Local Class Field Theory

Pan Yan

Summer 2015

These are notes for a reading course with D. Wright on Local Class Field Theory in Summer 2015. The notes are prepared and written by Pan Yan (pyan@math.okstate.edu). If you notice any mistakes or have any comments, please let me know.

Contents

1 Introduction

1.1 Outline of the course

Group Cohomology – Chapter IV of [CF67] (this will take about 2-3 weeks);
Profinite Groups – Chapter V of [CF67] (this will take about 2 weeks);
Local Class Field Theory – Chapter VI of [CF67] (this will take the rest of the summer semester).

1.2 References

The main reference is *Algebraic Number Theory* by Cassels & Fröhlich [CF67]. Other references include [ANT], [Cas86], [FT91], [LT65], [Mil13], [Neu86], [Ser80], [Sha].

Note: Errata for Cassels & Fröhlich [CF67] can be found at `http://wwwf.imperial.ac.uk/~buzzard/errata.pdf` (maintained by Kevin Buzzard).

1.3 Goals of the course

Class Field Theory is the study of abelian extensions of (local or global) fields. In the case of Local Class Field Theory, we are mainly interested in abelian extensions of nonarchimedean local fields. Specifically, given a nonarchimedean local field K, we want to describe all finite abelian extensions of K totally in terms of the arithmetic of the base field K.

To this end, we want to understand group cohomology (especially Tate cohomology for finite groups and Tate's Theorem), inverse limits and profinite groups, direct limits, cohomology of profinite groups and Galois cohomology, the statements and proofs of Local Reciprocity Law and Local Existence Theorem.

2 Group Cohomology

2.1 Group rings

Definition 2.1.1. Let G be a group, R a commutative ring with identity. The *group ring* $R[G]$ is the set of all formal finite sums $\sum_{g\in G} a_g g$ with each $a_g \in R$, i.e.,

$$\begin{aligned} R[G] &= \left\{ \sum_{g\in G} a_g g \mid a_g \in R, \text{ almost all } a_g = 0 \right\} \\ &= \left\{ \sum_{g\in G} a_g g \mid a_g \in R, \text{ only finitely many } a_g \neq 0 \right\}. \end{aligned}$$

The addition is defined as

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

and the multiplication is the involution

$$\left(\sum_{g\in G} a_g g \right) \left(\sum_{g\in G} b_g g \right) = \sum_{g,h\in G} (a_g b_h gh) = \sum_{g\in G} \left(a_{gh^{-1}} b_h \right) g.$$

In this course we are mainly interested in the integral group ring

$$\mathbb{Z}[G] = \left\{ \sum_{g\in G} a_g g \mid a_g \in \mathbb{Z}, \text{ almost all } a_g = 0 \right\}.$$

2.2 G-modules

From now on G always means a group, unless otherwise indicated.

Definition 2.2.1. A (left) *G-module* is an abelian group A together with a G-action on A (i.e., a map $G \times A \to A$ defined by $(g, a) \mapsto g \cdot a$) such that
(i) $1 \cdot a = a, \forall a \in A$;
(ii) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a, \forall a \in A, g_1, g_2 \in G$;
(iii) $g \cdot (a_1 + a_2) = g \cdot a_1 + g \cdot a_2, \forall a_1, a_2 \in A, g \in G$.

Remark 2.2.2. *(i) A right G-module is defined similarly by replacing the above G-action with $A \times G \to A$ defined by $(a, g) \mapsto g^{-1} a$.*

(ii) We will assume all G-modules are left G-modules unless otherwise indicated.

(iii) G-modules are the same as $\mathbb{Z}[G]$-modules.

Definition 2.2.3. A *homomorphism* $\varphi : A \to B$ of G-modules is a homomorphism of abelian groups such that $\varphi(ga) = g\varphi(a)$ for all $a \in A, g \in G$ (hence it is compatible with the G-action). The group of G-module homomorphisms is denoted as $\mathrm{Hom}_G(A, B) = \mathrm{Hom}_{\mathbb{Z}[G]}(A, B)$.

A G-module homomorphism $\varphi : A \to B$ makes the following diagram commutative.

$$\begin{array}{ccc} A & \xrightarrow{G-\text{action}} & A \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi} \\ B & \xrightarrow{G-\text{action}} & B \end{array}$$

If A, B are G-modules, we denote the group of all abelian group homomorphisms $A \to B$ as $\mathrm{Hom}(A, B)$. Note that $\mathrm{Hom}(A, B)$ actually has a G-module structure: if $\varphi \in \mathrm{Hom}(A, B)$, we can define the map

$$\begin{aligned} G \times \mathrm{Hom}(A, B) &\to \mathrm{Hom}(A, B) \\ g \cdot (\varphi : A \to B) &\mapsto \begin{pmatrix} A \to B \\ a \mapsto g\varphi(g^{-1}a) \end{pmatrix} \end{aligned}$$

which makes $\mathrm{Hom}(A, B)$ as a G-module.

Definition 2.2.4. A G-module A is *trivial* if $g \cdot a = a$ for all $a \in A, g \in G$.

Definition 2.2.5. Let A be a G-module. The group of *G-invariants* of A, denoted as A^G, is

$$A^G = \{a \in A \mid g \cdot a = a, \forall g \in G, a \in A\}.$$

Remark 2.2.6. *(i) A^G is the maximal trivial submodule of A. Indeed, A^G is trivial, by definition. Now suppose $B \subset A$ is a trivial submodule of A. Let $b \in B$, for any $g \in G$, we have $g \cdot b = b$. So $b \in A^G$. Hence $B \subset A^G$.*

(ii) If A is a trivial G-module, then $A^G = A$.

If A, B are G-modules, then

$$\begin{aligned} \mathrm{Hom}_G(A, B) &= \{\varphi : A \to B \mid \varphi(ga) = g\varphi(a), \forall g \in G, a \in A\}, \\ (\mathrm{Hom}(A, B))^G &= \{\varphi : A \to B \mid \varphi(a) = g \cdot \varphi(a) = g\varphi(g^{-1}a), \forall g \in G, a \in A\}. \end{aligned}$$

Hence

$$\mathrm{Hom}_G(A, B) = (\mathrm{Hom}(A, B))^G.$$

So

$$\mathrm{Hom}_G(\mathbb{Z}, A) = (\mathrm{Hom}(\mathbb{Z}, A))^G \cong A^G.$$

Since the covariant functor Hom is left exact, it follows that A^G is also a covariant left exact functor. More specifically, if $0 \to A \to B \to C$ is an exact sequence of G-modules, then $0 \to A^G \to B^G \to C^G$ is an exact sequence of abelian groups. The i-th cohomology group $H^i(G, A)$ of G with coefficients in A can be defined as the i-th derived functor on A of the functor of G-invariants. Alternatively, we give more specific definitions in the following two sections.

2.3 Group cohomology via cochains

Definition 2.3.1. Let A be a G-module, and $i \geq 1$.

(i) The group of *i-cochains* of G with coefficients in A, denoted as $C^i(G, A)$, is the set of functions from G^i to A, i.e., $C^i(G, A) = \{\varphi : G^i \to A\}$.

(ii) The *i-th differential* $d^i = d^i_A : C^i(G, A) \to C^{i+1}(G, A)$ is the map

$$\begin{aligned} d^i(\varphi)(g_0, g_1, \cdots, g_i) =& g_0\varphi(g_1, \cdots, g_i) + \sum_{j=1}^{i}(-1)^j\varphi(g_0, \cdots, g_{j-2}, g_{j-1}g_j, \cdots, g_i) \\ &+ (-1)^{i+1}\varphi(g_0, \cdots, g_{i-1}). \end{aligned}$$

Remark 2.3.2. $C^0(G, A) = \{\varphi : G^0 \to A\} = \{\varphi : \{p\} \to A\} \cong A$.

Lemma 2.3.3. *For any $i \geq 0$, we have $d^{i+1} \circ d^i = 0$. So $(C^i(G, A), d^i)$ is a cochain complex*

$$0 \longrightarrow C^0(G, A) \xrightarrow{d^0} C^1(G, A) \xrightarrow{d^1} C^2(G, A) \longrightarrow \cdots .$$

Definition 2.3.4. Let $i \geq 0$.

(i) The group $Z^i(G, A) = \ker d^i$ is the group of *i-cocycles* of G with coefficients in A.

(ii) The group $B^0(G, A) = 0, B^i(G, A) = \mathrm{im}d^{i-1}$ $(i \geq 1)$ is the group of *i-coboundaries* of G with coefficients in A.

Remark 2.3.5. $B^i(G, A) \subset Z^i(G, A)$ *since* $d^i \circ d^{i-1} = 0$.

Definition 2.3.6. The *i-th cohomology group* of G with coefficients in A is defined as

$$H^i(G, A) = \frac{Z^i(G, A)}{B^i(G, A)}.$$

Remark 2.3.7. *The cohomology groups measure how far the cochain complex $(C^i(G, A), d^i)$ is from being exact.*

Here are some examples of cohomology groups of low degrees.

Lemma 2.3.8. *(i)* $H^0(G,A) = A^G$.

(ii)

$$Z^1(G,A) = \{\varphi : G \to A \mid \varphi(gh) = g\varphi(h) + \varphi(g), \forall g,h \in G\}.$$
$$B^1(G,A) = \{\varphi : G \to A \mid \exists a \in A \text{ such that } \varphi(g) = ga - a, \forall g \in G\}.$$

(Elements in $Z^1(G,A)$ are called crossed homomorphism.)

(iii) If A is a trivial G-module, then $H^1(G,A) = \mathrm{Hom}(G,A)$.

Proof. (i) $H^0(G,A) = Z^0(G,A)/B^0(G,A) = Z^0(G,A)$ since $B^0(G,A) = 0$ by definition. $Z^0(G,A) = \ker d^0$, where $d^0 : C^0(G,A) = A \to C^1(G,A)$ is defined by $d^0(a)(g) = ga - a$. So $\ker d^0 = \{a \in A \mid ga - a = 0, \forall g \in G\} = A^G$. Hence $H^0(G,A) = A^G$.

(ii) By definition,

$$B^1(G,A) = \text{ im } d^0 = \{\varphi : G \to A \mid \exists a \in A \text{ such that } \varphi(g) = ga - a, \forall g \in G\}.$$

$Z^1(G,A) = \ker d^1$, where $d^1 : C^1(G,A) \to C^2(G,A)$ is defined by

$$d^1(\varphi)(g,h) = g\varphi(h) - \varphi(gh) + \varphi(g), \text{ where } (g,h) \in G^2.$$

Hence

$$\begin{aligned} Z^1(G,A) &= \{\varphi : G \to A \mid g\varphi(h) - \varphi(gh) + \varphi(g) = 0, \forall g,h \in G\} \\ &= \{\varphi : G \to A \mid \varphi(gh) = g\varphi(h) + \varphi(g), \forall g,h \in G\}. \end{aligned}$$

(iii) If A is a trivial G-module, then

$$\begin{aligned} Z^1(G,A) &= \{\varphi : G \to A \mid \varphi(gh) = g\varphi(h) + \varphi(g), \forall g,h \in G\} \\ &= \{\varphi : G \to A \mid \varphi(gh) = \varphi(h) + \varphi(g), \forall g,h \in G\} \\ &= \mathrm{Hom}(G,A). \end{aligned}$$

On the other hand, $B^1(G,A) = 0$ since $ga - a = 0$ for any $g \in G, a \in A$. Hence, $H^1(G,A) = Z^1(G,A)/B^1(G,A) = \mathrm{Hom}(G,A)$. □

We can also compute 2-cocycle and 2-coboundary.

$$\begin{aligned} B^2(G,A) = \text{ im } d^1 = \{\varphi : G^2 \to A \mid \exists \varphi_0 : G \to A \text{ such that} \\ \varphi(g,h) = g\varphi_0(h) - \varphi_0(gh) + \varphi_0(g), \forall g,h \in G\}. \end{aligned}$$

$d^2 : C^2(G,A) \to C^3(G,A)$ is defined by

$$d^2(\varphi)(g_0,g_1,g_2) = g_0\varphi(g_1,g_2) - \varphi(g_0g_1,g_2) + \varphi(g_0,g_1g_2) - \varphi(g_0,g_1).$$

So

$$Z^2(G,A) = \{\varphi : G^2 \to A \mid g_0\varphi(g_1,g_2) - \varphi(g_0g_1,g_2) + \varphi(g_0,g_1g_2) - \varphi(g_0,g_1) = 0, \forall g_0,g_1,g_2 \in G\}.$$

Such functions in $Z^2(G,A)$ are called *factor systems*.

Lemma 2.3.9. *If $\alpha : A \to B$ is a G-module homomorphism, then for each $i \geq 0$, there is an induced homomorphism of groups*

$$\begin{aligned} \alpha^i : C^i(G, A) &\to C^i(G, B) \\ f &\mapsto \alpha \circ f \end{aligned}$$

which is compatible with the differentials, i.e.,

$$d_B^i \circ \alpha^i = \alpha^{i+1} \circ d_A^i.$$

Proof. We only need to check the compatibility.

$$\begin{aligned} d_B^i(\alpha \circ f)(g_0, \cdots, g_i) =& g_0 \cdot (\alpha \circ f)(g_1, \cdots, g_i) + \sum_{j=1}^{i} (-1)^i (\alpha \circ f)(g_0, \cdots, g_{j-1}g_j, \cdots, g_i) \\ &+ (-1)^{i+1} (\alpha \circ f)(g_0, \cdots, g_{i-1}) \\ =& \alpha(g_0 f(g_1, \cdots, g_i) + \sum_{j=1}^{i} (-1)^j f(g_0, \cdots, g_{j-1}g_j, \cdots, g_i) \\ &+ (-1)^{i+1} f(g_0, \cdots, g_{i-1})) \\ =& \alpha \circ d_A^i(g_0, \cdots, g_i). \end{aligned}$$

□

Corollary 2.3.10. *If $\alpha : A \to B$ is a G-module homomorphism, then there are induced maps*

$$\alpha^* : H^i(G, A) \to H^i(G, B)$$

on cohomology. (Here we are omitting the superscripts.)

Actually $C^i(G, \cdot)$ is an exact functor of G-modules.

Lemma 2.3.11. *Suppose*

$$0 \longrightarrow A \xrightarrow{\iota} B \xrightarrow{\pi} C \longrightarrow 0$$

is a short exact sequence of G-modules. Then the resulting sequence

$$0 \longrightarrow C^i(G, A) \xrightarrow{\iota^i} C^i(G, B) \xrightarrow{\pi^i} C^i(G, C) \longrightarrow 0$$

is exact.

Proof. First, we prove the injectivity of ι^i. Suppose $\iota^i(f) = \iota \circ f = 0$, then $\iota(f(g_1, \cdots, g_i)) = 0$ for any $(g_1, \cdots, g_i) \in G^i$. So $f(g_1, \cdots, g_i) = 0$ for any $(g_1, \cdots, g_i) \in G^i$ since ι is injective. Hence $f = 0$.

Second, we prove that $\operatorname{im} \iota^i \subset \ker \pi^i$. Let $f \in \operatorname{im} \iota^i$, then there exists $f_0 \in C^i(G, A)$ such that $f = \iota \circ f_0$. Then $\pi^i(f) = \pi \circ f = \pi \circ (\iota \circ f_0) = (\pi \circ \iota) \circ f_0 = 0$. So $f \in \ker \pi^i$ and hence $\operatorname{im} \iota^i \subset \ker \pi^i$.

Third, we prove that $\ker \pi^i \subset \operatorname{im} \iota^i$. Let $f \in \ker \pi^i$, $(g_1, \cdots, g_i) \in G^i$. Then $\pi \circ f(g_1, \cdots, g_i) = 0$. So $f(g_1, \cdots, g_i) \in \ker \pi = \operatorname{im} \iota$. So there exists $a \in A$ such that $f(g_1, \cdots, g_i) = \iota(a)$. For every $(g_1, \cdots, g_i) \in G^i$ and the corresponding $a \in A$, define $f_0 \in C^i(G, A)$ such that $f_0(g_1, \cdots, g_i) = a$. Then

$$f(g_1, \cdots, g_i) = \iota(a) = \iota \circ f_0(g_1, \cdots, g_i)$$

and hence $f = \iota \circ f_0 = \iota^i(f_0)$. Hence $f \in \operatorname{im} \iota^i$.

Finally, we prove the surjectivity of π^i. Let $f \in C^i(G, C)$, $(g_1, \cdots, g_i) \in G^i$. Then $f(g_1, \cdots, g_i) \in C$. So there exists $b \in B$ such that $f(g_1, \cdots, g_i) = \pi(b)$ by the surjectivity of π. For every $(g_1, \cdots, g_i) \in G^i$ and the corresponding $b \in B$, define $f_0 \in C^i(G, B)$ such that $f_0(g_1, \cdots, g_i) = b$. Then

$$f(g_1, \cdots, g_i) = \pi(b) = \pi \circ f_0(g_1, \cdots, g_i)$$

and hence $f = \pi \circ f_0 = \pi^i(f_0)$. □

Here is the main theorem of this section.

Theorem 2.3.12. *Suppose that*

$$0 \longrightarrow A \xrightarrow{\iota} B \xrightarrow{\pi} C \longrightarrow 0$$

is a short exact sequence of G-modules. Then there exists a long exact sequence of abelian groups

$$0 \longrightarrow H^0(G, A) \xrightarrow{\iota^*} H^0(G, B) \xrightarrow{\pi^*} H^0(G, C) \xrightarrow{\delta^0} H^1(G, A) \longrightarrow \cdots .$$

Proof. Consider the following diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C^i(G, A) & \xrightarrow{\iota} & C^i(G, B) & \xrightarrow{\pi} & C^i(G, C) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d_A^i} & & \downarrow{\scriptstyle d_B^i} & & \downarrow{\scriptstyle d_C^i} & & \\ 0 & \longrightarrow & C^{i+1}(G, A) & \xrightarrow{\iota} & C^{i+1}(G, B) & \xrightarrow{\pi} & C^{i+1}(G, C) & \longrightarrow & 0 \end{array}$$

for $i \geq 0$. We claim that the following diagram is commutative with exact rows.

$$\begin{array}{ccccccc} \frac{C^i(G,A)}{B^i(G,A)} & \xrightarrow{\iota} & \frac{C^i(G,B)}{B^i(G,B)} & \xrightarrow{\pi} & \frac{C^i(G,C)}{B^i(G,C)} & \longrightarrow & 0 \\ \downarrow{\scriptstyle d_A^i} & & \downarrow{\scriptstyle d_B^i} & & \downarrow{\scriptstyle d_C^i} & & \\ 0 \longrightarrow Z^{i+1}(G,A) & \xrightarrow{\iota} & Z^{i+1}(G,B) & \xrightarrow{\pi} & Z^{i+1}(G,C) & & \end{array}$$

Here is the proof of the claim.

First, the maps ι, π in the upper row are well-defined. For example,

$$\begin{aligned} \frac{C^i(G,A)}{B^i(G,A)} &\xrightarrow{\iota} \frac{C^i(G,B)}{B^i(G,B)} \\ f + B^i(G,A) &\mapsto \iota \circ f + B^i(G,B). \end{aligned}$$

Suppose we have $g + B^i(G,B) \in \frac{C^i(G,B)}{B^i(G,B)}$, then $g \in C^i(G,C)$, and so there exists $f \in C^i(G,B)$ such that $\pi \circ f = g$. Hence $\pi \circ (f + B^i(G,B)) = \pi \circ f + B^i(G,C) = g + B^i(G,C)$. Hence the map π in the upper row is surjective. Suppose we have $g + B^i(G,B) \in \text{im } \iota$, then there exists $f + B^i(G,A) \in \frac{C^i(G,A)}{B^i(G,A)}$ such that $\iota(f + B^i(G,A)) = \iota \circ f + B^i(G,B) = g + B^i(G,B)$. Hence $\pi(g + B^i(G,B)) = \pi \circ \iota(f + B^i(G,A)) = B^i(G,C)$ and so $g + B^i(G,C) \in \ker \pi$. Hence $\text{im } \iota \subset \ker \pi$.

Second, the maps in the lower row are also well-defined. For example,

$$\begin{aligned} Z^{i+1}(G,A) &\xrightarrow{\iota} Z^{i+1}(G,B) \\ f &\mapsto \iota \circ f. \end{aligned}$$

Suppose $f \in Z^{i+1}(G,A) = \ker d_A^{i+1}$, then $f \in C^{i+1}(G,A)$, So $\iota(f) \in C^{i+1}(G,B)$. Since $d_B^{i+1}(\iota(f)) = \iota \circ d_A^{i+1}(f) = 0$ and so $\iota \circ f \in \ker d_B^{i+1} = Z^{i+1}(G,B)$. Thus the map ι is well-defined. Similarly, π is also well-defined. Suppose $f \in \ker \iota$. Then $f \in C^{i+1}(G,A)$ and $\iota(f)(g_1, \cdots, g_{i+1}) = \iota(f(g_1, \cdots, g_{i+1})) = 0$ for any $(g_1, \cdots, g_{i+1}) \in G^{i+1}$. Hence $f(g_1, \cdots, g_{i+1}) = 0$ for any $(g_1, \cdots, g_{i+1}) \in G^{i+1}$ since $\iota : A \to B$ is injective. So ι in the lower row is injective. Now suppose $g \in \text{im } \iota$. Then there exists $f \in Z^{i+1}(G,A)$ such that $g = \iota(f)$. Then $\pi(g) = \pi \circ \iota(f) = (\pi \circ \iota)(f) = 0$. So $f \in \ker \pi$. Therefore, $\text{im } \iota \subset \ker \pi$.

