K)$, and q is multiplication by $[K' : K]$. In fact, if χ_0 is the generator of $H^1(G(L/K), \mathbb{Q}/\mathbb{Z})$ such that $\chi_0(\sigma_K) = \frac{1}{[L:K]}$, then we have $res(\chi_0)(\sigma_{K'}) = \chi_0(\sigma_{K'}) = [K' : K]\frac{1}{[L:K]}$.

Therefore, if $L/K'/K$ is any tower of finite extensions with L/K Galois, K'/K separable, then the following diagram commutes

$$\begin{array}{ccc} H^2(G(L/K), L^\times) & \xrightarrow{inv_{L/K}} & \mathbb{Q}/\mathbb{Z} \\ \downarrow res & & \downarrow q \\ H^2(G(L/K'), L^\times) & \xrightarrow{inv_{L/K'}} & \mathbb{Q}/\mathbb{Z} \end{array},$$

where q denotes multiplication by $[K' : K]$. Letting $L\,(\supseteq K')$ ranges over all Galois extensions over K, the above argument proves

Theorem 11. *Suppose K'/K is a finite separable extension of nonarchimedean local fields. Then the following diagram commutes.*

$$\begin{array}{ccc} Br(K) & \xrightarrow{inv_K} & \mathbb{Q}/\mathbb{Z} \\ \downarrow res & & \downarrow q \\ Br(K') & \xrightarrow{inv_{K'}} & \mathbb{Q}/\mathbb{Z} \end{array},$$

where q denotes multiplication by $[K' : K]$.

6.2 The Fundamental Class and Norm Limitation

In this subsection, K denotes a nonarchimedean local field.

Definition 21. Suppose L/K is a finite Galois extension of, we call the element $u_{L/K} \in Br(L/K)$ that satisfies $inv_{L/K}(u_{L/K}) = \frac{1}{[L:K]}$ the fundamental class of L/K.

If $L/K'/K$ is a tower of finite extensions with L/K Galois and K'/K separable, then by the previous subsection we have

$$res(u_{L/K}) = u_{L/K'}.$$

Note that $cor \circ res$ is multiplication by $[K' : K]$ (Exercise 6), we obtain

$$cor(u_{L/K'}) = [K' : K]u_{L/K}.$$

To establish the artin map in a purely cohomological way, recall Tate's vanishing theorem. With a few efforts we have its corollary that *if G is a finite group, C a G-module with the property*

$$\begin{cases} H^1(H, C) = 0 \\ H^2(H, C) \simeq \frac{1}{\#H}\mathbb{Z}/\mathbb{Z} \end{cases}, \quad \forall H \leq G, \tag{3}$$

then there are isomorphisms

$$\begin{array}{c} H_T^i(G, \mathbb{Z}) \xrightarrow[\cup u]{\sim} H_T^{i+2}(G, C) \\ \phi \longmapsto \phi \cup u \end{array}$$

for all $i \in \mathbb{Z}$, depending only on the choice of the generator u of $H^2(G, C)$. Combined with Hilbert 90 and Theorem 9, this immediately proves

Theorem 12. *Suppose L/K is a finite Galois extension, $i \in \mathbb{Z}$. The homomorphism*

$$\begin{aligned} H_T^r(G(L/K),\mathbb{Z}) &\longrightarrow H_T^{r+2}(G(L/K),L^\times) \\ x &\longmapsto x \cup u_{L/K} \end{aligned}$$

is an isomorphism. In particular, when $i=-2$, this isomorphism becomes

$$G(L/K)^{ab} \xrightarrow{\sim} K^\times/N_{L/K}(L^\times). \tag{4}$$

Proof. The $G(L/K)$-module $L^\times$ indeed satisfies (3). When $i=-2$, we have

$$H_T^{-2}(G(L/K),\mathbb{Z}) := H_1(G(L/K),\mathbb{Z}) \simeq G(L/K)^{ab}.$$

Hence, the isomorphism $\cup u_{L/K}$ on $H_T^{-2}(G(L/K,\mathbb{Z}))$ becomes $G(L/K)^{ab} \xrightarrow{\sim} K^\times/N_{L/K}(L^\times)$. □

Denote the inverse of the map (4) by $\psi_{L/K}$, inducing the artin map $\psi_K : K^\times \to G(K^{ab}/K)$ of K. By cohomological calculation, we can prove $\psi_K(\pi)|_{K^{unr}} = \sigma_K$, the arithmetic Frobenius of K. From Theorem 12, we see that the norm group of a finite Galois extension L/K depends only on its maximal abelian subextension. In fact, we have

Theorem 13. *Suppose L/K is a finite separable extension. Let M be the largest abelian extension of K contained in L. Then $N_{L/K}(L^\times) = N_{M/K}(M^\times)$.*

Proof. Clearly we have $N_{L/K}(L^\times) \subseteq N_{M/K}(M^\times)$. If L/K is Galois, we have

$$K^\times/N_{L/K}(L^\times) \simeq G(L/K)^{ab} = G(M/K) \simeq K^\times/N_{M/K}(M^\times)$$

Therefore $N_{L/K}(L^\times)$ and $N_{M/K}(M^\times)$ have the same index in $K^\times$, thus $N_{L/K}(L^\times) = N_{M/K}(M^\times)$. If L/K is not Galois, let L' be its Galois closure. For any $a \in N_{M/K}(M^\times) = Ker(\psi_{M/K})$, we need to prove $a \in N_{L/K}(L^\times)$. Consider the following commutative diagram

$$\begin{array}{ccccc} L^\times & \xrightarrow{\psi_{L'/L}} & G(L'/L)^{ab} & \xrightarrow{\sim} & H_1(G(L'/L),\mathbb{Z}) \\ \downarrow{\scriptstyle N_{L/K}} & & & & \downarrow{\scriptstyle cor} \\ K^\times & \xrightarrow{\psi_{L'/K}} & G(L'/K)^{ab} & \xrightarrow{\sim} & H_1(G(L'/K),\mathbb{Z}) \\ & \searrow^{\psi_{M/K}} & & & \downarrow{\scriptstyle coinf} \\ & & G(M/K) & \xrightarrow{\sim} & H_1(G(M/K),\mathbb{Z}) \\ & & & & \downarrow \\ & & & & 0 \end{array}$$

Since the right vertical sequence is exact, and $\psi_{L'/L}$ is surjective, by chasing the diagram we can find $b \in L^\times$ such that $N_{L/K}(b)^{-1}a \in Ker(\psi_{L'/K}) = N_{L'/K}(L'^\times)$, thus $a \in N_{L/K}(b)N_{L'/K}(L'^\times) \subseteq N_{L/K}(L^\times)$. □

Theorem 13 is referred to as norm limitation theorem, in the sense that there is no hope of classifying all (non-abelian) extensions of K by their norm groups.

6.3 Local Existence

Let K be a nonarchimedean local field, π a uniformizer.

Recall what we did in Section 2, 4, and Subsection 1, 2 of Section 6. We have discussed local artin reciprocity, which explains the abelian extensions via arithmetic information in $K^\times$ and gives rise to the notion of norm groups. The previous subsection have seen the fact that we cannot expect to classify non-abelian extensions by looking only at norm groups. If we focus on abelian extensions, it is trivial that if two finite abelian extensions $L/K, L'/K$ share the same norm group N, then they share the same Galois group, therefore $L = L'$. This indicates that a finite abelian extension is uniquely determined by its norm group.

Note that every norm group is of finite index and open in $K^\times$. To finish the proof of local class field theory, we need to study whether such a subgroup of $K^\times$ is always a norm group.

Definition 22. For a subgroup N of $K^\times$, if L is an abelian extension of K such that $N = N_{L/K}(L^\times)$, we call L the (unique) class field of N.

Lemma 6. *Suppose L_n is the field of π^n-division points over K. Then we have $U_K^{(n)} \subseteq N_{L_n/K}(L_n^\times)$.*

Proof. By the Lubin-Tate theory, we know that $G(L_n/K) \simeq Aut_{\mathcal{O}_K}(\mathcal{O}_K/\pi^n)$ (Theorem 8). Fix any Lubin-Tate polynomial e for π. For every element $u \in U_K^{(n)}$, $\psi_K(u) = [u^{-1}]_e$, which is equivalent to multiplication by u^{-1} on $\mathcal{O}_K/\pi^n$, which is trivial since $u^{-1} = 1 + \pi^n a$ for some $a \in \mathcal{O}_K$. Therefore by local artin reciprocity we have $U_K^{(n)} \subseteq N_{L_n/K}(L_n^\times)$. □

Theorem 14. *For any finite-index open subgroup N of $K^\times$, the class field of N uniquely exists.*