Third, we need to check the column maps make sense. This is because

$$d_A^i(C^i(G,A)) \subset \ker d_A^{i+1} = Z^{i+1}(G,A),$$

and

$$d_A^i(B^i(G,A)) = d_A^i(\text{im } d_A^{i-1}) = 0.$$

Finally, we need to check the diagram is commutative. Let $f + B^i(G,A) \in \frac{C^i(G,A)}{B^i(G,A)}$. Then

$$d_B^i \circ \iota \left(f + B^i(G,A)\right) = d_B^i \left(\iota \circ f + B^i(G,B)\right) = d_B^i \left(\iota(f)\right),$$

$$\iota \circ d_A^i \left(f + B^i(G,A)\right) = \iota \left(d_A^i(f)\right).$$

$d_B^i \circ \iota = \iota \circ d_A^i$ by Lemma 2.3.9. Hence the diagram is commutative. So we have proved the claim.

Now apply the Snake Lemma to get the exact sequence

$$\ker d_A^i \to \ker d_B^i \to \ker d_C^i \to \mathrm{coker} d_A^i \to \mathrm{coker} d_B^i \to \mathrm{coker} d_C^i$$

for all $i \geq 0$. Note that

$$\ker d_A^i = \frac{Z^i(G,A)}{B^i(G,A)} = H^i(G,A),$$

$$\mathrm{coker} d_A^i = \frac{Z^{i+1}(G,A)}{\mathrm{im}\ d_A^i} = \frac{Z^{i+1}(G,A)}{B^{i+1}(G,A)} = H^{i+1}(G,A).$$

The exactness of

$$\begin{aligned} 0 \to H^0(G,A) &\to H^0(G,B) \\ a &\mapsto \iota(a) \end{aligned}$$

is obvious. So we get the long exact sequence

$$0 \longrightarrow H^0(G,A) \xrightarrow{\iota^*} H^0(G,B) \xrightarrow{\pi^*} H^0(G,C) \xrightarrow{\delta^0} H^1(G,A) \longrightarrow \cdots.$$

□

2.4 Group cohomology via projective resolutions

The cohomology groups defined in the last section can also be defined in terms of projective resolutions.

For $i \geq 0$, let G^{i+1} denote the direct product of $i+1$ copies of G. $\mathbb{Z}[G^{i+1}]$ can be viewed as a G-module with the left action

$$g \cdot (g_0, g_1, \cdots, g_i) = (gg_0, gg_1, \cdots, gg_i).$$

Definition 2.4.1. The *standard resolution* of $\mathbb{Z}$ by G-modules is a sequence of G-module homomorphisms

$$\cdots \longrightarrow \mathbb{Z}[G^{i+1}] \xrightarrow{d_{i-1}} \mathbb{Z}[G^i] \longrightarrow \cdots \longrightarrow \mathbb{Z}[G^2] \xrightarrow{d_0} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

where $\epsilon : \mathbb{Z}[G] \to \mathbb{Z}$ is the *augmentation map* defined by

$$\epsilon\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} a_g$$

and

$$\begin{aligned} d_i : \mathbb{Z}[G^{i+2}] &\to \mathbb{Z}[G^{i+1}] \\ (g_0, \cdots, g_{i+1}) &\mapsto \sum_{j=0}^{i+1} (-1)^j (g_0, \cdots, g_{j-1}, g_{j+1}, \cdots, g_{i+1}) \end{aligned}$$

for each $i \geq 0$.

Remark 2.4.2. *We may use $(g_0, \cdots, \hat{g_j}, \cdots, g_i) \in G^i$ to denote the i-tuple excluding g_j.*

Lemma 2.4.3. *The standard resolution is exact.*

Proof. Let $d_{-1} = \varepsilon$. For each $i \geq 0$, we have

$$d_{i-1} \circ d_i(g_0, \cdots, g_{i+1}) = \sum_{k=0, k\neq j}^{i+1} (-1)^{j+k-s(j,k)} (g_0, \cdots, \hat{g_j}, \cdots, \hat{g_k}, \cdots, g_{i+1}),$$

where $s(j,k) = 0$ if $k < j$, $s(j,k) = 1$ if $k > j$. Each possible i-tuple appears twice in the term with opposite sign. Therefore, $d_{i-1} \circ d_i = 0$.

Next, define

$$\begin{aligned} \theta_i : \mathbb{Z}[G^{i+1}] &\to \mathbb{Z}[G^{i+2}] \\ (g_0, \cdots, g_i) &\mapsto (1, g_0, \cdots, g_i). \end{aligned}$$

Then

$$\begin{aligned} d_i \circ \theta_i(g_0, \cdots, g_i) &= (g_0, \cdots, g_i) - \sum_{j=0}^{i} (-1)^i \cdot (1, g_0, \cdots, \hat{g_j}, \cdots, g_i) \\ &= (g_0, \cdots, g_i) - \theta_{i-1} \circ d_{i-1}(g_0, \cdots, g_i). \end{aligned}$$

So

$$d_i \circ \theta_i + \theta_{i-1} \circ d_{i-1} = id_{\mathbb{Z}[G^{i+1}]}.$$

If $\alpha \in \ker d_{i-1}$, then $d_i(\theta_i(\alpha)) = \alpha$ and so $\alpha \in \text{im } d_i$. Hence $\ker d_{i-1} \subset \text{im } d_i$. To conclude, $\ker d_{i-1} = \text{im } d_i$. □

We want to consider the following complex

$$0 \longrightarrow \text{Hom}_G(\mathbb{Z}[G], A) \longrightarrow \cdots \longrightarrow \text{Hom}_G(\mathbb{Z}[G^{i+1}], A) \xrightarrow{D^i} \text{Hom}_G(\mathbb{Z}[G^{i+2}], A) \longrightarrow \cdots$$

where $D^i = D^i_A$ is defined by

$$D^i(\varphi) = \varphi \circ d_i.$$

Theorem 2.4.4. *The maps*

$$\begin{aligned}\psi^i : \mathrm{Hom}_G(\mathbb{Z}[G^{i+1}], A) &\to C^i(G, A)\\ \psi^i(\varphi)(g_1, \cdots, g_i) &= \varphi(1, g_1, g_1g_2, \cdots, g_1g_2\cdots g_i)\end{aligned}$$

are isomorphisms for all $i \geq 0$. Moreover, we have isomorphisms of complexes via

$$\psi^{i+1} \circ D^i = d^i \circ \psi^i.$$

Proof. First, we prove that ψ^i is injective. Suppose $\psi^i(\varphi) = 0$, then

$$\varphi(1, g_1, g_1g_2, \cdots, g_1g_2\cdots g_i) = 0$$

for any $g_1, \cdots, g_i \in G$. Let $h_0, \cdots, h_i \in G$ and define $g_j = h_{j-1}^{-1}h_j$ for all $1 \leq j \leq i$. Then

$$\begin{aligned}\varphi(h_0, h_1, \cdots, h_i) &= h_0\varphi(1, h_0^{-1}h_1, \cdots, h_0^{-1}h_i)\\ &= h_0 \cdot \varphi(1, g_1, \cdots, g_1\cdots g_i)\\ &= 0.\end{aligned}$$

Hence ψ^i is injective.

Second, we prove that ψ^i is also surjective. If $f \in C^i(G, A)$, define

$$\varphi(h_0, h_1, \cdots, h_i) = h_0 f(h_0^{-1}h_1, \cdots, h_{i-1}^{-1}h_i).$$

Then

$$\begin{aligned}\varphi(gh_0, gh_1, \cdots, gh_i) &= gh_0 f((gh_0)^{-1}gh_1, \cdots, (gh_{i-1})^{-1}gh_i)\\ &= gh_0 f(h_0^{-1}h_1, \cdots, h_{i-1}^{-1}h_i)\\ &= g\varphi(h_0, h_1, \cdots, h_i)\end{aligned}$$

and hence

$$\psi^i(\varphi)(h_1, \cdots, h_i) = \varphi(1, h_1, h_1h_2, \cdots, h_1h_2\cdots h_i) = f(h_1, \cdots, h_i).$$

So ψ^i is surjective. Therefore, ψ^i is an isomorphism.

Let $\varphi \in \mathrm{Hom}_G(\mathbb{Z}[G^{i+1}], A)$, $(g_1, \cdots, g_{i+1}) \in G^{i+1}$. Then

$$\begin{aligned}
&\psi^{i+1}(D^i(\varphi))(g_1, \cdots, g_{i+1}) \\
=&D^i(\varphi)(1, g_1, \cdots, g_1 \cdots g_{i+1}) \\
=&\psi \circ d_i(1, g_1, \cdots, g_1 \cdots g_{i+1}) \\
=&\sum_{j=0}^{i+1}(-1)^j \varphi(1, g_1, \cdots, \widehat{g_1 \cdots g_j}, \cdots, g_1 \cdots g_{i+1}) \\
=&\varphi(g_1, g_1 g_2, \cdots, g_1 \cdots g_{i+1}) + \sum_{j=1}^{i}(-1)^j \varphi(1, \cdots, \widehat{g_1 \cdots g_j}, \cdots, g_1 \cdots g_{i+1}) \\
&+ (-1)^{i+1}\varphi(1, g_1, \cdots, g_1 \cdots g_{i+1}) \\
=&g_1 \psi^i(\varphi)(g_2, \cdots, g_{i+1}) + \sum_{j=1}^{i}(-1)^j \psi^i(\varphi)(g_1, \cdots, g_{j-2}, g_{j-1}g_j, g_{j+1}, \cdots, g_{i+1}) \\
&+ (-1)^{i+1}\psi^i(\varphi)(g_1, \cdots, g_i) \\
=&d^i(\psi^i(\varphi))(g_1, \cdots, g_{i+1}).
\end{aligned}$$

□

Corollary 2.4.5. *The i-th cohomology group of the complex $(\mathrm{Hom}_G(\mathbb{Z}[G^{i+1}], A), D_A^i)$ is isomorphic to $H^i(G, A)$.*

Remark 2.4.6. *Actually the standard resolution is a projective resolution, this is because $\mathbb{Z}[G^{i+1}] \cong \bigoplus_{(g_1, \cdots, g_i) \in G^i} \mathbb{Z}[G](1, g_1, \cdots, g_i)$ is free and the fact that every free module is projective.*

2.5 Homology

Let A, B be G-modules. Let $A \otimes B$ denote their tensor product over $\mathbb{Z}$, and $A \otimes_G B = A \otimes_{\mathbb{Z}[G]} B$ denote their tensor product over $\mathbb{Z}[G]$. Note that $A \otimes B$ has a G-module structure via the action $g(a \otimes b) = (ga) \otimes (gb)$.

Definition 2.5.1. The *augmentation map* is the homomorphism defined by

$$\begin{aligned}
\epsilon : \mathbb{Z}[G] &\to \mathbb{Z} \\
\sum_g a_g g &\mapsto \sum_g a_g.
\end{aligned}$$

The *augmentation ideal* is $I_G = \ker \epsilon$.

Lemma 2.5.2. *I_G is equal to the ideal of $\mathbb{Z}[G]$ generated by $\{g - 1 \mid g \in G\}$.*

Proof. Clearly, $g-1 \in \ker \epsilon$ for any $g \in G$. Conversely, if $\sum_{g\in G} a_g = 0$, then $\sum_{g\in G} a_g g = \sum_{g\in G} a_g(g-1)$. So $\ker \epsilon$ is contained in the ideal generated by $\{g-1 \mid g \in G\}$. □

Definition 2.5.3. The group of *G-coinvariants* of A, denoted as A_G, is

$$A_G = A/I_G A.$$

We have an exact sequence

$$0 \longrightarrow I_G \xrightarrow{\iota} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0.$$

Since tensor product is right exact,

$$I_G \otimes_G A \xrightarrow{\iota\otimes \mathrm{id}} \mathbb{Z}[G] \otimes_G A \xrightarrow{\epsilon\otimes \mathrm{id}} \mathbb{Z} \otimes_G A \longrightarrow 0$$

is exact. Hence,

$$\mathbb{Z} \otimes_G A = \mathrm{im}(\epsilon \otimes \mathrm{id}) \cong \frac{\mathbb{Z}[G] \otimes_G A}{\ker(\epsilon \otimes \mathrm{id})} \cong \frac{A}{\mathrm{im}(\iota \otimes \mathrm{id})} \cong \frac{A}{I_G \otimes_G A} \cong \frac{A}{I_G A} = A_G.$$

Definition 2.5.4. The i-th *homology group* $H_i(G, A)$ of G with coefficients in A is defined to be the i-th homology group of the sequence

$$\cdots \longrightarrow \mathbb{Z}[G^3] \otimes_G A \xrightarrow{d_1} \mathbb{Z}[G^2] \otimes_G A \xrightarrow{d_0} \mathbb{Z}[G] \otimes_G A \xrightarrow{d_{-1}} 0$$

induced by the standard resolution. More specifically,

$$H_i(G, A) = \frac{Z_i(G, A)}{B_i(G, A)},$$

where $Z_i(G, A) = \ker d_{i-1}$ is the *i-cycle* of G with coefficients in A, and $B_i(G, A) = \mathrm{im}\ d_i$ is the *i-boundary* of G with coefficients in A.

Lemma 2.5.5. *$H_0(G, A) = A_G$ for any G-module A.*

Proof. Well,

$$Z_0(G, A) = \ker d_{-1} = \mathbb{Z}[G] \otimes_G A \cong A.$$

The map d_0 is defined by

$$d_0\left((g_0, g_1) \otimes a\right) = (g_1 - g_0)a.$$

So

$$B_0(G, A) = \mathrm{im}\ d_0 = I_G A.$$

Hence,

$$H_0(G, A) = \frac{Z_0(G, A)}{B_0(G, A)} \cong \frac{A}{I_G A} = A_G.$$

□

If $\alpha : A \to B$ is a G-module homomorphism, then there are induced maps $\alpha_* : H_i(G, A) \to H_i(G, B)$ on homology groups for each $i \geq 0$.

Theorem 2.5.6. *Suppose that*

$$0 \longrightarrow A \xrightarrow{\iota} B \xrightarrow{\pi} C \longrightarrow 0$$

is a short exact sequence of G-modules. Then there exists a long exact sequence of abelian groups

$$\cdots \longrightarrow H_1(G, C) \xrightarrow{\delta_*} H_0(G, A) \xrightarrow{\iota_*} H_0(G, B) \xrightarrow{\pi_*} H_0(G, C) \longrightarrow 0$$

where $\delta_* : H_i(G, C) \to H_{i-1}(G, A)$ is a connecting homomorphism.

Proposition 2.5.7. *Let G be a group, A be a G-module. Let $[G, G]$ be the commutator subgroup of G so that $G^{ab} = G/[G, G]$ is the largest abelian quotient of G. Then*

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

Proof. Consider the exact sequence

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0$$

of G-modules. First, we will show that $H_1(G, \mathbb{Z}[G]) = 0$. Suppose that $(g_0, g_1) \otimes g_2 \in \ker d_0 = Z_1(G, \mathbb{Z}[G])$ and $g_2 \neq 0$. Then

$$d_0\left((g_0, g_1) \otimes g_2\right) = (g_1 - g_0) \otimes g_2 = 0$$

and hence $g_0 = g_1$. So

$$d_1\left((x, g_1, y) \otimes g_2\right) = \left((g_1, y) - (x, y) + (x, g_1)\right) \otimes g_2 = (g_1, g_1) \otimes g_2$$

and hence $(g_0, g_1) \otimes g_2 \in \mathrm{im} d_1 = B_1(G, \mathbb{Z}[G])$. Hence $H_1(G, \mathbb{Z}[G]) = 0$. By Theorem 2.5.6, we have the following exact sequence

$$0 \longrightarrow H_1(G, \mathbb{Z}) \longrightarrow \frac{I_G}{I_G^2} \longrightarrow \frac{\mathbb{Z}[G]}{I_G} \to H_0(G, \mathbb{Z}) \to 0.$$

Note that the map $\frac{I_G}{I_G^2} \to \frac{\mathbb{Z}[G]}{I_G}$ is induced by $I_G \to \mathbb{Z}[G]$, hence is zero. Therefore, we have

$$H_1(G, \mathbb{Z}) \cong \frac{I_G}{I_G^2}.$$

Note that $I_G^2 = I_G \cdot I_G$ is the submodule of $\mathbb{Z}[G]$ generated by elements of the form

$$(g - 1)(g' - 1), g, g' \in G.$$

The map

$$\begin{aligned}\frac{G}{[G,G]} &\to \frac{I_G}{I_G^2}\\ g &\mapsto (g-1)+I_G^2\end{aligned}$$

is an isomorphism. Hence

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

□

2.6 Change of groups

Let $H \subset G$ be a subgroup. Suppose B is a H-module. Then we can construct a G-module $\mathrm{Hom}_H(\mathbb{Z}[G], B)$ by the G-action

$$(g \cdot \varphi)(\alpha) = \varphi(\alpha \cdot g).$$

This type of G-modules are *coinduced* from H to G.

Theorem 2.6.1 (Shapiro's Lemma)**.** *For all $i \geq 0$, we have*

$$H^i(G, \mathrm{Hom}_H(\mathbb{Z}[G], B)) \cong H^i(H, B).$$

Proof. Let P be the standard resolution of $\mathbb{Z}$ by G-modules. Define the map

$$\begin{aligned}\psi_i : \mathrm{Hom}_G\left(P_i, \mathrm{Hom}_H(\mathbb{Z}[G], B)\right) &\to \mathrm{Hom}_H(P_i, B)\\ \psi_i(\theta)(x) &\mapsto \theta(x)(1).\end{aligned}$$

If $\theta \in \ker \psi_i$, then

$$\theta(x)(g) = (g \cdot \theta(x))(1) = \theta(gx)(1) = 0$$

for all $x \in P_i, g \in G$. Hence $\theta = 0$. So ψ_i is injective. Conversely, if $\varphi \in \mathrm{Hom}_H(P_i, B)$, then define θ by $\theta(x)(g) = \varphi(gx)$, then we have $\psi_i(\theta) = \varphi$. So ψ_i is surjective. Hence ψ_i is an isomorphism. Then the result follows. □

Remark 2.6.2. *There is an analogous result for homology. We can form $\mathbb{Z}[G] \otimes_H B$ as a G-module via the G-action $g \cdot (\alpha \otimes b) = (g\alpha) \otimes b$. This type of G-modules are induced from H to G. Then we have*

$$H_i(G, \mathbb{Z}[G] \otimes_H B) \cong H_i(H, B)$$

for any $i \geq 0$.

Definition 2.6.3. We say that G-modules of the form

$$\mathbb{Z}[G] \otimes_{\mathbb{Z}} X \text{ and } \mathrm{Hom}(\mathbb{Z}[G], X)$$

where X is an abelian group, are *induced* and *coinduced* G-modules, respectively.