Proof. Decompose $K^\times$ as $K^\times = \mathcal{O}_K^\times \times \pi^{\mathbb{Z}}$. Then there exists positive integers n, m such that $N_{n,m} := U_K^{(n)} \times \pi^{m\mathbb{Z}} \subseteq N$. Let $L_{n,m} = L_n K_m$, where $K_m \subseteq K^{unr}$ denotes the unique unramified extension over K of degree m. We have π^m acting trivially on L_n by Lubin-Tate theory, acting trivially on K_m as $Frob_{K_m/K}^m = 1$. Therefore By Lemma 6, we have $U_K^{(n)} \times \pi^{m\mathbb{Z}} \subseteq N_{L_{n,m}/K}(L_{n,m}^\times)$. Since

$$(K^\times : N_{n,m}) = q^{n-1}(q-1)m = [L_{n,m} : K] = (K^\times : N(L_{n,m}^\times)),$$

where $q = \#(\mathcal{O}_K/\pi)$, we have $N_{n,m} = N(L_{n,m}^\times)$. Thus, the subgroup N contains a norm group, and therefore is a norm group itself. □

Proposition 29. For any two abelian extension L_1, L_2 over K, we have

$$N(L_1^\times) \cap N(L_2^\times) = N((L_1 L_2)^\times), \tag{5}$$

$$N(L_1^\times) N(L_2^\times) = N((L_1 \cap L_2)^\times), \tag{6}$$

$$N(L_1^\times) \subseteq N(L_2^\times) \iff L_1 \supseteq L_2. \tag{7}$$

Proof. For $a \in K^\times$, $a \in N(L_1^\times) \cap N(L_2^\times)$ if and only if $\psi_K(a)$ act trivially on L_1, L_2, if and only if $a \in N((L_1 L_2)^\times)$. This proves (5). Hence we have

$$\begin{aligned}(N(L_1^\times)N(L_2^\times) : N(L_1^\times)) &= (N(L_2^\times) : N((L_1 L_2)^\times)) \\ &= [L_1 L_2 : L_2] \\ &= [L_1 : L_1 \cap L_2] \\ &= (N((L_1 \cap L_2)^\times) : N(L_1^\times)).\end{aligned}$$

With the trivial fact that $N(L_1^\times)N(L_2^\times) \subseteq N((L_1 \cap L_2)^\times)$, this proves (6). To prove the nontrivial part " $\Longrightarrow$ " of (7), note that (5) gives $N((L_1L_2)^\times) = N(L_1^\times)$, and therefore they corresponds to the same class field $L_1L_2 = L_1$, completing the proof. $\square$

As a special case of Theorem 14, if the subgroup N has index n coprime to the characteristic of K (including the case when $charK = 0$), we can prove it without reliance on local artin reciprocity. In fact, it suffices to show that $(K^\times)^n$ contains a group of norms. We may assume that K contains the group $\mu(n)$ of n-th roots of 1. For if it does not, put $K_1 = K(\mu(n))$. If $(K_1^\times)^n$ contains $N_{L/K_1}(L^\times)$ for some Galois extension L/K_1, then

$$N_{L/K}(L^\times) = N_{K_1/K}N_{L/K_1}(L^\times) \subseteq N_{K_1/K}(K_1^\times)^n \subseteq (K^\times)^n.$$

Now let $L_n = K((K^\times)^{1/n})$ be the maximal abelian extension of exponent n, then $(K^\times)^n = N_{L_n/K}(L_n^\times)$ (See Example 9), completing the proof.

For the case when $charK$ divides the index of the subgroup, it is possible to do without Lubin-Tate theory, at the expense of *ad hoc* arguments. In abstract formulation, we extract the properties that artin maps satisfy as axioms, establishing the notion of class formation, which can deal with both the local case and the global case.

References

[1] Jürgen Neukirch, Algebraic Number Theory, Springer-Verlag, 1999.

[2] Andrew Sutherland, Class Field Theory: Ray Class Groups and Ray Class Fields, 2021.

[3] Andrew Sutherland, The Main Theorems of Global Class Field Theory, 2021.

[4] Jean-Pierre Serre, Galois Cohomology, Springer-Verlag, 2002.

[5] Jürgen Neukirch and Alexander Schmidt and Kay Wingberg, Cohomology of Number Fields, 2nd Edition, Springer, 2008.

[6] David S. Dummit and Richard M. Foote, Abstract algebra, 3rd Edition, John Wiley and Sons, Inc. 2004.

[7] J.S. Milne, Class Field Theory, Version 4.03, 2020

[8] Serge Lang, Algebra, Graduate Texts in Mathematics, 211, 3rd Edition, Springer, 2002.

[9] Andrew Sutherland, Local Class Field Theory, 2021.

[10] Yiwen Ding, Number Theory II.

[11] Weibel, Charles A. An Introduction to Homological Algebra. Vol. 38 of Cambridge Studies in Advanced Mathematics. Cambridge: Cambridge University Press, 1994.

[12] John Tate, The Higher Dimensional Cohomology Groups of Class Field Theory, Annals of Mathematics, Vol. 52, No. 2, 1952.

[13] Andrew Sutherland, Lubin-Tate Formal Groups, 2018.