Theorem 2.6.4. *Suppose that A is a coinduce (resp. induced) G-module. Then we have $H^i(G, A) = 0$ (resp. $H_i(G, A) = 0$) for all $i \geq 1$.*

Proof. Let X be an abelian group such that $A = \mathrm{Hom}(\mathbb{Z}[G], X)$. By Theorem 2.6.1, we have

$$H^i(G, A) = H^i(G, \mathrm{Hom}(\mathbb{Z}[G], X)) = H^i(G, \mathrm{Hom}_{\{1\}}(\mathbb{Z}[G], X)) \cong H^i(\{1\}, X)$$

for $i \geq 1$. Since $\mathbb{Z}$ has a projective resolution of $\mathbb{Z}$ by itself, it follows that $H^i(\{1\}, X) = 0$ for $i \geq 1$. (Here is another way to show that. Suppose $\varphi : \{1\} \to X$ is a 1-cocycle, then $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) + \varphi(1)$ and hence $\varphi(1) = 0$. Let $x \in X$, then $\varphi(1) = 1 \cdot x - x$. So φ is also a 1-coboundary. Hence $H^1(\{1\}, X) = 0$. Now by the long exact sequence of cohomology groups, $H^i(\{1\}, X) = 0$ for all $i \geq 1$.) Similarly, $H_i(G, A) = 0$ for $i \geq 1$. □

Suppose $f : G' \to G$ is a homomorphism of groups, we can regard a G-module A as a G'-module via the map f under the G'-action $(g', a) \mapsto f(g')a$. There is an induced homomorphism $P' \to P$ of the standard resolution of $\mathbb{Z}$, and hence homomorphisms of the cohomology groups

$$f^* : H^i(G, A) \to H^i(G', A)$$

for any G-module A, $i \geq 0$. In particular, if $G' = H$ is a subgroup of G, and $f : H \to G$ is the embedding, then we have the *restriction homomorphisms*

$$\mathrm{Res} : H^i(G, A) \to H^i(H, A).$$

If H is a normal subgroup of G, consider $f : G \to G/H$. For any G-module A, A^H is a G/H-module via the G/H-action

$$\begin{aligned} G/H \times A^H &\to A^H \\ (g + H, a) &\mapsto (g + 1)a. \end{aligned}$$

Hence we have the homomorphism

$$H^i(G/H, A^H) \to H^i(G, A^H). \tag{2.1}$$

The *inflation homomorphisms* are the composition of (2.1) with the homomorphism induced by $A^H \to A$, i.e.,

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

Remark 2.6.5. *Similarly, for homology, if $f : G' \to G$ is a homomorphism of groups, then we have homomorphisms of homology groups*

$$f_* : H_i(G', A) \to H_i(G, A)$$

for any G-module A and $i \geq 0$. In particular, if $G' = H$ is a subgroup of G, and $f : H \to G$ is the embedding, then we have the corestriction homomorphisms

$$Cor : H_i(H, A) \to H_i(G, A).$$

Now back to cohomology, and consider the case $G' = G$, $f : G \to G$ being the inner automorphism $s \mapsto tst^{-1}$. This turns A into another G-module, denoted as A^t, and gives the homomorphism

$$H^i(G, A) \to H^i(G, A^t). \tag{2.2}$$

Now the map $\varphi : A^t \to A$ defined by $a \mapsto t^{-1}a$ is an isomorphism, and hence gives the homomorphism

$$H^i(G, A^t) \to H^i(G, A). \tag{2.3}$$

Proposition 2.6.6. *The composition of (2.2) with (2.3) is the identity map on $H^i(G, A)$.*

Before proving Proposition 2.6.6, we need a useful technique in group cohomology – *dimension shifting*.

Let A be a G-module, and let G act on $\mathrm{Hom}(\mathbb{Z}[G], A)$ by

$$(g \cdot \varphi)(a) = g\varphi(g^{-1}a).$$

We have an exact sequence

$$0 \to A \xrightarrow{\iota} \mathrm{Hom}(\mathbb{Z}[G], A) \xrightarrow{\pi} A^* \to 0 \tag{2.4}$$

where ι is defined by $\iota(a)(g) = a, \forall a \in A, g \in G$, and $A^* = \mathrm{coker}(\iota) = \mathrm{Hom}(\mathbb{Z}[G], A)/A$. Then we have

Theorem 2.6.7 (Dimension Shifting)**.** *For any $i \geq 1$, we have*

$$H^{i+1}(G, A) \cong H^i(G, A^*).$$

Proof. The exactness of (2.4) gives rise to the long exact sequence

$$\cdots \to H^i(G, \mathrm{Hom}(\mathbb{Z}[G], A)) \to H^i(G, A^*) \xrightarrow{\delta^i} H^{i+1}(G, A) \xrightarrow{\iota^*} H^{i+1}(G, \mathrm{Hom}(\mathbb{Z}[G], A)) \to \cdots$$

for $i \geq 0$. Since $\mathrm{Hom}(\mathbb{Z}[G], A)$ is coinduced, $H^i(G, \mathrm{Hom}(\mathbb{Z}[G], A)) = 0$ for all $i \geq 1$, by Theorem 2.6.4. So

$$0 \to H^i(G, A^*) \xrightarrow{\delta^i} H^{i+1}(G, A) \to 0$$

is exact, hence δ^i is both surjective and injective for all $i \geq 1$. Therefore, δ^i is an isomorphism for all $i \geq 1$ and hence

$$H^i(G, A^*) \cong H^{i+1}(G, A)$$

for all $i \geq 1$. □

Remark 2.6.8. *There is an analogous result for homology. We regard $\mathbb{Z}[G] \otimes A$ as a G-module via the G-action*

$$g \cdot (\alpha \otimes a) = g\alpha \otimes ga.$$

We have a short exact sequence

$$0 \to A_* \to \mathbb{Z}[G] \otimes A \xrightarrow{\pi} A \to 0$$

where $A_* = \ker \pi$. Then we have

$$H_{i+1}(G, A) \cong H_i(G, A_*)$$

for any $i \geq 1$.

Now we are ready to prove Proposition 2.6.6.

Proof of Proposition 2.6.6. We first verify the case $i = 0$, then use dimension shifting to prove it by induction.

For $i = 0$, we have

$$\begin{aligned} H^0(G, A^t) = (A^t)^G &= \{a \in A^t \mid g \cdot a = a, \forall g \in G\} \\ &= \{a \in A \mid tgt^{-1}a = a, \forall g \in G\} \\ &= \{a \in A \mid gt^{-1}a = t^{-1}a, \forall g \in G\} \\ &= t \cdot A^G. \end{aligned}$$

So (2.2) is just multiplication by t, and (2.3) is multiplication by t^{-1}. Hence the composition is the identity. This proved the case $i = 0$.

Now assume $i \geq 1$ and the result holds for i. By the Dimension Shifting, we have the following commutative diagram

$$\begin{array}{ccc} H^i(G, A^*) & \xrightarrow{\delta} & H^{i+1}(G, A) \\ \downarrow{\scriptstyle \sigma_i} & & \downarrow{\scriptstyle \sigma_{i+1}} \\ H^i(G, A^*) & \xrightarrow{\delta} & H^{i+1}(G, A) \end{array}$$

where σ_i, σ_{i+1} are the composition of (2.2) with (2.3), δ is an isomorphism, σ_i is the identity map by the inductive hypothesis. Hence σ_{i+1} is the identity map on $H^{i+1}(G, A)$. This completes the proof. □

Proposition 2.6.9 (The Restriction-Inflation Sequence)**.** *Let G be a group, A a G-module and H a normal subgroup of G. Then*

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

is exact.

Proof. Suppose $f : G/H \to A^H \in Z^1(G/H, A^H)$ is a 1-cocycle, then it induces a map $\text{Inf}\ (f) : G \to A$ via

$$G \to G/H \overset{f}{\to} A^H \hookrightarrow A.$$

Let $g_0, g_1 \in G$. Then

$$\begin{aligned}\text{Inf}\ (f)(g_0g_1) =& f(g_0g_1H) = f((g_0H)(g_1H)) \\ =& (g_0H)f(g_1H) + f(g_0H) \\ =& g_0f(g_1H) + f(g_0H) \ \ (\text{ since } f(g_1H) \in A^H) \\ =& g_0\text{Inf}\ (f)(g_1) + \text{Inf}\ (f)(g_0).\end{aligned}$$

So $\text{Inf}\ (f)$ is an crossed homomorphism and hence $\text{Inf}\ (f) \in Z^1(G, A)$.

Suppose $f : G/H \to A^H \in B^1(G/H, A^H)$ is a 1-coboundary, then there exists some $a \in A^H$ such that $f(gH) = gH \cdot a - a = ga - a$ for all $g \in G$. So $\text{Inf}\ (f)(g) = f(gH) = ga - a$ for all $g \in G$. Hence $\text{Inf}\ (f) \in B^1(G, A)$.

Suppose $f : G \to A \in Z^1(G, A)$ is a 1-cocycle, then

$$\begin{aligned}\text{Res}\ (f)(h_0h_1) =& f(h_0h_1) \\ =& h_0f(h_1) + f(h_0) \\ =& h_0\text{Res}\ (f)(h_1) + \text{Res}\ (f)(h_1)\end{aligned}$$

for any $h_0, h_1 \in H$. So $\text{Res}\ (f) \in Z^1(H, A)$.

Suppose $f : G \to A \in B^1(G, A)$ is a 1-coboundary, then there exists some $a \in A$ such that $\text{Res}\ (f)(h) = f(h) = ha - a$ for all $h \in H$. Hence $\text{Res}\ (f) \in B^1(H, A)$.

Now we verify the exactness. Suppose $\text{Inf}\ (f) \in B^1(G, A)$, we need to show that $f \in B^1(G/H, A^H)$. There exists some $a \in A$ such that $\text{Inf}\ (f)(g) = ga - a = f(gH)$ for all $g \in G$. In particular, $f(H) = Ha - a = 0$ and hence $a \in A^H$. Therefore, $f \in B^1(G/H, A^H)$. This proves that the inflation is injective.

Suppose $f : G/H \to A^H \in B^1(G/H, A^H)$ is a 1-coboundary. Then for any $h \in H$, we have

$$\text{Res} \circ \text{Inf}\ (f)(h) = \text{Res}\ (f(H)) = \text{Res}\ (0) = 0.$$

Hence $\text{Res} \circ \text{Inf} = 0$. □

Proposition 2.6.10. *Let G be a group, A a G-module and H a normal subgroup of G. Let $i \geq 1$ and suppose that $H^j(H, A) = 0$ for all $1 \leq j \leq i-1$. Then the sequence*

$$0 \to H^i(G/H, A^H) \overset{Inf}{\to} H^i(G, A) \overset{Res}{\to} H^i(H, A)$$

is exact.

Proof. We argue by induction via dimension shifting. We already proved the case $i = 1$. Now suppose $i \geq 2$ and suppose that the statement is true for $i-1$. We have the exact sequence of G-modules

$$0 \longrightarrow A \longrightarrow \mathrm{Hom}(\mathbb{Z}[G], A) \longrightarrow A^* \longrightarrow 0$$

where $A^* = \mathrm{Hom}(\mathbb{Z}[G], A)/A$. It is also an exact sequence of H-modules. So have have an exact sequence

$$0 \longrightarrow H^0(H, A) \longrightarrow H^0(H, \mathrm{Hom}(\mathbb{Z}[G], A)) \longrightarrow H^0(H, A^*) \longrightarrow H^1(H, A)$$

in H-cohomology by Theorem 2.3.12. Since $H^1(H, A) = 0$ and by Lemma 2.3.8, we have a short exact sequence

$$0 \longrightarrow A^H \longrightarrow (\mathrm{Hom}(\mathbb{Z}[G], A))^H \longrightarrow (A^*)^H \longrightarrow 0$$

in H-cohomology. Moreover,

$$(\mathrm{Hom}(\mathbb{Z}[G], A))^H \cong \mathrm{Hom}(\mathbb{Z}[G/H], A) \cong \mathrm{Hom}(\mathbb{Z}[G/H], A^H)$$

with the trivial H-action. Thus the connecting homomorphism

$$\delta^{i-1} : H^{i-1}(G/H, (A^*)^H) \to H^i(G/H, A^H)$$

is an isomorphism for $i \geq 2$. Now consider the following commutative diagram

$$\begin{array}{ccccc} 0 \longrightarrow & H^{i-1}(G/H, (A^*)^H) & \overset{\mathrm{Inf}}{\longrightarrow} & H^{i-1}(G, A^*) & \overset{\mathrm{Res}}{\longrightarrow} H^{i-1}(H, A^*) \\ & \downarrow{\scriptstyle \delta^{i-1}} & & \downarrow{\scriptstyle \delta^{i-1}} & \downarrow{\scriptstyle \delta^{i-1}} \\ 0 \longrightarrow & H^i(G/H, A^H) & \xrightarrow{\mathrm{Inf}} & H^i(G, A) & \xrightarrow{\mathrm{Res}} H^i(H, A) \end{array}$$

with vertical maps isomorphisms, and top row exact by inductive hypothesis. Hence the button row is also exact. This completes the proof. □

Corollary 2.6.11. *Let G be a group, A a G-module and H a normal subgroup of G. Let $i \geq 1$ and suppose that $H^j(H, A) = 0$ for all $1 \leq j \leq i-1$. Then*

$$H^j(G/H, A^H) \cong H^j(G, A)$$

for $1 \leq j \leq i-1$.

2.7 Tate cohomology

In this section we assume that G is a finite group. The *norm element* of $\mathbb{Z}[G]$ is defined as $N_G = \sum_{g\in G} g$, which defines a map

$$\begin{aligned} N = N_A = N_{G,A} : A &\to A \\ a &\mapsto \sum_{g\in G} g\cdot a \end{aligned}$$

by left multiplication on any G-module A. The image

$$\text{im } (N) = N(A) = \{\sum_{g\in G} g\cdot a \mid a\in A\}$$

is the group of *G-norms* of A.

Lemma 2.7.1. *The norm element induces a map $N^* : A_G \to A^G$.*

Proof. For any $g_0 \in G, a \in A$, we have

$$N((g_0-1)a) = \sum_{g\in G} g\cdot(g_0-1)a = \sum_{g\in G} gg_0a - \sum_{g\in G} ga = 0$$

and hence $I_GA \subset \ker N$. Moreover,

$$g_0\cdot N(a) = g_0\cdot\sum_{g\in G} ga = \sum_{g\in G} g_0ga = \sum_{g\in G} ga = N(a)$$

and hence $N(A)\subset A^G$. □

Definition 2.7.2. We define

$$\begin{aligned} \hat{H}^0(G,A) = \text{coker}(N^*) &= \frac{A^G}{N(A)}, \\ \hat{H}_0(G,A) = \ker(N^*) &= \frac{\ker(N)}{I_GA}. \end{aligned}$$

Since G is a finite group, the map

$$\begin{aligned} \text{Hom}(\mathbb{Z}[G],X) &\to \mathbb{Z}[G]\otimes X \\ \varphi &\mapsto \sum_{g\in G} g\otimes\varphi(g) \end{aligned}$$

with its inverse

$$\begin{aligned} \mathbb{Z}[G]\otimes X &\to \text{Hom}(\mathbb{Z}[G],X) \\ \sum_{g\in G} g\otimes x_g &\mapsto (\varphi : g\mapsto x_g) \end{aligned}$$

where X is an abelian group, make these two G-modules an isomorphism. Hence the notion of induced and coinduced G-modules coincide for a finite group G.

Proposition 2.7.3. *Let G be a finite group and A an induced G-module. Then $\hat{H}^0(G,A) = \hat{H}_0(G,A) = 0$.*

Proof. Let X be an abelian group such that $A = \mathbb{Z}[G] \otimes X$. Each element of A is uniquely of the form $\sum_{g\in G} g \otimes x_g$ where $x_g \in X$. Suppose $a = \sum_{g\in G} g \otimes x_g \in A^G$, then

$$g_0 \cdot a = \sum_{g\in G} g_0 g \otimes g_0 x_g = \sum_{g\in G} g_0 g \otimes x_g = a = \sum_{g\in G} g \otimes x_g$$

for any $g_0 \in G$. Hence all the x_g are equal. Hence $a = \sum_{g\in G} g \otimes x = N(1 \otimes x)$ and that $a \in N(A)$. Therefore, $A^G = N(A)$ and hence $\hat{H}^0(G,A) = 0$.

Now suppose $a = \sum_{g\in G} g \otimes x_g \in \ker(N)$, then $N\left(\sum_{g\in G} g \otimes x_g\right) = 0$. Hence $\sum_{g\in G} x_g = 0$. So

$$a = \sum_{g\in G} g \otimes x_g = \sum_{g\in G} (g-1)(1 \otimes x_g) \in I_G A.$$

So $\ker(N) \subset I_G A$ and hence $\hat{H}_0(G,A) = 0$. □

Definition 2.7.4. Let G be a finite group and A a G-module. Let $i \in \mathbb{Z}$. We define the i-th *Tate cohomology group* to be

$$\hat{H}^i(G,A) = \begin{cases} H^i(G,A), & i \geq 1, \\ \hat{H}^0(G,A), & i = 0, \\ \hat{H}_0(G,A), & i = -1, \\ H_{-i-1}(G,A), & i \leq -2. \end{cases}$$

Theorem 2.7.5. *Let G be a finite group and A an induced G-module. Then $\hat{H}^i(G,A) = 0$ for all $i \in \mathbb{Z}$.*

Proof. By Theorem 2.6.4, $H^i(G,A) = H_i(G,A) = 0$ for all $i \geq 1$. It suffices to check $\hat{H}^0(G,A)$ and $\hat{H}_0(G,A)$, which are proved in Proposition 2.7.3. □

Theorem 2.7.6 (Tate)**.** *Let G be a finite group. Suppose*

$$0 \longrightarrow A \xrightarrow{\iota} B \xrightarrow{\pi} C \longrightarrow 0$$

is a short exact sequence of G-modules. Then there exists a long exact sequence of abelian groups

$$\cdots \longrightarrow \hat{H}^i(G,A) \xrightarrow{\iota^*} \hat{H}^i(G,B) \xrightarrow{\pi^*} \hat{H}^i(G,C) \xrightarrow{\delta^i} \hat{H}^{i+1}(G,A) \longrightarrow \cdots$$

extending infinitely in both directions.

Proof. Apply the Snake Lemma to the commutative diagram

$$\begin{array}{ccccccccc}
\cdots \longrightarrow & H_1(G,C) & \longrightarrow & H_0(G,A) & \longrightarrow & H_0(G,B) & \longrightarrow & H_0(G,C) & \longrightarrow 0 \\
& \downarrow & & \downarrow{\scriptstyle N_A} & & \downarrow{\scriptstyle N_B} & & \downarrow{\scriptstyle N_C} & \downarrow \\
& 0 & \longrightarrow & H^0(G,A) & \longrightarrow & H^0(G,B) & \longrightarrow & H^0(G,C) & \longrightarrow H^1(G,A) \longrightarrow \cdots .
\end{array}$$

□

We also have dimension shifting for Tate cohomology groups. Actually the Tate cohomology groups can be shifted both up and down.

Theorem 2.7.7 (Dimension Shifting)**.** *Let G be a finite group and A a G-module. Then*

$$\hat{H}^{i+1}(G,A) \cong \hat{H}^i(G,A^*) \text{ and } \hat{H}^{i-1}(G,A) \cong \hat{H}^i(G,A_*)$$

for any $i \in \mathbb{Z}$, where $A^* = \mathrm{Hom}(\mathbb{Z}[G],A)/A$, A_* is the kernel of the map $\pi : \mathbb{Z}[G] \otimes A \to A$ defined by $\pi(g \otimes a) = a$ for $a \in A, g \in G$.

Proof. This follows from Theorem 2.6.7 and Remark 2.6.8. □

Let H be a subgroup of G. Recall that we have defined the restriction homomorphisms

$$\mathrm{Res} : H^i(G,A) \to H^i(H,A)$$

for all $i \geq 0$. Hence it is defined for the Tate cohomology groups $\hat{H}^i(G,A)$ for all $i \geq 1$. By dimension shifting via the following commutative diagram

$$\begin{array}{ccc}
\hat{H}^{i-1}(G,A) & \xrightarrow{\mathrm{Res}} & \hat{H}^{i-1}(H,A) \\
\downarrow & & \downarrow \\
\hat{H}^i(G,A_*) & \xrightarrow{\mathrm{Res}} & \hat{H}^i(H,A_*)
\end{array}$$

it is defined for $\hat{H}^i(G,A)$ for all $i \in \mathbb{Z}$.

Similarly, we have defined the corestriction homomorphisms

$$\mathrm{Cor} : H^i(H,A) \to H^i(G,A)$$

for all $i \geq 0$. It is defined for all the Tate cohomology groups $\hat{H}^i(G,A)$ by dimension shifting.

Definition 2.7.8. We define

$$\begin{aligned}
\mathrm{Res} : H_0(G,A) &\to H_0(H,A) \\
a &\mapsto \sum_{\overline{g} \in G/H} g^{-1} \cdot \tilde{a},
\end{aligned}$$

where $a \in A_G$, $\tilde{a} \in A^H$ is any lift of a, g is any coset representative of $\overline{g} \in G/H$. We define

$$\begin{aligned} \mathrm{Cor} : H^0(H, A) &\to H^0(G, A) \\ a &\mapsto \sum_{\overline{g} \in G/H} g \cdot a. \end{aligned}$$

Proposition 2.7.9. *Let G be a finite group, H a subgroup of G. There are maps*

$$Res : H_i(G, A) \to H_i(H, A)$$

and

$$Cor : H^i(H, A) \to H^i(G, A)$$

for all $i \geq 0$ that provide morphisms of δ-functors.

Proof. We consider only the case of restriction since the case of corestriction is very similar. The exactness of

$$0 \longrightarrow A_* \longrightarrow \mathbb{Z}[G] \otimes A \xrightarrow{\pi} A \longrightarrow 0$$

where $A_* = \ker \pi$, gives rise to the following commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & H_1(G, A) & \longrightarrow & H_0(G, A_*) & \longrightarrow & H_0(G, \mathbb{Z}[G] \otimes A) \\ & & \vdots \mathrm{Res} & & \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} \\ 0 & \longrightarrow & H_1(H, A) & \longrightarrow & H_0(H, A_*) & \longrightarrow & H_0(H, \mathbb{Z}[G] \otimes A). \end{array}$$

The restriction Res : $H_0(G, \mathbb{Z}[G] \otimes A)) \to H_0(H, \mathbb{Z}[G] \otimes A))$ is induced from Res : $H_0(G, A) \to H_0(H, A)$, hence it induces the restriction Res : $H_0(G, A_*) \to H_0(H, A_*)$ since $A_* = \ker \pi \subset \mathbb{Z}[G] \otimes A$. By the above diagram we are able to define Res : $H_1(G, A) \to H_1(H, A)$. Hence we can define Res : $H_i(G, A) \to H_i(H, A)$ for all $i \geq 2$ as well via dimension shifting. □

Corollary 2.7.10. *Let G be a finite group, H a subgroup of G. There are maps*

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

and

$$Cor : \hat{H}^i(H, A) \to \hat{H}^i(G, A)$$

for all $i \in \mathbb{Z}$ that provide morphisms of δ-functors.

Proof. We only need to check the commutativity of one diagram in each case, and we check the case for restriction since the case for corestriction is very similar. Specifically, suppose

$$0 \longrightarrow A \xrightarrow{\iota} B \xrightarrow{\pi} C \longrightarrow 0$$

is an exact sequence of G-modules, then we need to check that the diagram

$$\begin{array}{ccc} \hat{H}^{-1}(G,C) & \xrightarrow{\delta} & \hat{H}^0(G,A) \\ \downarrow{\scriptstyle \text{Res}} & & \downarrow{\scriptstyle \text{Res}} \\ \hat{H}^{-1}(H,C) & \xrightarrow{\delta} & \hat{H}^0(H,A) \end{array}$$

is commutative.

Let $c \in \ker(N_G : C \to C) \subset C$, and denote $\overline{c}$ to be its image in $\hat{H}^{-1}(G,C) = \frac{\ker(N_G)}{I_G C}$. Choose $b \in B$ such that $\pi(b) = c$ and consider $N(b) \in B^G$. Note that

$$\pi(N_G(b)) = \pi \sum_{g \in G} g \cdot b = \sum_{g \in G} g \cdot \pi(b) = \sum_{g \in G} g \cdot c = 0,$$

so $N_G(b) \in \ker(\pi : B^G \to C^G) = \text{im}(\iota : A^G \to B^G)$. So there exists some $a \in A^G$ such that $\iota(a) = N_G(b)$. Then $\delta(\overline{c})$ is the image of a in $\hat{H}^0(G,A)$. Then $\text{Res}\,(\delta(\overline{c}))$ is the image of a in $\hat{H}^0(H,A)$. On the other hand,

$$\text{Res}(\overline{c}) = \sum_{\overline{g} \in G/H} g^{-1} \cdot \tilde{c},$$

where $\tilde{c}$ is the image of c in $\hat{H}^{-1}(H,C)$. We lift c to $\sum_{\overline{g} \in G/H} g^{-1} \cdot c$ in the kernel of N_H on C, then lift it to $\sum_{\overline{g} \in G/H} g^{-1} \cdot b \in B$. Note that

$$N_H \left(\sum_{\overline{g} \in G/H} g^{-1} \cdot b \right) = N_G(b) = \iota(a),$$

hence $\delta(\text{Res}(\overline{c})$ is again the image of a in $\hat{H}^0(H,A)$. □

Proposition 2.7.11. *Let G be a finite group, H a subgroup of G. Suppose the index $[G:H] = n$ is finite, then Cor $\circ$ Res is just the multiplication by n on Tate cohomology groups.*

Proof. It suffices to show this on the zeroth cohomology and homology groups and then apply the dimension shifting. On cohomology we have

$$A^G \xrightarrow{\text{Res}} A^H \xrightarrow{\text{Cor}} A^G$$

where Res is just the natural inclusion, and Cor is the map defined in Definition 2.7.8. Let $a \in A^G$, then $g \cdot a = a$ for any $g \in G$ and hence

$$\mathrm{Cor} \circ \mathrm{Res}(a) = \mathrm{Cor}(a) = \sum_{\overline{g} \in G/H} g \cdot a = \sum_{\overline{g} \in G/H} a = na.$$

On homology, we have

$$A_G \xrightarrow{\mathrm{Res}} A_H \xrightarrow{\mathrm{Cor}} A_G$$

where Res is the map defined in 2.7.8, and Cor is the natural quotient map. Let $a \in A_G$ and $\tilde{a} \in A_H$ be a lift of a, then

$$\mathrm{Cor} \circ \mathrm{Res}(a) = \mathrm{Cor}(\sum_{\overline{g} \in G/H} g^{-1} \cdot \tilde{a}) = na.$$

□

Remark 2.7.12. *This also applies to homology groups and cohomology groups of an arbitrary group G (i.e., G need not be finite).*

Corollary 2.7.13. *Suppose G is a group of order n, A a G-module. Then all the Tate cohomology groups $\hat{H}^i(G, A)$ vanishes by n.*

Proof. Let $H = \{1\}$, then $[G, \{1\}] = n$. Corollary 2.7.11 implies that $\mathrm{Cor} \circ \mathrm{Res} = n$ on $\hat{H}^i(G, A)$ for all $i \in \mathbb{Z}$. On the other hand, $\hat{H}^i(H, A) = 0$ for all $i \in \mathbb{Z}$ (for the detail, see the Proof of Theorem 2.6.4). So $\mathrm{Cor} \circ \mathrm{Res} = 0$. □

Corollary 2.7.14. *Suppose G is a finite group, A a finitely generated G-module. Then $\hat{H}^i(G, A)$ is finite for all $i \in \mathbb{Z}$.*

Proof. By the definitions of cohomology and homology groups in terms of cochains and chains, these groups are finitely generated. By Corollary 2.7.13, they are torsion, hence they are finite. □

Let p be a prime and suppose p^m is the highest power of p dividing the order $|G|$ of a finite group G, i.e., $|G| = p^m q$ where $(p, q) = 1$. Sylow's Theorem tells us that there exists subgroups of G having order p^m and they are called *Sylow p-subgroups* of G.

Corollary 2.7.15. *Suppose G is a finite group, and G_p is a Sylow p-subgroup of G for a prime p. Then for any G-module A and $i \in \mathbb{Z}$, the kernel of*

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

has no element of order p (alternatively, Res is injective on the p-primary component of $\hat{H}^i(G, A)$).

Proof. Let $\alpha \in \hat{H}^i(G, A)$ with $p^n\alpha = 0$ for some $n \geq 0$. Then $\mathrm{Cor} \circ \mathrm{Res}(\alpha) = [G : G_p]\alpha$. But $[G : G_p]$ is prime to p, hence $[G : G_p]\alpha \neq 0$ if $\alpha \neq 0$. Hence $\alpha \notin \ker(\mathrm{Res})$ if $\alpha \neq 0$. □

Corollary 2.7.16. *Suppose G is a finite group, A any G-module, and G_p a Sylow p-subgroup of G for each prime p. Fix $i \in \mathbb{Z}$, and suppose that*

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

is trivial for all primes p. Then $\hat{H}^i(G, A) = 0$.

Proof. By Corollary 2.7.15, the p-primary components of $\hat{H}^i(G, A)$ is trivial for all primes p. Hence $\hat{H}^i(G, A) = 0$. □

2.8 Tate cohomology via complete resolutions

Let G be a finite group. Tate cohomology can also be formed by complete resolution of G. Let $P \to \mathbb{Z}$ be a resolution by finitely generated free G-modules (e.g. the standard resolution).

Definition 2.8.1. The *dual* of P is defined as $P^* = \mathrm{Hom}_{\mathbb{Z}}(P, \mathbb{Z})$ with the G-module structure

$$(g \cdot \varphi)(x) = \varphi(g^{-1}x).$$

We have two exact sequences

$$\cdots \to P_1 \to P_0 \xrightarrow{\epsilon} \mathbb{Z} \to 0,$$
$$0 \to \mathbb{Z} \xrightarrow{\epsilon^*} P_0^* \to P_1^* \to \cdots .$$

We write $P_{-n} = P_{n-1}^*$ for $n \geq 1$ and gluing the above two resolutions together gives a complete resolution

$$L : \quad \cdots \to P_1 \to P_0 \to P_{-1} \to P_{-2} \to \cdots .$$

Proposition 2.8.2. *Let G be a finite group and A be a G-module. Then $\hat{H}^i(G, A)$ is isomorphic to the i-th cohomology group of the cochain $\mathrm{Hom}_G(L, A)$.*

2.9 Cup products

Let G be a group and A, B any G-modules. We let G act on $A \otimes_{\mathbb{Z}} B$ by $g \cdot (a \otimes b) = g \cdot a \otimes g \cdot b$. We consider the following maps on the standard complex

$$\varphi_{i,j} : P_{i+j} \to P_i \otimes_{\mathbb{Z}} P_j$$
$$(g_0, \cdots, g_{i+j}) \mapsto (g_0, \cdots, g_i) \otimes (g_i, \cdots, g_{i+j})$$

for $i, j \geq 0$. There is an natural map

$$\begin{aligned}\mathrm{Hom}_G(P_i, A) \otimes_{\mathbb{Z}} \mathrm{Hom}_G(P_j, B) &\to \mathrm{Hom}_G(P_i \otimes_{\mathbb{Z}} P_j, A \otimes_{\mathbb{Z}} B) \\ \varphi \otimes \varphi' &\mapsto (\alpha \otimes \beta \mapsto \varphi(\alpha) \otimes \varphi'(\beta)).\end{aligned}$$

These give rise to a map

$$\begin{aligned}\mathrm{Hom}_G(P_i, A) \otimes_{\mathbb{Z}} \mathrm{Hom}_G(P_j, B) &\to \mathrm{Hom}_G(P_{i+j}, A \otimes_{\mathbb{Z}} B) \\ \varphi \otimes \varphi' &\mapsto \varphi \cup \varphi'.\end{aligned}$$

Definition 2.9.1. Let $\varphi \in \mathrm{Hom}_G(P_i, A)$, $\varphi' \in \mathrm{Hom}_G(P_j, B)$, $i, j \geq 0$. The *cup product* $\varphi \cup \varphi' \in \mathrm{Hom}_G(P_{i+j}, A \otimes_{\mathbb{Z}} B)$ is defined by

$$\left(\varphi \cup \varphi'\right)(g_0, \cdots, g_{i+j}) = \varphi(g_0, \cdots, g_i) \otimes \varphi'(g_i, \cdots, g_{i+j}).$$

Remark 2.9.2. *In cochains, we can define cup products*

$$C^i(G, A) \otimes_{\mathbb{Z}} C^j(G, B) \to C^{i+j}(G, A \otimes_{\mathbb{Z}} B)$$

by

$$\left(f \cup f'\right)(g_1, \cdots, g_{i+j}) = f(g_1, \cdots, g_i) \otimes g_1 g_2 \cdots g_i f'(g_{i+1}, \cdots, g_{i+j}).$$

Theorem 2.9.3. *The cup products in Definition 2.9.1 induce unique maps which are also called cup products,*

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

for $i, j \geq 0$ that are natural in A and B and satisfy the following properties.

(i) For $i = j = 0$, the cup product

$$A^G \otimes_{\mathbb{Z}} B^G \to (A \otimes_{\mathbb{Z}} B)^G$$

is induced by the identity on $A \otimes_{\mathbb{Z}} B$.

(ii) If

$$0 \to A_1 \to A \to A_2 \to 0$$

is an exact sequence of G-modules, and

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

is also exact, then

$$\delta(\alpha_2 \cup \beta) = \delta(\alpha_2) \cup \beta \in H^{i+j+1}(G, A \otimes_{\mathbb{Z}} B)$$

for all $\alpha_2 \in H^i(G, A_2), \beta \in H^j(G, B)$.

(iii) If

$$0 \to B_1 \to B \to B_2 \to 0$$

is an exact sequence of G-modules, and

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

is also exact, then

$$\delta(\alpha \cup \beta_2) = (-1)^i \alpha \cup \delta(\beta) \in H^{i+j+1}(G, A \otimes_{\mathbb{Z}} B)$$

for all $\alpha \in H^i(G, A), \beta_2 \in H^j(G, B_2)$.

Proposition 2.9.4. *Let G be a group and A, B, C any G-modules. Let $\alpha \in H^i(G, A)$, $\beta \in H^j(G, B)$, $\gamma \in H^k(G, C)$. Then*

$$(\alpha \cup \beta) \cup \gamma = \alpha \cup (\beta \cup \gamma) \in H^{i+j+k}(G, A \otimes_{\mathbb{Z}} B \otimes_{\mathbb{Z}} C).$$

Proposition 2.9.5. *Let G be a group and A, B any G-modules. Consider the natural isomorphism*

$$\begin{aligned} s_{AB} : A \otimes_{\mathbb{Z}} B &\to B \otimes_{\mathbb{Z}} A \\ a \otimes b &\mapsto b \otimes a \end{aligned}$$

and the maps that it induces on cohomology. For all $\alpha \in H^i(G, A)$, $\beta \in H^j(G, B)$, we have

$$s^*_{AB}(\alpha \cup \beta) = (-1)^{ij}(\beta \cup \alpha).$$

Proposition 2.9.6. *Let G be a group and A, B any G-modules. Let H be a subgroup of G of finite index.*

(i) If $\alpha \in H^i(G, A), \beta \in H^j(G, B)$, then

$$Res\ (\alpha \cup \beta) = Res\ (\alpha) \cup Res\ (\beta).$$

(ii) If $\alpha \in H^i(H, A), \beta \in H^j(G, B)$, then

$$Cor\ (\alpha) \cup \beta = Cor\ \left(\alpha \cup Res\ (\beta)\right).$$

For finite groups, we also have cup products on Tate cohomology.

Theorem 2.9.7. *Let G be a finite group and A, B any G-modules. There exists unique maps*

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

for $i, j \in \mathbb{Z}$ that are natural in A and B and satisfy the following properties.

(i) The diagram

$$\begin{array}{ccc} H^0(G,A) \otimes_{\mathbb{Z}} H^0(G,B) & \xrightarrow{\cup} & H^0(G, A \otimes_{\mathbb{Z}} B) \\ \downarrow & & \downarrow \\ \hat{H}^0(G,A) \otimes_{\mathbb{Z}} \hat{H}^0(G,B) & \xrightarrow{\cup} & \hat{H}^0(G, A \otimes_{\mathbb{Z}} B) \end{array}$$

commutes.

(ii) If

$$0 \to A_1 \to A \to A_2 \to 0$$

is an exact sequence of G-modules, and

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

is also exact, then

$$\delta(\alpha_2 \cup \beta) = \delta(\alpha_2) \cup \beta \in \hat{H}^{i+j+1}(G, A \otimes_{\mathbb{Z}} B)$$

for all $\alpha_2 \in \hat{H}^i(G, A_2), \beta \in \hat{H}^j(G,B)$.

(iii) If

$$0 \to B_1 \to B \to B_2 \to 0$$

is an exact sequence of G-modules, and

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

is also exact, then

$$\delta(\alpha \cup \beta_2) = (-1)^i \alpha \cup \delta(\beta) \in \hat{H}^{i+j+1}(G, A \otimes_{\mathbb{Z}} B)$$

for all $\alpha \in \hat{H}^i(G,A), \beta_2 \in \hat{H}^j(G, B_2)$.

2.10 Tate cohomology of cyclic groups

Let $G =< s >$ be a finite cyclic group of order n. Let $D = s - 1$, $N = \sum_{g \in G} g = \sum_{i=0}^{n-1} s^i$. Then $I_G =< g - 1 \mid g \in G >=< D >$ as a $\mathbb{Z}[G]$-module. Let A be any G-module. Notice that the action of G on A is determined by s, hence

$$a \in A^G \Leftrightarrow s \cdot a = a \Leftrightarrow (s-1) \cdot a = 0 \Leftrightarrow a \in \ker(D : A \to A),$$

$$I_G A = \text{im } (D : A \to A).$$

Therefore, $A^G = \ker(D), I_G A = \text{im } (D)$. Hence,

$$\hat{H}^0(G, A) = \frac{A^G}{N(A)} = \frac{\ker(D)}{\text{im } (N)},$$
$$\hat{H}_0(G, A) = \frac{\ker(N)}{I_G A} = \frac{\ker(N)}{\text{im } (D)}.$$

In particular, if A is induced, then $\ker(D) = \text{im } (N)$ and $\ker(N) = \text{im } (D)$.

Now consider a complete resolution K for G. Let $K_i = \mathbb{Z}[G]$ for each i, and define maps $d : K_{i+1} \to K_i$ by multiplication by D if i is even, and multiplication by N if i is odd. Then we obtain a complete resolution of $\mathbb{Z}$

$$\cdots \to \mathbb{Z}[G] \xrightarrow{D} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{D} \mathbb{Z}[G] \to \cdots .$$

Then the complex $\text{Hom}_G(K, A)$ is

$$\cdots \leftarrow A \xleftarrow{N} A \xleftarrow{D} A \xleftarrow{N} A \leftarrow \cdots .$$

Thus $\hat{H}^i(G, A) \cong H^i(\text{Hom}_G(K, A))$. In particular, $\hat{H}^{i+2}(G, A) \cong \hat{H}^i(G, A)$ since K is of periodic 2.

Proposition 2.10.1. *For any $i \in \mathbb{Z}$, we have*

$$\hat{H}^i(G, A) = \begin{cases} \frac{A^G}{N(A)}, & i \equiv 0 \pmod 2, \\ \frac{\ker(N)}{D(A)}, & i \equiv 1 \pmod 2. \end{cases}$$

In particular, $\hat{H}^2(G, \mathbb{Z}) = \mathbb{Z}^G / N(\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$.

Theorem 2.10.2. *Cup product by a generator of $\hat{H}^2(G, \mathbb{Z})$ gives rise to an isomorphism*

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

for all $i \in \mathbb{Z}$ and any G-module A.

Proof. Consider the two exact sequences of G-modules

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

and

$$0 \longrightarrow \mathbb{Z} \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{D} I_G \to 0.$$

Since $\hat{H}^i(G, \mathbb{Z}[G]) = 0$ for all $i \in \mathbb{Z}$, we have two isomorphisms

$$\hat{H}^0(G, \mathbb{Z}) \xrightarrow{\delta} \hat{H}^1(G, I_G) \xrightarrow{\delta} \hat{H}^2(G, \mathbb{Z}).$$

Therefore, it reduces to show that cup product by a generator of $\hat{H}^0(G, \mathbb{Z})$ induces an automorphism of $\hat{H}^i(G, A)$. By dimension shifting we reduce to the case $i = 0$. Note that

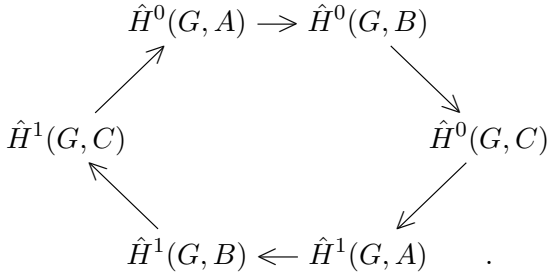
$$\hat{H}^0(G, \mathbb{Z}) = \frac{\mathbb{Z}^G}{N(\mathbb{Z})} = \mathbb{Z}/n\mathbb{Z},$$

where $n = |G|$. A generator b of $\hat{H}^0(G, \mathbb{Z})$ is represented by an integer β which is prime to n, and cup product with b is multiplication by β. Since β is prime to n, there exists an integer γ such that $\beta\gamma \equiv 1 \pmod{n}$. Since $\hat{H}^0(G, \mathbb{Z})$ vanishes by multiplication of n, multiplication by β is therefore an automorphism of $\hat{H}^0(G, A)$. □

Corollary 2.10.3. *Suppose G is a finite cyclic group. A short exact sequence*

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

of G-modules gives rise to an exact hexagon



Definition 2.10.4. Suppose that $\hat{H}^0(G, A)$ and $\hat{H}^1(G, A)$ are finite groups, and let $h_0(A)$, $h_1(A)$ be their orders. We define the *Herbrand quotient* of A to be

$$h(A) = \frac{h_0(A)}{h_1(A)}.$$

Proposition 2.10.5. *Let G be a finite cyclic group. Let*

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

be a short exact sequence of G-modules. If any two of $h(A), h(B), h(C)$ are defined, then the third one is also defined, and

$$h(B) = h(A)h(C).$$

Proof. Without loss of generality, we assume that $h_0(A), h_1(A), h_0(B), h_1(B)$ are finite. We have an exact hexagon, and let M_1 be the image of $\hat{H}^0(G,A)$ in $\hat{H}^0(G,B)$, M_2 be the image of $\hat{H}^0(G,B)$ in $\hat{H}^0(G,C)$, and so on in clockwise direction round the hexagon. Then

$$0 \to M_2 \to \hat{H}^0(G,C) \to M_3 \to 0$$

is exact. Now M_2 is finite because it is a homomorphic image of $\hat{H}^0(G,B)$, and M_3 is finite because it is a subgroup of $\hat{H}^1(G,A)$. Thus $\hat{H}^0(G,C)$ is also finite. Similarly, $\hat{H}^1(G,C)$ is finite. Thus $h(C)$ is defined.

Let m_i be the order of M_i for $1 \leq i \leq 6$. Consider

$$\hat{H}^1(G,C) \xrightarrow{\delta} \hat{H}^0(G,A) \xrightarrow{\iota} \hat{H}^0(G,B),$$

we have

$$M_1 = \text{im } (\iota) \cong \frac{\hat{H}^0(G,A)}{\ker(\iota)} = \frac{\hat{H}^0(G,A)}{\text{im } (\delta)} = \frac{\hat{H}^0(G,A)}{M_6}.$$

Hence $|\hat{H}^0(G,A)| = m_1 m_6$. Similarly, $|\hat{H}^0(G,B)| = m_1 m_2, |\hat{H}^0(G,C)| = m_2 m_3, |\hat{H}^1(G,A)| = m_3 m_4, |\hat{H}^1(G,B)| = m_4 m_5, |\hat{H}^1(G,C)| = m_5 m_6$. Therefore,

$$h(B) = \frac{h_0(B)}{h_1(B)} = \frac{m_1 m_2}{m_4 m_5} = \frac{m_1 m_6}{m_3 m_4} \cdot \frac{m_2 m_3}{m_5 m_6} = h(A)h(C).$$

□

Proposition 2.10.6. *Let G be a finite cyclic group. If A is a finite G-module, then $h(A) = 1$.*

Proof. The sequence

$$0 \longrightarrow A^G \xrightarrow{\iota} A \xrightarrow{D} A \xrightarrow{\pi} A_G \longrightarrow 0$$

is exact. Hence,

$$A_G = \text{im}(\pi) \cong A/\ker(\pi) = A/\text{im}(D),$$
$$A/A_G \cong A/\text{im}(\iota) = A/\ker(D) \cong \text{im}(D),$$

and so $|A^G| = |A_G|$. On the other hand,

$$0 \longrightarrow \hat{H}^1(G,A) \longrightarrow A_G \xrightarrow{N^*} A^G \longrightarrow \hat{H}^0(G,A) \longrightarrow 0$$

is exact because $\hat{H}^1(G,A) = \hat{H}^{-1}(G,A) = \hat{H}_0(G,A)$. The same technique implies that $|\hat{H}^1(G,A)| = |\hat{H}^0(G,A)|$ and hence $h(A) = 1$. □

Corollary 2.10.7. *Let G be a finite cyclic group, A, B any G-modules. Suppose $f : A \to B$ is a G-homomorphism with finite kernel and cokernel. If either of $h(A), h(B)$ is defined, then so is the other, and they are equal.*

Proof. Without loss of generality, we assume that $h(A)$ is defined. The exactness of

$$0 \longrightarrow \ker(f) \longrightarrow A \longrightarrow f(A) \rightarrow 0$$

implies that $h(f(A))$ is defined, and

$$h(A) = h(\ker(f)) \cdot h(f(A)) = h(f(A))$$

by Proposition 2.10.5 and Proposition 2.10.6. Similarly, the exactness of

$$0 \longrightarrow f(A) \longrightarrow B \longrightarrow \operatorname{coker}(f) \rightarrow 0$$

implies that $h(B)$ is defined, and

$$h(B) = h(f(A)) \cdot h(\operatorname{coker}(f)) = h(f(A)).$$

Therefore, $h(A) = h(B)$. □

2.11 Cohomological triviality

We assume G to be a finite group.

Definition 2.11.1. Let G be a finite group. A G module A is *cohomologically trivial* if $\hat{H}^i(H, A) = 0$ for all $i \in \mathbb{Z}$ and all subgroup H of G.

Example 2.11.2. Induced G-modules are cohomologically trivial. This is because an induced G-module is also an induced H-module, and by Theorem 2.6.4.

Example 2.11.3. Free G-modules are cohomologically trivial. To see this, let F be a free module over $\mathbb{Z}[G]$, hence over $\mathbb{Z}[H]$ on a generating set I for any subgroup $H \subset G$. Then $F \cong \bigoplus_{i \in I} \mathbb{Z}[H]$ and so $F^H = 0$ and $\hat{H}^0(H, F) = 0$. Hence $\hat{H}^i(H, F) = 0$ for any $i \in \mathbb{Z}$ by the long exact sequence of Tate cohomology and dimension shifting.

Let p be a prime number. Recall that a finite group G is called a *p-group* if its order $|G|$ is a power of p.

Lemma 2.11.4. *Let G be a p-group where p is a prime number, and A be a G-module such that $pA = 0$. Then the following are equivalent.*
(i) $A = 0$.
(ii) $H^0(G, A) = A^G = 0$.
(iii) $H_0(G, A) = A_G = 0$.

Proof. It is clear that (i) ⇒ (ii) and (i) ⇒ (iii).

(ii) ⇒ (i): Let $A^G = 0$ and $a \in A$. Then the submodule B of A generated by a is finite, of order a power of p, and $B^G = 0$. The G-orbits in B are either $\{0\}$ or a multiple of p since $B^G = 0$. Since B has p-power order, the order of B has to be 1, and hence $B = 0$. Since A was arbitrary, $A = 0$.

(iii) $\Rightarrow$ (i): Suppose $A_G = 0$. Then $X = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{F}_p)$ satisfies $pX = 0$, and

$$X^G = (\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{F}_p))^G = \mathrm{Hom}_{\mathbb{Z}[G]}(A, \mathbb{F}_p) = \mathrm{Hom}_{\mathbb{Z}[G]}(A_G, \mathbb{F}_p) = 0.$$

By the direction (ii) $\Rightarrow$ (i) we just proved, $X = 0$, and hence $A = 0$. □

Lemma 2.11.5. *Let G be a p-group, and A be a G-module such that $pA = 0$. If $H_1(G, A) = 0$, then A is a free module over $\mathbb{F}_p[G]$.*

Proof. Since $pA = 0$, $pA_G = 0$ and so A_G is a vector space over $\mathbb{F}_p$. Let e_λ be a basis of A_G over $\mathbb{F}_p$, and lift it to $a_\lambda \in A$. Let F be the free $\mathbb{F}_p[G]$-module generated by a_λ, then we have the canonical surjection $\pi : F \to A$, and let $R = \ker(\pi)$. Then

$$0 \longrightarrow R \longrightarrow F \xrightarrow{\pi} A \longrightarrow 0$$

is exact, and hence

$$0 \longrightarrow R_G \longrightarrow F_G \xrightarrow{\tilde{\pi}} A_G \longrightarrow 0$$

is exact because $H_1(G, A) = 0$ implies $H_1(G, R) = 0$. The map $\tilde{\pi}$ induced by π is an isomorphism, so $R_G = 0$. Since $pR = 0$, we have $R = 0$ by Lemma 2.11.4. Hence π is an isomorphism. That is, $A \cong F$ is a free module over $\mathbb{F}_p[G]$. □

Theorem 2.11.6. *Let G be a p-group, and A be a G-module such that $pA = 0$. The following are equivalent.*
(i) A is an induced G-module.
(ii) A is cohomologically trivial.
(iii) A is a free $\mathbb{F}_p[G]$-module.
(iv) There exists some $i \in \mathbb{Z}$ such that $\hat{H}^i(G, A) = 0$.

Proof. It's easy to see that (i) $\Rightarrow$ (ii) $\Rightarrow$ (iv).

(iii) $\Rightarrow$ (i): Suppose A is free over $\mathbb{F}_p[G]$ on a generating set I, then

$$A = \bigoplus_{i \in I} \mathbb{F}_p[G] \cong \bigoplus_{i \in I} \mathbb{Z}[G]/p\mathbb{Z}[G] \cong \bigoplus_{i \in I} \mathbb{Z}[G] \otimes (\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}[G] \otimes (\bigoplus_{i \in I} \mathbb{F}_p).$$

Hence A is induced.

(iv) $\Rightarrow$ (iii): Since $pA = 0$, $pA^* = pA_* = 0$. By dimension shifting, there is a G-module B such that $pB = 0$ and

$$\hat{H}^{j-2}(G, B) \cong \hat{H}^{i+j}(G, A)$$

for all $j \in \mathbb{Z}$. In particular, $H_1(G, B) = \hat{H}^{-2}(G, B) \cong \hat{H}^i(G, A)$ is trivial. By Lemma 2.11.5, B is a free module over $\mathbb{F}_p[G]$. By the case (iii) $\Rightarrow$ (i) we just proved, B is cohomologically trivial, and hence A is also a cohomologically trivial G-module. Apply Lemma 2.11.5 again, and we obtain that A is a free $\mathbb{F}_p[G]$-module. □

Theorem 2.11.7. *Let G be a p-group, and A be a G-module with no element of order p. Then the following are equivalent.*
(i) A is cohomologically trivial.
(ii) There exists some $i \in \mathbb{Z}$ such that $\hat{H}^i(G, A) = \hat{H}^{i+1}(G, A) = 0$.
(iii) A/pA is a free $\mathbb{F}_p[G]$-module.

Proof. It is clear that (i) $\Rightarrow$ (ii).

(ii) $\Rightarrow$ (iii): Since A has no p-torsion,

$$0 \longrightarrow A \xrightarrow{p} A \longrightarrow A/pA \longrightarrow 0$$

is an exact sequence, and so we have an exact sequence

$$\hat{H}^i(G, A) \xrightarrow{p} \hat{H}^i(G, A) \to \hat{H}^i(G, A/pA) \to \hat{H}^{i+1}(G, A) \xrightarrow{p} \hat{H}^{i+1}(G, A).$$

Since $\hat{H}^i(G, A) = \hat{H}^{i+1}(G, A) = 0$, we have $\hat{H}^i(G, A/pA) = 0$ by the long exact sequence of Tate cohomology groups. By Theorem 2.11.6, A/pA is a free $\mathbb{F}_p[G]$-module.

(iii) $\Rightarrow$ (i): Suppose A/pA is a free $\mathbb{F}_p[G]$-module, then A/pA is cohomologically trivial by Theorem 2.11.6. Hence the map $p : \hat{H}^i(G, A) \to \hat{H}^i(G, A)$ of multiplication by p is an isomorphism on $\hat{H}^i(G, A)$ for all $i \in \mathbb{Z}$. For any subgroup $H \subset G$, consider the commutative diagram

$$\begin{array}{ccc} \hat{H}^i(H, A) & \xrightarrow{p} & \hat{H}^i(H, A) \\ \downarrow{\scriptstyle \mathrm{Cor}} & & \downarrow{\scriptstyle \mathrm{Cor}} \\ \hat{H}^i(G, A) & \xrightarrow{p} & \hat{H}^i(G, A). \end{array}$$

It follows that the map $p : \hat{H}^i(H, A) \to \hat{H}^i(H, A)$ of multiplication by p is also an isomorphism on $\hat{H}^i(H, A)$ for any subgroup $H \subset G$ and any $i \in \mathbb{Z}$. But $\hat{H}^i(H, A)$ is a p-group by Corollary 2.7.13, hence $\hat{H}^i(H, A) = 0$. Hence A is cohomologically trivial. □

Corollary 2.11.8. *Let G be a p-group, and A be a G-module that is free over $\mathbb{Z}$ and cohomologically trivial. If a G-module B is $\mathbb{Z}$-torsion free, then* $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ *is cohomologically trivial.*

Proof. Since B is $\mathbb{Z}$-torsion free, the sequence

$$0 \longrightarrow B \xrightarrow{p} B \longrightarrow B/pB \longrightarrow 0$$

is exact, and hence so is the sequence

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(A, B) \xrightarrow{p} \mathrm{Hom}_{\mathbb{Z}}(A, B) \to \mathrm{Hom}_{\mathbb{Z}}(A, B/pB) \longrightarrow 0.$$

In particular, $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ has no p-torsion, and

$$\mathrm{Hom}_{\mathbb{Z}}(A, B)/p\mathrm{Hom}_{\mathbb{Z}}(A, B) \cong \mathrm{Hom}_{\mathbb{Z}}(A, B/pB) \cong \mathrm{Hom}_{\mathbb{Z}}(A/pA, B/pB).$$

A/pA is free over $\mathbb{F}_p[G]$ by Theorem 2.11.7, hence it is an induced G-module, by Theorem 2.11.6. Let X be an abelian group such that $A/pA = \mathbb{Z}[G] \otimes_{\mathbb{Z}} X$, then

$$\mathrm{Hom}_{\mathbb{Z}}(A/pA, B/pB) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G] \otimes_{\mathbb{Z}} X, B/pB) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \mathrm{Hom}_{\mathbb{Z}}(X, B/pB))$$

by the Adjoint Isomorphism Theorem for Tensor and Hom. So $\mathrm{Hom}_{\mathbb{Z}}(A/pA, B/pB)$, and hence $\mathrm{Hom}_{\mathbb{Z}}(A, B)/p\mathrm{Hom}_{\mathbb{Z}}(A, B)$, are induced G-modules. Applying Theorem 2.11.6 again to conclude that $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ is cohomologically trivial. □

Proposition 2.11.9. *Let G be a finite group, and G_p be a Sylow p-subgroup of G for each prime p. Then A is cohomologically trivial as a G-module if and only if A is cohomologically trivial as a G_p-module for each prime p.*

Proof. Suppose A is cohomologically trivial as a G_p-module for all p. Since all the Sylow p-subgroups are conjugate to each other, given a subgroup $H \subset G$, there exists some $g \in G$ such that $H_p \subset gG_pg^{-1}$. By the cohomological triviality of G_p, we have $\hat{H}^i(g^{-1}H_pg, A) = 0$ for all $i \in \mathbb{Z}$. Since conjugation by g is an isomorphism, we have $\hat{H}^i(H_p, A) = 0$. Therefore, the restriction homomorphism Res:$\hat{H}^i(H, A) \to \hat{H}^i(H_p, A)$ is 0. Since this holds for all prime p, it follows that $\hat{H}^i(H, A) = 0$ by Corollary 2.7.16. Hence A is a cohomologically trivial G-module. □

A G-module A is *projective* if $\mathrm{Hom}_G(A, \cdot)$ is an exact functor (or equivalent, A is a direct summand of a free G-module).

Example 2.11.10. Projective G-modules are cohomologically trivial. Suppose P and Q are projective G-modules with $F = P \oplus Q$ being a free G-module. For any subgroup $H \subset G$, F is also free over $\mathbb{Z}[H]$. Then

$$\hat{H}^i(H, P) \hookrightarrow \hat{H}^i(H, P) \oplus \hat{H}^i(H, Q) \cong \hat{H}^i(H, P \oplus Q) = \hat{H}^i(H, F) = 0$$

for all $i \in \mathbb{Z}$. Therefore, P is cohomologically trivial.

We have the following theorem.

Theorem 2.11.11. *Let G be a finite group, A a G-module that is free over $\mathbb{Z}$. Then A is a cohomologically trivial G-module if and only if A is a projective G-module.*

Proof. We already showed that projective G-modules are cohomologically trivial. Suppose that A is a cohomologically trivial G-module. Since A is $\mathbb{Z}$-free, it follows that $\mathbb{Z}[G] \otimes A$ is a free G-module, A_* is $\mathbb{Z}$-torsion free, and the sequence

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(A, A_*) \to \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Z}[G] \otimes A) \to \mathrm{Hom}_{\mathbb{Z}}(A, A) \longrightarrow 0$$

is exact. Moreover, $\mathrm{Hom}_{\mathbb{Z}}(A, A_*)$ is a cohomologically trivial G-module by Corollary 2.11.8. Note that

$$H^0\left(G, \mathrm{Hom}_{\mathbb{Z}}(A, A_*)\right) = \left(\mathrm{Hom}_{\mathbb{Z}}(A, A_*)\right)^G \cong \mathrm{Hom}_{\mathbb{Z}[\mathbb{G}]}(A, A_*),$$

$$H^0\left(G, \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Z}[G] \otimes A)\right) = \left(\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Z}[G] \otimes A)\right)^G \cong \mathrm{Hom}_{\mathbb{Z}[\mathbb{G}]}(A, \mathbb{Z}[G] \otimes A).$$

Hence the map

$$\mathrm{Hom}_{\mathbb{Z}[\mathbb{G}]}(A, \mathbb{Z}[G] \otimes A) \to \mathrm{Hom}_{\mathbb{Z}[\mathbb{G}]}(A, A_*)$$

is surjective by the long exact cohomology sequence attached to the above exact sequence. So the identity map of A lifts to a G-homomorphism $A \to \mathbb{Z}[G] \otimes A$. Hence A is a direct summand of the free G-module $\mathbb{Z}[G] \otimes A$. Therefore, A is projective. □

Finally, we consider the general case.

Theorem 2.11.12. *Let G be a finite group, and A a G-module. Then the following are equivalent.*
(i) A is cohomologically trivial.
(ii) For each prime p, there exists some $i \in \mathbb{Z}$ such that $\hat{H}^i(G_p, A) = \hat{H}^{i+1}(G_p, A) = 0$.
(iii) There is an exact sequence of G-modules

$$0 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow A \longrightarrow 0$$

where P_0, P_1 are projective G-modules.

Proof. It is clear that (i) ⇒ (ii). (iii) ⇒ (i) follows from the long exact sequence of Tate cohomology and the fact that projective G-modules are cohomologically trivial.

(ii) ⇒ (iii): Choose a free (hence projective) G-module F which maps surjectively onto A, and let B be the kernel of the map. Then the sequence

$$0 \longrightarrow B \longrightarrow F \longrightarrow A \longrightarrow 0$$

is exact. Since F is cohomologically trivial, we have

$$\hat{H}^{j-1}(G_p, A) \cong \hat{H}^j(G_p, B)$$

for every $j \in \mathbb{Z}$ by the long exact sequence of Tate cohomology. It follows that $\hat{H}^j(G_p, B)$ vanishes for two consecutive values of j. B is $\mathbb{Z}$-free because B is a subgroup of F. Then Theorem 2.11.7, Proposition 2.11.9, and Theorem 2.11.11 imply that B is projective. □

2.12 Tate's Theorem

Proposition 2.12.1. *Let G be a finite group, $f : A \to B$ a G-homomorphism. Let G_p be a Sylow p-subgroup of G for each prime p. Suppose that, for each prime p, there exists some $j \in \mathbb{Z}$ such that*

$$f_p^* : \hat{H}^i(G_p, A) \to \hat{H}^i(G_p, B)$$

is surjective for $i = j - 1$, an isomorphism for $i = j$, and injective for $i = j + 1$. Then

$$f^* : \hat{H}^i(H, A) \to \hat{H}^i(H, B)$$

is an isomorphism for all $i \in \mathbb{Z}$ and subgroups $H \subset G$.

Proof. For each prime p, consider the canonical injection

$$f_p \otimes \iota : A \to B \otimes \mathrm{Hom}(\mathbb{Z}[G_p], A)$$

of G_p-modules. Let C be the cokernel of the injection $f_p \otimes \iota$. Then we have an exact sequence

$$0 \longrightarrow A \longrightarrow B \otimes \mathrm{Hom}(\mathbb{Z}[G_p], A) \longrightarrow C \longrightarrow 0$$

of G_p-modules. Since $\mathrm{Hom}(\mathbb{Z}[G_p], A)$ is G_p-cohomologically trivial,

$$\hat{H}^i(G_p, B \otimes \mathrm{Hom}(\mathbb{Z}[G_p], A)) \cong \hat{H}^i(G_p, B)$$

for all $i \in \mathbb{Z}$. So we have the long exact sequence

$$\cdots \to \hat{H}^i(G_p, A) \overset{f_p^*}{\to} \hat{H}^i(G_p, B) \to \hat{H}^i(G_p, C) \overset{\delta}{\to} \hat{H}^{i+1}(G_p, A) \overset{f_p^*}{\to} \hat{H}^{i+1}(G_p, B) \to \cdots .$$

Consider the case $i = j - 1$. The map f_p^* being surjective on $\hat{H}^{j-1}(G_p, A)$ and f_p^* being an isomorphism and hence injective on $\hat{H}^j(G_p, A)$ implies that $\hat{H}^{j-1}(G_p, C) = 0$. Similarly, for $i = j$, f_p^* being an isomorphism and hence surjective on $\hat{H}^j(G_p, A)$ and being injective on $\hat{H}^{j+1}(G_p, A)$ implies that $\hat{H}^j(G_p, C) = 0$. By Theorem 2.11.12, C is a cohomologically trivial G_p-module. Therefore, each f^* must be an isomorphism by the long exact sequence of Tate cohomology groups. □

Theorem 2.12.2. *Let G be a finite group, A, B, C be any G-modules, and*

$$\theta : A \otimes_{\mathbb{Z}} B \to C$$

be a G-module map. Let $k \in \mathbb{Z}$ and $\alpha \in \hat{H}^k(G, A)$. For each subgroup $H \subset G$, define

$$\begin{aligned} \Theta^i_{H,\alpha} : \hat{H}^i(H, B) &\to \hat{H}^{i+k}(H, C) \\ \beta &\mapsto \theta^*(Res(\alpha) \cup \beta). \end{aligned}$$

For each prime p, suppose that there exists some $j \in \mathbb{Z}$ such that the map $\Theta^i_{G_p,\alpha}$ is surjective for $i = j - 1$, an isomorphism for $i = j$, and injective for $i = j + 1$. Then $\Theta^i_{H,\alpha}$ is an isomorphism for all $i \in \mathbb{Z}$ and any subgroup $H \subset G$.

Proof. First we consider the case $k = 0$. For $\alpha \in \hat{H}^0(G, A)$, let $a \in A^G$ represent α. Consider the map $\psi : B \to C$ given by $\psi(b) = \theta(a \otimes b)$. Note that for any $g \in G$,

$$\psi(gb) = \theta(a \otimes gb) = \theta(ga \otimes gb) = \theta(g(a \otimes b)) = g\theta(a \otimes b) = g\psi(b).$$

So ψ is a G-homomorphism. We claim that the induced map on Tate cohomology

$$\psi^* : \hat{H}^i(H, B) \to \hat{H}^i(H, C)$$

agrees with the map $\Theta^i_{H,\alpha}$.

To see the claim, we first consider the case $i = 0$. Let $b \in B^H$ represent $\beta \in \hat{H}^0(H, B)$. Then

$$\psi^*(\beta) = \theta(a \otimes b) + N(C) = \theta^*(\mathrm{Res}(\alpha) \cup \beta) = \Theta^i_{H,\alpha}(\beta).$$

In general, we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (A \otimes_{\mathbb{Z}} B)_* & \to & \mathbb{Z}[G] \otimes_{\mathbb{Z}} (A \otimes_{\mathbb{Z}} B) & \to & A \otimes_{\mathbb{Z}} B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \theta'} & & \downarrow{\scriptstyle \mathrm{id}_{\mathbb{Z}[G]} \otimes \theta} & & \downarrow{\scriptstyle \theta} & & \\ 0 & \longrightarrow & C_* & \longrightarrow & \mathbb{Z}[G] \otimes C & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

with exact rows. Moreover, the top row of the above diagram is isomorphic to

$$0 \longrightarrow A \otimes_{\mathbb{Z}} B_* \to A \otimes_{\mathbb{Z}} (\mathbb{Z}[G] \otimes_{\mathbb{Z}} B) \to A \otimes_{\mathbb{Z}} B \longrightarrow 0$$

and we have a map $\psi' : B_* \to C_*$ given by $\psi'(b') = \theta'(a \otimes b')$ for all $b' \in B_*$. Then we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B_* & \longrightarrow & \mathbb{Z}[G] \otimes_{\mathbb{Z}} B & \longrightarrow & B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \psi'} & & \downarrow{\scriptstyle \mathrm{id}_{\mathbb{Z}[G]} \otimes \psi} & & \downarrow{\scriptstyle \psi} & & \\ 0 & \longrightarrow & C_* & \longrightarrow & \mathbb{Z}[G] \otimes_{\mathbb{Z}} C & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

with exact rows. Then we have commutative diagrams

$$\begin{array}{ccc} \hat{H}^{i-1}(H, B) & \xrightarrow{\delta} & \hat{H}^i(H, B_*) \\ \downarrow{\scriptstyle \psi^*} & & \downarrow{\scriptstyle (\psi')^*} \\ \hat{H}^{i-1}(H, C) & \xrightarrow{\delta} & \hat{H}^i(H, C_*) \end{array}$$

and

$$\begin{array}{ccc} \hat{H}^{i-1}(H, B) & \xrightarrow{\delta} & \hat{H}^i(H, B_*) \\ \downarrow{\scriptstyle \Theta^{i-1}_{H,\alpha}} & & \downarrow{\scriptstyle (\Theta')^i_{H,\alpha}} \\ \hat{H}^{i-1}(H, C) & \xrightarrow{\delta} & \hat{H}^i(H, C_*) \end{array}$$

where $(\Theta')^i_{H,\alpha}(\beta) = (\theta')^*(\mathrm{Res}(\alpha) \cup \beta)$, and the connecting homomorphisms δ are isomorphisms since $\mathbb{Z}[G] \otimes_{\mathbb{Z}} B$ and $\mathbb{Z}[G] \otimes_{\mathbb{Z}} C$ are induced and hence cohomologically trivial. Now suppose $(\psi')^* = (\Theta')^i_{H,\alpha}$ on $\hat{H}^i(H, B_*)$, then we have $\psi^* = \Theta^{i-1}_{H,\alpha}$ on $\hat{H}^{i-1}(H, B)$ as well. That is to say, if the statement is true for i, then it is also true for $i - 1$. A similar argument allows us to shift from i to $i + 1$. Hence we proved the claim.

Now ψ^* satisfies the condition of Proposition 2.12.1, hence ψ^* is an isomorphism for all $i \in \mathbb{Z}$. This proves Theorem 2.12.2 for $k = 0$.

The general case follows from another piece of dimension shifting. Let $\alpha \in \hat{H}^{k-1}(H, A)$, $\alpha' = \delta(\alpha) \in \hat{H}^k(H, A_*)$. Note that we also have an exact sequence

$$0 \longrightarrow A_* \otimes_{\mathbb{Z}} B \to (\mathbb{Z}[G] \otimes_{\mathbb{Z}} A) \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B \longrightarrow 0.$$

Consider the diagram

$$\begin{array}{ccc} \hat{H}^i(H, B) & = & \hat{H}^i(H, B) \\ \downarrow{\scriptstyle \Theta^i_{H,\alpha}} & & \downarrow{\scriptstyle (\Theta')^i_{H,\alpha'}} \\ \hat{H}^{i+k-1}(H, C) & \xrightarrow{\delta} & \hat{H}^{i+k}(H, C_*). \end{array}$$

It is commutative because

$$\delta \circ \Theta^i_{H,\alpha}(\beta) = \delta \circ \theta(\mathrm{Res}(\alpha) \cup \beta) = \theta' \circ \delta(\mathrm{Res}(\alpha) \cup \beta) = \theta' \circ (\mathrm{Res}(\alpha') \cup \beta) = (\Theta')^i_{H,\alpha'}(\beta).$$

Also, the connecting homomorphism $\delta : \hat{H}^{i+k-1}(H, C) \to \hat{H}^{i+k}(H, C_*)$ is an isomorphism. By assumption, there exists some $j \in \mathbb{Z}$ such that the map $\Theta^i_{G_p,\alpha}$ is surjective for $i = j-1$, an isomorphism for $i = j$, and injective for $i = j+1$. By the commutativity of the above diagram, we have that the map $(\Theta')^i_{H,\alpha'}$ is surjective for $i = j$, an isomorphism for $i = j+1$, and injective for $i = j+2$. Assume Theorem 2.12.2 is true for k, then we have that all $(\Theta')^i_{H,\alpha'}$ are isomorphisms. By the commutativity of the above diagram again, all the maps $\Theta^i_{H,\alpha}$ are isomorphisms as well. This completes the proof. □

The following is a special case first due to Tate.

Theorem 2.12.3 (Tate)**.** *Let G be a finite group, A be a G-module, and $\alpha \in H^2(G, A)$. Let G_p be a Sylow p-subgroup of G for each prime p. Suppose for each prime p, $H^1(G_p, A) = 0$ and $H^2(G_p, A)$ is a cyclic group of order $|G_p|$ generated by the restriction of α. Then the map*

$$\begin{aligned} \hat{H}^i(H, \mathbb{Z}) &\to \hat{H}^{i+2}(H, A) \\ \beta &\mapsto \mathit{Res}(\alpha) \cup \beta \end{aligned}$$

is an isomorphism for any $i \in \mathbb{Z}$ and any subgroup $H \subset G$.

Proof. Take $H = G_p$. For $i = -1$, the map $\hat{H}^{-1}(G_p, \mathbb{Z}) \to \hat{H}^1(G_p, A)$ is surjective since $\hat{H}^1(G_p, A) = H^1(G_p, A) = 0$. For $i = 1$, the map $\hat{H}^1(G_p, \mathbb{Z}) \to \hat{H}^3(G_p, A)$ is injective since

$$\begin{aligned} \hat{H}^1(G_p, \mathbb{Z}) =& \mathrm{Hom}(G_p, \mathbb{Z}) \\ & \text{(since } \mathbb{Z} \text{ is a trivial } G_p\text{-module, and by Lemma 2.3.8)} \\ =& 0. \end{aligned}$$

For $i = 0$, we have

$$\hat{H}^0(G_p, \mathbb{Z}) = \frac{\mathbb{Z}^{G_p}}{N_{G_p}(\mathbb{Z})} = \frac{\mathbb{Z}}{|G_p|\mathbb{Z}},$$

The map $\hat{H}^0(G_p, \mathbb{Z}) \to \hat{H}^2(G_p, A)$ takes the image of $n \in \mathbb{Z}$ in $\hat{H}^0(G_p, \mathbb{Z})$ to $n\mathrm{Res}(\alpha)$, hence it is an isomorphism by the assumption on $H^2(G_p, A)$. Then Theorem 2.12.2 implies that all the maps are isomorphisms. □

3 Profinite Groups

3.1 Inverse systems and inverse limits

Definition 3.1.1. A *directed partially ordered set* $I = (I, \leq)$ is a non-empty set I together with a binary relation $\leq$ which satisfies the following conditions:
(i) (reflexive) $i \leq i$ for all $i \in I$.
(ii) (transitive) If $i \leq j$ and $j \leq k$, then $i \leq k$ for $i, j, k \in I$.
(iii) (antisymmetric) If $i \leq j$ and $j \leq i$, then $i = j$ for $i, j \in I$.
(iv) (directedness) If $i, j \in I$, then there exists some $k \in I$ such that $i \leq k, j \leq k$.

Definition 3.1.2. An *inverse system* (or *projective system*) of topological groups over I, is an object (G_i, φ_{ij}, I) where for each $i \in I$, G_i is a topological group, and for each $j \leq i$ in I, there is a morphism (continuous group homomorphism) $\varphi_{ij} : G_i \to G_j$ such that the diagram

$$\begin{array}{ccc} G_i & \xrightarrow{\varphi_{ij}} & G_j \\ & \searrow^{\varphi_{ik}} & \downarrow{\scriptstyle \varphi_{jk}} \\ & & G_k \end{array}$$

commutes whenever $i, j, k \in I$ and $k \leq j \leq i$. In addition, we assume that φ_{ii} is the identity map on G_i. We may simply write the inverse system as (G_i) if there is no confusion about the index set I.

Definition 3.1.3. Suppose (G_i, φ_{ij}, I) and $(G'_{i'}, \varphi'_{i'j'}, I')$ are two inverse systems. Let $\psi : I' \to I$ be an order preserving map (i.e., if $i' \leq j'$, then $\psi(i') \leq \psi(j')$). If for each $i' \in I'$, we have a morphism $f_{i'} : G_{\psi(i')} \to G'_{i'}$ such that the diagram

$$\begin{array}{ccc} G_{\psi(j')} & \xrightarrow{f_{j'}} & G'_{j'} \\ {\scriptstyle \varphi_{\psi(j')\psi(i')}}\downarrow & & \downarrow{\scriptstyle \varphi'_{j'i'}} \\ G_{\psi(i')} & \xrightarrow{f_{i'}} & G'_{i'} \end{array}$$

commutes whenever $i' \leq j'$ in I', then $\Psi = (\psi; f_{i'}, i' \in I')$ is a *morphism* from (G_i, φ_{ij}, I) to $(G'_{i'}, \varphi_{i'j'}, I')$.

Definition 3.1.4. The *inverse limit* (or *projective limit*)

$$G = \varprojlim_i G_i$$

of the inverse system (G_i, φ_{ij}, I) is the subgroup of the direct product $\prod_{i \in I} G_i$ of topological groups consisting of the tuples (g_i) that satisfy the condition $\varphi_{ij}(g_i) = g_j$ if $j \leq i$, and we assume that G has the topology induced by the product topology of $\prod_{i \in I} G_i$.

Lemma 3.1.5. *If (G_i, φ_{ij}, I) is an inverse system of Hausdorff topological groups, then $\varprojlim G_i$ is a closed subgroup of $\prod_{i\in I} G_i$.*

Proof. We show that $\left(\prod_{i\in I} G_i\right) \setminus \left(\varprojlim G_i\right)$ is open in $\prod_{i\in I} G_i$. Let $(g_i) \in \left(\prod_{i\in I} G_i\right) \setminus \left(\varprojlim G_i\right)$. Then there are some $m, n \in I$ such that $m \leq n$ and $\varphi_{nm}(g_n) \neq g_m$. Choose disjoint neighborhoods U and V of $\varphi_{nm}(g_n)$ and g_m in G_m, respectively. Let $U' \subset G_n$ be an open neighborhood of g_n such that $\varphi_{nm}(U') \subset U$. Consider the open subset $W = \prod_{i\in I} W_i \subset \prod_{i\in I} G_i$, where $W_n = U'$, $W_m = V$, and $W_i = G_i$ for $i \neq m, n$. Then W is an open neighborhood of (g_i) in $\left(\prod_{i\in I} G_i\right)$, disjoint from $\varprojlim G_i$. Hence $\left(\prod_{i\in I} G_i\right) \setminus \left(\varprojlim G_i\right)$ is open in $\prod_{i\in I} G_i$ and therefore, $\varprojlim G_i$ is closed in $\prod_{i\in I} G_i$. □

3.2 Topological structure of profinite groups

Definition 3.2.1. We say that $G = \varprojlim_i G_i$ is a *profinite group*, *pro-p group*, or *pronilpotent group* if all G_i are, respectively, finite groups, finite p-groups for a fixed prime p, or finite nilpotent groups, with the discrete topologies.

Example 3.2.2. Any finite group is trivially profinite.

To characterize profinite groups in terms of topological properties, we give some facts about topological groups.

Lemma 3.2.3. *(i) An open subgroup H of a topological group G is closed.*

(ii) If G is a compact topological group, then a subgroup H is open if and only if H is closed of finite index.

Proof. (i) Let H be an open subgroup of G, then every left coset xH is an open set in G. Since $H = G \setminus (\cup_{x\notin H} xH)$, H is closed.

(ii) ($\Rightarrow$): Suppose H be an open subgroup of G, then H is closed in G by (i), and the left coset xH is also an open subset of G. Moreover, the left cosets of H in G form an open cover of G, hence H has finite index by the compactness of G.

($\Leftarrow$): Suppose H is a closed subgroup of G of finite index. To prove that H is open, we will prove that the complement of H, which is $\cup_{x\notin H} xH$, is closed. Since H is of finite index, $\cup_{x\notin H} xH$ is a finite union of closed sets, hence $\cup_{x\notin H} xH$ is closed. Therefore, H is open. □

Recall that a topological space is *totally disconnected* if the only non-empty connected subsets are the one-point sets, or equivalently, if for any two points there is an open and closed subset containing exactly one of them.

Lemma 3.2.4. *Suppose G is a Hausdorff, compact, and totally disconnected topological group. If $\{N_i, i \in I\}$ is a set of open normal subgroups of G, then $\cap_{i\in I} N_i = \{1\}$.*

Theorem 3.2.5. *If G is a topological group, then G is profinite if and only if G is Hausdorff, compact, and totally disconnected.*

Corollary 3.2.6. *If G is a profinite group, then*

$$G \cong \varprojlim_N G/N$$

where N runs through all open normal subgroup of G.

Corollary 3.2.7. *Let G be a profinite group, and $H \subset G$ be a closed subgroup of G, then*

$$H \cong \varprojlim_N H/H \cap N$$

where N runs through all open normal subgroup of G.

Corollary 3.2.8. *Let G be a profinite group, and $H \subset G$ be a closed normal subgroup of G, then*

$$G/H \cong \varprojlim_N G/NH$$

where N runs through all open normal subgroup of G.

3.3 Examples of profinite groups

Let G be a topological group. Consider the family $\mathcal{N} = \{N_i, i \in I\}$ of all normal subgroups of finite index in G. Note that $\mathcal{N}$ is not empty because $G \in \mathcal{N}$. If $H \in \mathcal{N}, K \in \mathcal{N}$, then $H \cap K \in \mathcal{N}$. We make $\mathcal{N}$ into a directed partially ordered set by defining $j \leq i$ if N_i is an open subgroup of N_j for $N_i, N_j \in \mathcal{N}$. If $N_i, N_j \in \mathcal{N}$ and $j \leq i$, define $\varphi_{ij} : G/N_i \to G/N_j$ to be the natural homomorphism. Then $(G/N_i, \varphi_{ij}, I)$ is an inverse system of finite groups. We say that

$$\hat{G} = \varprojlim_{i \in I} G/N_i$$

is the *profinite completion* of G.

For a fixed prime p, if $\mathcal{N} = \{N_i, i \in I\}$ is the family of all normal subgroups of G of index a power of p, then

$$G_{\hat{p}} = \hat{G}_p = \varprojlim_{i \in I} G/N_i$$

is called the *pro-p completion* of G.

Example 3.3.1. As a special example, consider the group of integers $\mathbb{Z}$. Its profinite completion is

$$\hat{\mathbb{Z}} = \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z}.$$

This is isomorphic to the product of all p-adic integers:

$$\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p.$$

Its pro-p completion is

$$\hat{\mathbb{Z}}_p = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p.$$

Profinite groups also arise from Galois theory. Let E/F be a Galois extension of fields. Let $\{K_i, i \in I\}$ be the family of all finite intermediate Galois extensions: $F \subset K_i \subset E$ and K_i/F is a finite Galois extension. Then

$$E = \bigcup_{i\in I} K_i.$$

From Galois theory, we know that
(i) $\mathrm{Gal}(E/K_i)$ is a normal subgroup of $\mathrm{Gal}(E/F)$.
(ii) $\mathrm{Gal}(E/F)/\mathrm{Gal}(E/K_i) \cong \mathrm{Gal}(K_i/F)$ is a finite group.
(iii) If $i, j \in I$, then there is some $n \in I$ such that $\mathrm{Gal}(E/K_n)$ is a subgroup of $\mathrm{Gal}(E/K_i) \cap \mathrm{Gal}(E/K_j)$.
(iv) $\cap_{i\in I}\mathrm{Gal}(E/K_i) = \{1\}$.

There is a unique topology on $\mathrm{Gal}(E/F)$, called the *Krull topology*, such that the collection $\{\mathrm{Gal}(E/K_i), i \in I\}$ is a fundamental system of neighborhoods of the identity element 1 of $\mathrm{Gal}(E/F)$. If the Galois extension E/F is finite, then the Krull topology on $\mathrm{Gal}(E/F)$ is the discrete topology.

Consider the family of finite Galois groups $\{\mathrm{Gal}(K_i/F), i \in I\}$. We define the relation $j \le i$ if $K_j \subset K_i$, or equivalently, if $\mathrm{Gal}(E/K_i) \subset \mathrm{Gal}(E/K_j)$. Note that if K_{i_1}, K_{i_2} are finite Galois extensions of F contained in E, then so is the F-composite $K_{i_1}K_{i_2}$, which is some K_j, and $i_1 \le j, i_2 \le j$. Hence I is a directed partially ordered set. For $j \le i$, we define

$$\varphi_{ij} : \mathrm{Gal}(K_i/F) \to \mathrm{Gal}(K_j/F)$$

by restriction, that is, $\varphi_{ij}(\sigma) = \sigma|_{K_j}$, where $\sigma \in \mathrm{Gal}(K_i/F)$. Then $(\mathrm{Gal}(K_i/F), \varphi_{ij}, I)$ forms an inverse system of finite Galois groups.

Proposition 3.3.2. $\mathrm{Gal}(E/F) \cong \varprojlim_i \mathrm{Gal}(K_i/F)$. *In particular,* $\mathrm{Gal}(E/F)$ *is a profinite group.*

Proof. Consider the homomorphism

$$\Psi : \mathrm{Gal}(E/F) \to \varprojlim_i \mathrm{Gal}(K_i/F) \subset \prod_{i\in I} \mathrm{Gal}(K_i/F)$$
$$\sigma \mapsto (\sigma|_{K_i}).$$

We will prove that Ψ is an isomorphism (algebraically).

If $\sigma \neq 1$, then there exists $x \in E^*$ such that $\sigma(x) \neq x$, and there is some $i \in I$ such that $x \in K_i$. Now $\sigma|_{K_i} \neq 1$, so $\Psi(\sigma) = (\sigma|_{K_i}) \neq 1$. Hence Ψ is one-to-one.

Suppose $(\sigma_i) \in \varprojlim_i \mathrm{Gal}(K_i/F)$, define $\sigma : E \to E$ by $\sigma(x) = \sigma_i(x)$ for $x \in K_i$. Then $\sigma \in \mathrm{Gal}(E/F)$ and $\Psi(\sigma) = (\sigma_i)$. Hence Ψ is surjective.

Finally we use the isomorphism Ψ to transfer the topology from $\varprojlim_i \mathrm{Gal}(K_i/F)$ to $\mathrm{Gal}(E/F)$. □

We showed that every Galois group of a Galois extension can be interpreted as a profinite group in Proposition 3.3.2. Actually the converse is also true. Every profinite group can be realized as the Galois group of some field extensions.

Theorem 3.3.3. *Let G be a profinite group. Then it is the Galois group of some field extension.*

Remark 3.3.4. *Theorem 3.3.3 was proved in [Wat73] by generalizing Artin's theorem that finite automorphism groups are Galois groups. However, it is still unknown whether any profinite group is the Galois group of some field extension over a fixed base field.*

3.4 Direct systems and direct limits

Definition 3.4.1. Let $I = (I, \leq)$ be a directed partially ordered set. A *direct (or inductive) system* of abelian groups over I, is an object (A_i, φ_{ij}, I) where for each $i \in I$, A_i is an abelian group, and for each $i \leq j$ in I, there is a group homomorphism $\varphi_{ij} : A_i \to A_j$ such that the diagram

$$\begin{array}{ccc} A_i & \xrightarrow{\varphi_{ij}} & A_j \\ & \searrow^{\varphi_{ik}} & \downarrow{\scriptstyle \varphi_{jk}} \\ & & A_k \end{array}$$

commutes whenever $i, j, k \in I$ and $i \leq j \leq k$. In addition, we assume that φ_{ii} is the identity map on A_i. We may simply write the direct system as (A_i) or (A_i, φ_{ij}) if there is no confusion about the index set I.

Definition 3.4.2. Suppose (A_i, φ_{ij}, I) and $(A'_{i'}, \varphi'_{i'j'}, I')$ are two direct systems. Let $\psi : I \to I'$ be an order preserving map (i.e., if $i \leq j$, then $\psi(i) \leq \psi(j)$). If for each $i \in I$, we have a homomorphism $f_i : A_i \to A'_{\psi(i)}$ such that the diagram

$$\begin{array}{ccc} A_i & \xrightarrow{f_i} & A'_{\psi(i)} \\ {\scriptstyle \varphi_{ij}}\downarrow & & \downarrow{\scriptstyle \varphi'_{\psi(i)\psi(j)}} \\ A_j & \xrightarrow{f_j} & A'_{\psi(j)} \end{array}$$

commutes whenever $i \leq j$ in I, then $\Psi = (\psi; f_i, i \in I)$ is a *morphism* from (A_i, φ_{ij}, I) to $(A'_{i'}, \varphi'_{i'j'}, I')$.

Definition 3.4.3. The *direct limit* of the direct system (A_i, φ_{ij}, I) is defined as the disjoint union of the groups A_i module an equivalence relation

$$\varinjlim A_i = \sqcup_{i \in I} A_i / \sim$$

where for $x \in A_i, y \in A_j$, $x \sim y$ if there exists some $k \in I$ with $i \leq k, j \leq k$ such that $\varphi_{ik}(x) = \varphi_{jk}(y)$.

3.5 Discrete G-modules

Let G be a profinite group and A a (left) G-module. If H is an open subgroup of G, A^H is the group of H-invariants in A. A G-module A satisfying

$$A = \bigcup_{N \text{ open normal subgroup of } G} A^N$$

is called a *discrete G-module*.

Remark 3.5.1. *In the definition, "normal" doesn't matter so much. In fact, for a G-module A,*

$$\bigcup_{N \text{ open normal subgroup of } G} A^N = \bigcup_{H \text{ open subgroup of } G} A^H.$$

The direction $\subseteq$ is trivial. To see the other direction, let $a \in \bigcup_{H \text{ open subgroup of } G} A^H$, then there is some open subgroup H of G such that $a \in A^H$. Let $N = \bigcap_{g \in G} g^{-1}Hg$. Since G is compact, N is a finite intersection of open sets, hence N is open. N is also a normal subgroup of G. Moreover, $N \subset H$. Hence $a \in A^H \subset A^N$.

Proposition 3.5.2. *Let G be a profinite group, and A be a G-module. The following are equivalent.*
(i) A is a discrete G-module.
(ii) For every $a \in A$, the stabilizer $Stab_G(a) = \{g \in G : ga = a\}$ is an open subgroup of G.
(iii) The multiplication map $G \times A \to A$ is continuous, where G has the usual topology for profinite groups and A is given the discrete topology.

Proof. (i) $\Rightarrow$ (iii): Let $(g, a) \in G \times A$. Then there is some open normal subgroup N of G such that $a \in A^N$. Then $gN \times \{a\}$ is an open neighborhood of $(g, a) \in G \times A$ mapping to ga. Hence the multiplication map $G \times A \to A$ is continuous.

(iii) $\Rightarrow$ (ii): Let $a \in A$. Consider the restriction of the multiplication map to $G \times \{a\}$. The preimage of $a \in A$ is $\mathrm{Stab}_G(a) \times \{a\}$, which must be an open set. Hence $\mathrm{Stab}_G(a)$ is open.

(ii) $\Rightarrow$ (i): For any $a \in A$, there is an open normal subgroup

$$N = \bigcap_{g \in G} g^{-1}\mathrm{Stab}_G(a)g$$

of G that is contained in $\mathrm{Stab}_G(a)$, so $a \in A^{\mathrm{Stab}_G(a)} \subset A^N$. □

Example 3.5.3. Let G be a profinite group. Then any G-module A with the trivial G-action is a discrete G-module. Less trivial examples of discrete G-modules come from Galois theory. Let E/F be a Galois extension of fields with $G = \mathrm{Gal}(E/F)$. The following are discrete G-modules with action defined by $g \cdot a = g(a)$:
(i) the additive group E;
(ii) the multiplicative group $E^* = E\backslash\{0\}$;
(iii) the multiplicative group of roots of 1 in E.

3.6 Cohomology of profinite groups

Let G be a profinite group and A a discrete G-module. For $n \geq 0$, we consider the group of n-th continuous cochains $C^n(G, A) = \{\varphi : G^n \to A \mid \varphi \text{ is continuous}\}$ and define the $n-$th (continuous) differential $d^n : C^n(G, A) \to C^{n+1}(G, A)$ by

$$\begin{aligned} d^n(\varphi)(g_0, g_1, \cdots, g_n) =& g_0\varphi(g_1, \cdots, g_n) + \sum_{j=1}^{n}(-1)^j\varphi(g_0, \cdots, g_{j-2}, g_{j-1}g_j, \cdots, g_n) \\ &+ (-1)^{n+1}\varphi(g_0, \cdots, g_{n-1}). \end{aligned}$$

Then $(C^n(G, A), d^n)$ is a cochain complex.

Definition 3.6.1. We define the *n-th cohomology group* of the profinite group G with coefficients in the discrete G-module A to be

$$H^n(G, A) = \frac{Z^n(G, A)}{B^n(G, A)},$$

where $Z^n(G, A) = \ker d^n$ for $n \geq 0$ are the (continuous) n-cocycles and $B^0(G, A) = 0$, $B^n(G, A) = \text{im } d^{n-1}$ for $n \geq 1$ are the (continuous) n-coboundaries.

The cohomology group $H^n(G, A)$ of a profinite group G with coefficients in a discrete G-module A are actually built up from the cohomology groups of finite groups. Let $\mathcal{N} = \{N_i, i \in I\}$ be the family of all open normal subgroups of G (hence G/N_i is finite, by Lemma 3.2.3). We define $i \leq j$ if U_j is an open subgroup of U_i. If $N_j \subset N_i$, then the projections

$$G^{n+1} \to (G/N_j)^{n+1} \to (G/N_i)^{n+1}$$

induce homomorphisms

$$C^n(G/N_i, A^{N_i}) \to C^n(G/N_j, A^{N_j}) \to C^n(G, A).$$

Hence we have homomorphisms

$$H^n(G/N_i, A^{N_i}) \to H^n(G/N_j, A^{N_j}) \xrightarrow{\text{Inf}} H^n(G, A).$$

We define $\varphi_{ij} : H^n(G/N_i, A^{N_i}) \to H^n(G/N_j, A^{N_j})$. Then $(H^n(G/N_i, A^{N_i}), \varphi_{ij}, I)$ is a direct system.

Proposition 3.6.2. *Let G be a profinite group, and A be a discrete G-module. For any nonnegative integer $n \geq 0$, we have*

$$H^n(G, A) \cong \varinjlim_i H^n(G/N_i, A^{N_i}),$$

where $(H^n(G/N_i, A^{N_i}), \varphi_{ij}, I)$ is a direct system describe above.

3.7 Galois cohomology

Let E/F be a Galois extension with Galois group $G = \mathrm{Gal}(E/F)$, which is a profinite group by Proposition 3.3.2. Let $\{K_i, i \in I\}$ be the family of all finite Galois extensions of F contained in E, and denote $N_i = \mathrm{Gal}(E/K_i)$, which are open normal subgroups of G. Then

$$G = \varprojlim_i G/N_i$$

by Corollary 3.2.6.

Consider the additive group E, which is a discrete G-module. We have $E^{N_i} = K_i$, each K_i is a $\mathrm{Gal}(K_i/F)$-module and $\mathrm{Gal}(K_i/F) \cong G/N_i$. Let $n \geq 0$ be an integer. Then

$$H^n(G, E) = \varinjlim_i H^n(G/N_i, E^{N_i}) \cong \varinjlim_i H^n(\mathrm{Gal}(K_i/F), K_i).$$

Proposition 3.7.1. *Let E/F be a Galois extension with Galois group $G = \mathrm{Gal}(E/F)$. Then $H^n(G, E) = 0$ for all $n \geq 1$.*

Proof. This is a consequence of Proposition 3.7.2. □

Proposition 3.7.2. *Let E/F be a finite Galois extension with Galois group $G = \mathrm{Gal}(E/F)$. Then the Tate cohomology groups $\hat{H}^n(G, E) = 0$ for all $n \in \mathbb{Z}$.*

Proof. The Normal Basis Theorem says that there is an element $\alpha \in E$ such that $\{g(\alpha), g \in G\}$ is a basis of E/F. So $E \cong \mathbb{Z}[G] \otimes F$ is an induced G-module, hence cohomologically trivial. □

The cohomology of $\mathrm{Gal}(E/F)$ with coefficients in the additive group E is uninteresting.

Now we look at the multiplicative group $E^* = E\backslash\{0\}$ of E. Again, we have $(E^*)^{N_i} = K_i^*$, each K_i^* is a $\mathrm{Gal}(K_i/F)$-module and $\mathrm{Gal}(K_i/F) \cong G/N_i$. Let $n \geq 0$ be an integer. Then

$$H^n(G, E^*) = \varinjlim_i H^n(G/N_i, (E^*)^{N_i}) \cong \varinjlim_i H^n(\mathrm{Gal}(K_i/F), K_i^*).$$

Proposition 3.7.3 (Hilbert's Theorem 90, Cohomology Version)**.** *Let E/F be a Galois extension with Galois group $G = \mathrm{Gal}(E/F)$. Then $H^1(G, E^*) = 0$.*

Proof. Let $\varphi : G \to E^*$ be a 1-cocycle (note that the multiplicative version of crossed homomorphism is $\varphi(xy) = x(\varphi(y))\varphi(y), \forall x, y \in G$). By the algebraic independence of automorphisms, there is some $a \in E^*$ such that

$$b = \sum_{x \in G} \varphi(x) \cdot x(a)$$

is non-zero, i.e., $b \in E^*$. Let $y \in G$. Then

$$\begin{aligned} y(b) =& \sum_{x \in G} [y(\varphi(x))] \cdot [y \circ x(a)] \\ =& \sum_{x \in G} \varphi^{-1}(y) \cdot \varphi(yx) \cdot [y \circ x(a)] \\ =& \varphi^{-1}(y) \sum_{x \in G} \varphi(yx) \cdot [y \circ x(a)] \\ =& \varphi^{-1}(y) \sum_{z \in G} \varphi(z) \cdot z(a) \\ =& \varphi^{-1}(y) \cdot b. \end{aligned}$$

So $\varphi(y) = b \cdot y(b)^{-1}$. Replacing b with b^{-1}, we get $\varphi(y) = b^{-1} \cdot y(b^{-1})^{-1} = y(b) \cdot b^{-1}$. Hence φ is a 1-coboundary. □

Proposition 3.7.4 (Hilbert's Theorem 90)**.** *Let E/F be a finite cyclic extension with Galois group $G = \mathrm{Gal}(E/F)$ generated by σ. If $x \in E^*$ has norm 1, then there exists $y \in E^*$ such that $x = \frac{y}{\sigma(y)}$.*

Proof. Since G is finite cyclic, we have

$$H^1(G, E^*) = \frac{\{x \in E^* : N_{E/F}(x) = 1\}}{(1-\sigma)(E^*)} = \frac{\{x \in E^* : N_{E/F}(x) = 1\}}{\{\frac{y}{\sigma(y)}, y \in E^*\}}$$

by Proposition 2.10.1. The result follows since $H^1(G, E^*) = 0$ by Proposition 3.7.3. □

Definition 3.7.5. Let k be a field, let k^{sep} be a separable closure of k. The Brauer group of k is defined to be

$$\mathrm{Br}\ (k) = H^2(\mathrm{Gal}(k^{\mathrm{sep}}/k), k^{\mathrm{sep}*}).$$

Remark 3.7.6. *By definition, the Brauer group of a field k is the direct limit*

$$Br\ (k) = \varinjlim_i H^2(\mathrm{Gal}(K_i/k), K_i^*)$$

where $\{K_i, i \in I\}$ is the family of all finite Galois extension of k contained in k^{sep}.

Example 3.7.7. The Brauer group of the field $\mathbb{R}$ is

$$\mathrm{Br}\ (\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}.$$

This is because $\mathbb{R}^{\mathrm{sep}} = \mathbb{C}$, and $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ is finite cyclic of order 2. Hence

$$\mathrm{Br}\ (\mathbb{R}) = H^2(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^*) = \hat{H}^0(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^*) = \frac{\mathbb{C}^{*\mathrm{Gal}(\mathbb{C}/\mathbb{R})}}{N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^*)} = \frac{\mathbb{R}^*}{\mathbb{R}_+^*} \cong \mathbb{Z}/2\mathbb{Z}.$$

Proposition 3.7.8. *Let $k \subset K \subset L$ be a tower of field extensions with $L/k, K/k$ Galois. Then there is an exact sequence*

$$0 \longrightarrow H^2(\mathrm{Gal}(K/k), K^*) \to H^2(\mathrm{Gal}(L/k), L^*) \to H^2(\mathrm{Gal}(L/K), L^*).$$

Proof. Take $G = \mathrm{Gal}(L/k)$, $H = \mathrm{Gal}(L/K)$. Hilbert's Theorem 90 implies that $H^1(H, L^*) = 0$. The result follows by Proposition 2.6.10. □

Corollary 3.7.9. *Let K/k be a Galois extension. Then there is an exact sequence*

$$0 \longrightarrow H^2(\mathrm{Gal}(K/k), K^*) \to Br\,(k) \to Br\,(K).$$

Corollary 3.7.10. *Let $\{K_i, i \in I\}$ be the family of all finite Galois extensions of a field k in a separable closure k^{sep}. Then*

$$Br\,(k) = \bigcup_{i \in I} H^2(\mathrm{Gal}(K_i/k), K_i^*).$$

4 Local Class Field Theory

4.1 Statements of the main theorems

Recall that a field K is a *nonarchimedean local field* if it is complete with respect to the topology induced by a discrete valuation $v : K^* \twoheadrightarrow \mathbb{Z}$ with finite residue field.

Let K be a local field. If K is archimedean, then K is either $\mathbb{R}$ or $\mathbb{C}$. If K is nonarchimedean, then K is either a finite extension of the p-adic field $\mathbb{Q}_p$ for some prime p, or a finite extension of the field of formal Laurent series $\mathbb{F}_p((T))$ over a finite field $\mathbb{F}_p$. We are interested in the case where K is nonarchimedean.

Furthermore, for a nonarchimedean local field K, we denote:

$$\begin{aligned}
K^* &:= K\backslash\{0\} = \text{ the multiplicative group of } K,\\
\mathcal{O}_K &:= \{x \in K \mid v(x) \geq 0\} = \text{ the valuation ring of } K,\\
\mathfrak{m}_K &:= \{x \in K \mid v(x) > 0\} = \text{ the unique maximal ideal of } \mathcal{O}_K,\\
k &:= \mathcal{O}_K/\mathfrak{m}_K = \text{ the residue field of } K,\\
U_K &:= \{x \in K \mid v(x) = 0\} = \text{ the units of } \mathcal{O}_K,\\
U_K^{(n)} &:= 1 + \mathfrak{m}_K^n \text{ for } n \geq 1,\\
\pi &:= \text{ a prime element (uniformizer) of } K = \text{ a generator of } \mathfrak{m}_K\\
&\quad (\text{ such that } \mathfrak{m}_K = \pi\mathcal{O}_K),\\
\overline{K} &:= \text{ the algebraic closure of } K,\\
K^{\text{sep}} &:= \text{ a fixed separable closure of } K,\\
K^{\text{unr}} &:= \text{ the maximal unramified extension of } K \text{ in } K^{\text{sep}},\\
K^{\text{ab}} &:= \text{ the maximal abelian extension of } K \text{ in } K^{\text{sep}}.
\end{aligned}$$

Let L be a finite unramified extension over a nonarchimedean local field K. Then L is Galois over K, and $\mathrm{Gal}(L/K) = \mathrm{Gal}(l/k)$, where l is the residue field of L. Moreover, $\mathrm{Gal}(L/K)$ is a finite cyclic group, generated by the Frobenius element $\mathrm{Frob}_{L/K}$.

Theorem 4.1.1 (Local Reciprocity Law)**.** *Let K be a nonarchimedean local field. Then there exists a unique homomorphism*

$$\phi_K : K^* \to \mathrm{Gal}(K^{ab}/K)$$

satisfying the following properties:

(i) For every prime element $\pi \in K$ and every finite unramified extension L/K, $\phi_K(\pi)$ acts on L as $Frob_{L/K}$.

(ii) For every finite abelian extension L/K, $N_{L/K}(L^*)$ is contained in the kernel of the map $x \mapsto \phi_K(x)|L$, and ϕ_K induces an isomophism

$$\phi_{L/K} : K^*/N_{L/K}(L^*) \to \mathrm{Gal}(L/K).$$

Remark 4.1.2. *The maps $\phi_K, \phi_{L/K}$ are usually called the local Artin maps, the local reciprocity maps, or the norm residue symbols.*

Remark 4.1.3. *Local Reciprocity Law says that the following diagram*

$$\begin{array}{ccc} K^* & \xrightarrow{\phi_K} & \mathrm{Gal}(K^{ab}/K) \\ \downarrow & & \downarrow \\ \dfrac{K^*}{N_{L/K}(L^*)} & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

is commutative. This implies that for all finite extensions $K \subset E \subset L$ with L/K and E/K abelian, the diagram

$$\begin{array}{ccc} \dfrac{K^*}{N_{L/K}(L^*)} & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K) \\ \downarrow & & \downarrow \\ \dfrac{K^*}{N_{E/K}(E^*)} & \xrightarrow{\phi_{E/K}} & \mathrm{Gal}(E/K) \end{array}$$

is commutative.

Definition 4.1.4. A subgroup H of K^* is called a *norm subgroup* if there exists a finite abelian extension L/K such that $H = N_{L/K}(L^*)$.

Corollary 4.1.5. *Let K be a nonarchimedean local field. The map $L \mapsto N_{L/K}(L^*)$ is a bijection between the set of all finite abelian extensions and the set of norm subgroups of K^*.*

Corollary 4.1.5 says that finite abelian extension of a nonarchimedean local field K corresponds bijectively to a norm subgroup of K^*. But this is unsatisfactory because to define norm subgroup we still need to know the extension. Local Existence Theorem (Theorem 4.1.6) gives a topological characterization of the norm subgroups of K^*. Hence we can characterize finite abelian extension of K totally in terms of the arithmetic of the ground field K.

Theorem 4.1.6 (Local Existence Theorem)**.** *A subgroup H in K^* is a norm subgroup if and only if H is open of finite index in K^*.*

Part (i) of Local Reciprocity Law will be proved by Proposition 4.3.8 and Remark 4.3.9. Part (ii) of Local Reciprocity Law will be proved by Theorem 4.3.2 and Remark 4.3.3. Local Existence Theorem will be proved by Proposition 4.4.25 and Proposition 4.4.26.

4.2 The fundamental class

In this section, we will prove that for a finite Galois extension L of degree n over a nonarchimedean local field K, $\hat{H}^2(\mathrm{Gal}(L/K), L^*)$ is cyclic of order n, generated by the "fundamental class".

Lemma 4.2.1. *Let K be a nonarchimedean local field. Let L/K be a finite unramified extension. We have*

$$U_L/U_L^{(1)} \cong l^*,$$

and

$$U_L^{(i)}/U_L^{(i+1)} \cong l$$

as $\mathrm{Gal}(L/K)$-modules for any $i \geq 1$, where l is the residue field of L.

Proof. Note that since L/K is unramified, a prime element π of K is also a prime element of L. So

$$U_L^{(i)} = 1 + \mathfrak{m}_L^i = \{1 + a\pi^i \mid a \in \mathcal{O}_L\}.$$

The isomorphisms follow from the maps

$$\begin{aligned} U_L &\to l^* \\ u &\mapsto u \mod \mathfrak{m}_L \end{aligned}$$

and

$$\begin{aligned} U_L^{(i)} &\to l \\ 1 + a\pi^i &\mapsto a \mod \mathfrak{m}_L \end{aligned}$$

□

Lemma 4.2.2. *Let K be a nonarchimedean local field. Let L/K be a finite unramified extension. Then $\hat{H}^i(\mathrm{Gal}(L/K), l^*) = 0$ for all $i \in \mathbb{Z}$.*

Proof. Since L/K is finite unramified, $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(l/k)$ and $\mathrm{Gal}(L/K)$ is finite cyclic. Moreover, l^* is finite since it is the residue field of L. In particular, l^* is a finite $\mathrm{Gal}(L/K)$-module. Hence the Herbrand quotient

$$h(l^*) = \frac{|\hat{H}^0(\mathrm{Gal}(L/K), l^*)|}{|\hat{H}^1(\mathrm{Gal}(L/K), l^*)|} = 1$$

by Proposition 2.10.6. Hilbert's Theorem 90 implies that $\hat{H}^1(\mathrm{Gal}(L/K), l^*) = 0$. Hence $\hat{H}^0(\mathrm{Gal}(L/K), l^*) = 0$. Therefore, $\hat{H}^i(\mathrm{Gal}(L/K), l^*) = 0$ for all $i \in \mathbb{Z}$ since $\hat{H}^i(\mathrm{Gal}(L/K), l^*)$ is 2-periodic. □

Remark 4.2.3. *Lemma 4.2.2 implies that the norm map $N_{l/k} : l^* \to k^*$ is surjective. Note that the map $N : H_0(\mathrm{Gal}(L/K), l^*) \to H^0(\mathrm{Gal}(L/K), l^*)$ induced by the norm element is exactly the norm $N_{l/k} : l^* \to k^*$. Now*

$$\hat{H}^0(\mathrm{Gal}(l/k), l^*) = \frac{(l^*)^{\mathrm{Gal}(l/k)}}{N_{l/k}(l^*)} = \frac{k^*}{N_{l/k}(l^*)} = 0,$$

hence $N_{l/k}(l^*) = k^*$.

Lemma 4.2.4. *Let K be a nonarchimedean local field. Let L/K be a finite unramified extension. Then $\hat{H}^i(\mathrm{Gal}(L/K), l) = 0$ for all $i \in \mathbb{Z}$.*

Proof. Since L/K is finite unramified, $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(l/k)$ and $\mathrm{Gal}(L/K)$ is finite cyclic. The result follows from Proposition 3.7.2. □

Remark 4.2.5. *Similarly, Lemma 4.2.4 implies that the trace map $T_{l/k} : l \to k$ is surjective.*

Proposition 4.2.6. *Let K be a nonarchimedean local field. Let L/K be a finite unramified extension. Then the norm $N_{L/K} : U_L \to U_K$ is surjective.*

Proof. Let $u \in U_K$. We know that the norm map $N : l^* \to k^*$ is surjective, by Remark 4.2.3. We also know that

$$l^* \cong U_L/U_L^{(1)},$$

and

$$k^* \cong U_K/U_K^{(1)},$$

by Lemma 4.2.1. So there exists $v_0 \in U_L$ such that $N(v_0)U_K^{(1)} \equiv u \mod U_K^{(1)}$, i.e., $u/N(v_0) \in U_K^{(1)}$. We know that the trace map $T : l \to k$ is surjective, by Remark 4.2.5. Also, by Lemma 4.2.1, we have

$$l \cong U_L^{(i)}/U_L^{(i+1)},$$

and

$$k \cong U_K^{(i)}/U_K^{(i+1)},$$

for all $i \geq 1$. The norm map $N : U_L^{(1)}/U_L^{(2)} \to U_K^{(1)}/U_K^{(2)}$ is induced by the map $N : U_L^{(1)} \to U_K^{(1)}/U_K^{(2)}$ where

$$\begin{aligned}
N(1+\pi x) &= \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(1+\pi x) \\
&= \prod_{\sigma \in \mathrm{Gal}(L/K)} (1+\sigma(\pi x)) \\
&= 1 + \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\pi x) \mod \pi^2 \\
&= 1 + T(\pi x) \mod \pi^2 \\
&= T(\pi x) \mod U_K^{(2)}.
\end{aligned}$$

So the norm map $N : U_L^{(1)}/U_L^{(2)} \to U_K^{(1)}/U_K^{(2)}$ is also surjective. So there exists $v_1 \in U_L^{(1)}$ such that $N(v_1)U_K^{(2)} \equiv u/N(v_0) \mod U_K^{(2)}$, i.e., $u/N(v_0v_1) \in U_K^{(2)}$. We can proceed in this way to find a sequence $v_0 \in U_L, v_1 \in U_L^{(1)}, v_2 \in U_L^{(2)}, \cdots, v_n \in U_L^{(n)}$ such that $u/N(v_0v_1 \cdots v_n) \in U_K^{(n+1)}$. Let $v = \prod_{i=0}^{\infty} v_i$. Notice that

$$u/N(v) \in \bigcap_{i=1}^{\infty} U_K^{(i)} = \{1\}.$$

Therefore, $N(v) = u$. Hence the norm map $N_{L/K} : U_L \to U_K$ is surjective. □

Corollary 4.2.7. *Let K be a nonarchimedean local field. Let L/K be an arbitrary unramified extension (possibly infinite). Then*

$$\hat{H}^i(\mathrm{Gal}(L/K), U_L) = 0$$

for all $i \in \mathbb{Z}$ when $\mathrm{Gal}(L/K)$ is finite, and for all $i \geq 1$ when $\mathrm{Gal}(L/K)$ is infinite.

Proof. First consider the case where L/K is a finite unramified extension, then $\mathrm{Gal}(L/K)$ is finite cyclic. A prime element $\pi \in K$ is also a prime element in L. So

$$L^* \cong U_L \times \pi^{\mathbb{Z}}.$$

Hence, we have

$$\hat{H}^i(\mathrm{Gal}(L/K), L^*) \cong \hat{H}^i(\mathrm{Gal}(L/K), U_L) \oplus \hat{H}^i(\mathrm{Gal}(L/K), \pi^{\mathbb{Z}})$$

Hilbert's Theorem 90 says that $\hat{H}^1(\mathrm{Gal}(L/K), L^*) = 0$ and so $\hat{H}^1(\mathrm{Gal}(L/K), U_L) = 0$ as well. By Proposition 4.2.6, we have

$$\hat{H}^0(\mathrm{Gal}(L/K), U_L) = \frac{{U_L}^{\mathrm{Gal}(L/K)}}{N_{L/K}(U_L)} = \frac{U_K}{U_K} = 0.$$

Hence $\hat{H}^i(\mathrm{Gal}(L/K), U_L) = 0$ for all $i \in \mathbb{Z}$ since the Tate cohomology groups are 2-periodic.

Now suppose L/K is unramified and possibly infinite. We no longer have well-defined Tate cohomology groups for $i < 0$, but we can work with the cohomology groups $H^i(\mathrm{Gal}(L/K), U_L)$ for $i \geq 1$. In this case, we have

$$H^i(\mathrm{Gal}(L/K), U_L) = \varinjlim_{K_i \text{ finite unramified over } K} H^i(\mathrm{Gal}(K_i/K), U_{K_i}).$$

Since each term in the direct limit is 0, we have $H^i(\mathrm{Gal}(L/K), U_L) = 0$. This completes the proof. □

Remark 4.2.8. *Corollary 4.2.7 implies that* $H^i(\mathrm{Gal}(K^{unr}/K), U_K^{unr}) = 0$ *for the maximal unramified extension* K^{unr}/K *for all* $i > 0$.

Corollary 4.2.9. *Let* K *be a nonarchimedean local field. Let* L/K *be an arbitrary unramified extension (possibly infinite). Then*

$$\hat{H}^i(\mathrm{Gal}(L/K), L^*) \cong \hat{H}^i(\mathrm{Gal}(L/K), \mathbb{Z})$$

for all $i \in \mathbb{Z}$ *when* $\mathrm{Gal}(L/K)$ *is finite, and for all* $i \geq 1$ *when* $\mathrm{Gal}(L/K)$ *is infinite.*

Proof. We have an exact sequence

$$0 \longrightarrow U_L \longrightarrow L^* \xrightarrow{\mathrm{ord}_L} \mathbb{Z} \longrightarrow 0$$

of $\mathrm{Gal}(L/K)$-modules where $\mathrm{Gal}(L/K)$ acts trivially on $\mathbb{Z}$. The long exact sequence of Tate cohomology together with Corollary 4.2.7 give us the isomorphism. □

Let L/K be unramified of finite degree n over a nonarchimedean local field K. Now consider the exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \to 0$$

of $\mathrm{Gal}(L/K)$-modules with trivial actions. Since multiplication by any positive integer (in particular, $|\mathrm{Gal}(L/K)|$) on $\mathbb{Q}$ is an isomorphism $\mathbb{Q} \to \mathbb{Q}$, hence an isomorphism $\hat{H}^i(\mathrm{Gal}(L/K), \mathbb{Q}) \to \hat{H}^i(\mathrm{Gal}(L/K), \mathbb{Q})$. But $\mathrm{Gal}(L/K)$ is finite, hence $\hat{H}^i(\mathrm{Gal}(L/K), \mathbb{Q}) = 0$ for all $i \in \mathbb{Z}$. By the long exact sequence of the Tate cohomology, we have

$$\hat{H}^1(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) \cong \hat{H}^2(\mathrm{Gal}(L/K), \mathbb{Z}).$$

By Corollary 4.2.9, we have the isomorphism

$$\hat{H}^2(\mathrm{Gal}(L/K), L^*) \cong \hat{H}^1(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}).$$

Since $\mathbb{Q}/\mathbb{Z}$ is a trivial $\mathrm{Gal}(L/K)$-module,

$$\hat{H}^1(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z})$$

by Lemma 2.3.8. The map

$$\begin{aligned} \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) &\to \mathbb{Q}/\mathbb{Z} \\ f &\mapsto f(\mathrm{Frob}_{L/K}) \end{aligned}$$

is an isomorphism from $\mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z})$ onto a subgroup $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ of $\mathbb{Q}/\mathbb{Z}$ (because L/K is unramified). We define the *invariant map* to be the composition

$$\begin{aligned} \mathrm{inv}_{L/K} : \hat{H}^2(\mathrm{Gal}(L/K), L^*) \cong \hat{H}^2(\mathrm{Gal}(L/K), \mathbb{Z}) \cong \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) &\to \mathbb{Q}/\mathbb{Z} \\ f &\mapsto f(\mathrm{Frob}_{L/K}). \end{aligned}$$

The invariant map is compatible with inflation in the following sense.

Proposition 4.2.10. *Let K be a nonarchimedean local field. Let $K \subset L \subset E$ be a tower of fields with both L and E contained in K^{unr}. Then the diagram*

$$\begin{array}{ccc} \hat{H}^2(\mathrm{Gal}(L/K), L^*) & \xrightarrow{inv_{L/K}} & \mathbb{Q}/\mathbb{Z} \\ \downarrow Inf & & \downarrow = \\ \hat{H}^2(\mathrm{Gal}(E/K), E^*) & \xrightarrow{inv_{E/K}} & \mathbb{Q}/\mathbb{Z} \end{array}$$

is commutative.

Proposition 4.2.11. *Let K be a nonarchimedean local field. There is a canonical isomorphism*

$$inv_K : H^2(\mathrm{Gal}(K^{unr}/K), K^{unr*}) \cong \mathbb{Q}/\mathbb{Z}.$$

Proof. Let $\{L_i, i \in I\}$ be the family of all finite unramified extension of K. Then

$$H^2(\mathrm{Gal}(K^{\mathrm{unr}}/K), K^{\mathrm{unr}*}) \cong \varinjlim_i H^2(\mathrm{Gal}(L_i/K), L_i^*).$$

For every positive integer n, there exists an unramified extension L_n of degree n. Hence the image of inv_K contains $\frac{1}{n}$ for every n. Thus inv_K is an isomorphism. □

Proposition 4.2.12. *Let K be a nonarchimedean local field. Let L/K be a finite extension of degree n. Then the diagram*

$$\begin{array}{ccc} H^2(\mathrm{Gal}(K^{unr}/K), K^{unr*}) & \xrightarrow{Res} & H^2(\mathrm{Gal}(L^{unr}/L), L^{unr*}) \\ \downarrow inv_K & & \downarrow inv_L \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{\quad n \quad} & \mathbb{Q}/\mathbb{Z} \end{array}$$

is commutative.

Corollary 4.2.13. *Let K be a nonarchimedean local field. Let L/K be a finite extension of degree n. Let $H^2(L/K)_{unr} = H^2(\mathrm{Gal}(L/K), L^*) \cap H^2(\mathrm{Gal}(K^{unr}/K), K^{unr*})$. Then $H^2(L/K)_{unr}$ is cyclic of order n and is generated by the element $u_{L/K} \in H^2(\mathrm{Gal}(K^{unr}/K), K^{unr*})$ with $inv_K(u_{L/K}) = \frac{1}{n}$.*

Proof. The sequence

$$0 \longrightarrow H^2(L/K)_{\mathrm{unr}} \to H^2(\mathrm{Gal}(K^{\mathrm{unr}}/K), K^{\mathrm{unr}*}) \xrightarrow{\mathrm{Res}} H^2(\mathrm{Gal}(L^{\mathrm{unr}}/L), L^{\mathrm{unr}*})$$

is exact. By Proposition 4.2.12, the diagram

$$\begin{array}{ccccc} 0 \longrightarrow H^2(L/K)_{\mathrm{unr}} & \to & H^2(\mathrm{Gal}(K^{\mathrm{unr}}/K), K^{\mathrm{unr}*}) & \xrightarrow{\mathrm{Res}} & H^2(\mathrm{Gal}(L^{\mathrm{unr}}/L), L^{\mathrm{unr}*}) \\ & & \downarrow \mathrm{inv}_K & & \downarrow \mathrm{inv}_L \\ 0 \longrightarrow \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{\quad n \quad} & \mathbb{Q}/\mathbb{Z} \end{array}$$

is commutative with exact rows. Since inv_K and inv_L are isomorphisms by Proposition 4.2.11, we obtain that $H^2(L/K)_{\mathrm{unr}} \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ and hence the results follow. □

Corollary 4.2.14. *Let K be a nonarchimedean local field. Let L/K be a finite extension of degree n. Then n divides the order of $H^2(\mathrm{Gal}(L/K), L^*)$.*

Proof. Corollary 4.2.13 says that $H^2(\mathrm{Gal}(L/K), L^*)$ contains a subgroup of order n. $\mathrm{Gal}(L/K)$ is a finite group, and L^* is a finite generated $\mathrm{Gal}(L/K)$-module by the Normal Basis Theorem. Then Corollary 2.7.14 implies that $H^2(\mathrm{Gal}(L/K), L^*)$ is finite. Now Lagrange's Theorem in group theory implies that n divides the order of $H^2(\mathrm{Gal}(L/K), L^*)$. □

We have shown that for a finite unramified extension L over a nonarchimedean local field K, we have $\hat{H}^i(\mathrm{Gal}(L/K), U_L) = 0$ for all i, by Corollary 4.2.7. Such strong results do not hold for an arbitrary finite Galois extension. But we have the following results.

Lemma 4.2.15. *Let K be a nonarchimedean local field. Let L/K be a finite Galois extension with Galois group $\mathrm{Gal}(L/K)$. There exists an open subgroup V of $\mathcal{O}_L$ stable under the action and*

$$\hat{H}^i(\mathrm{Gal}(L/K), V) = 0$$

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

Proof. Normal Basis Theorem says that there is an element $x \in L$ such that $\{\sigma(x) \mid \sigma \in \mathrm{Gal}(L/K)\}$ is a basis for L/K. Then there is a common denominator d in $\mathcal{O}_K$ because $\mathrm{Gal}(L/K)$ is finite. Let $y_\sigma = d\sigma(x)$. Then $\{y_\sigma \mid \sigma \in \mathrm{Gal}(L/K)\}$ is a basis of L/K with elements in $\mathcal{O}_L$. Let $V = \sum_{\sigma \in \mathrm{Gal}(L/K)} \mathcal{O}_L y_\sigma$. Then

$$V \cong \mathcal{O}_L[\mathrm{Gal}(L/K)] \cong \mathbb{Z}[\mathrm{Gal}(L/K)] \otimes \mathcal{O}_L,$$

i.e., V is an induced $\mathrm{Gal}(L/K)$-module. Hence $\hat{H}^i(\mathrm{Gal}(L/K), V) = 0$ for all $i \in \mathbb{Z}$. □

Proposition 4.2.16. *Let K be a nonarchimedean local field. Let L/K be a finite Galois extension with Galois group $\mathrm{Gal}(L/K)$. There exists an open subgroup V of U_L stable under the action and*

$$\hat{H}^i(\mathrm{Gal}(L/K), V) = 0$$

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

Proof. We assume that K is of characteristic zero (for the characteristic p case, see page 134 of [CF67]). The power series

$$e^x = 1 + x + \cdots + \frac{x^n}{n!} + \cdots$$

converges for $\mathrm{ord}(x) > \mathrm{ord}(p)/(p-1)$. It defines an isomorphism of an open neighborhood of 0 in L onto an open neighborhood of 1 in L^*, with the inverse map

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots .$$

Both maps commute with the actions of G. Let V_0 be an open neighborhood of 0 with $\hat{H}^i(\mathrm{Gal}(L/K), V_0) = 0$ for all $i \in \mathbb{Z}$, as in Lemma 4.2.15. Then $\pi^m V_0$ will have the same properties. Now take $V = \exp(\pi^m V_0)$ and choose m sufficiently large enough such that exp is a local isomorphism. Then the result follows. □

Corollary 4.2.17. *Let K be a nonarchimedean local field. Let L/K be a cyclic extension of degree n with Galois group* $\mathrm{Gal}(L/K)$. *Then $h(U_L) = 1$ and $h(L^*) = n$.*

Proof. By Proposition 4.2.16, there exists an open subgroup V of U_L such that $\hat{H}^i(\mathrm{Gal}(L/K), V) = 0$ for all $i \in \mathbb{Z}$. Hence $h(V) = 1$. Since U_L is a compact set, U_L/V is finite. So $h(U_L/V) = 1$ by Proposition 2.10.6. The Herbrand quotient is multiplicative, hence

$$h(U_L) = h(V)h(U_L/V) = 1.$$

We know that $L^* = U_L \times \pi^{\mathbb{Z}}$, so $L^*/U_L = \pi^{\mathbb{Z}} \cong \mathbb{Z}$. So $h(L^*) = h(U_L)h(\mathbb{Z}) = h(\mathbb{Z})$. We have

$$\hat{H}^0(\mathrm{Gal}(L/K), \mathbb{Z}) = \frac{\mathbb{Z}^{\mathrm{Gal}(L/K)}}{N_{L/K}(\mathbb{Z})} = \frac{\mathbb{Z}}{n\mathbb{Z}},$$

and

$$\hat{H}^1(\mathrm{Gal}(L/K), \mathbb{Z}) = \hat{H}_0(\mathrm{Gal}(L/K), \mathbb{Z}) = \frac{\ker(N_{L/K})}{D(\mathbb{Z})} = 0.$$

Hence,

$$h(L^*) = h(\mathbb{Z}) = \frac{|\hat{H}^0(\mathrm{Gal}(L/K), \mathbb{Z})|}{|\hat{H}^1(\mathrm{Gal}(L/K), \mathbb{Z})|} = \frac{n}{1} = n.$$

□

Corollary 4.2.18. *Let K be a nonarchimedean local field. Let L/K be a cyclic extension of degree n with Galois group* $\mathrm{Gal}(L/K)$. *Then $\hat{H}^2(\mathrm{Gal}(L/K), L^*)$ is of order n.*

Proof. We have

$$h(L^*) = \frac{|\hat{H}^2(\mathrm{Gal}(L/K), L^*)|}{|\hat{H}^1(\mathrm{Gal}(L/K), L^*)|} = n$$

by Corollary 4.2.17. Moreover, Hilbert's Theorem 90 says that $\hat{H}^1(\mathrm{Gal}(L/K), L^*) = 0$ and so $|\hat{H}^1(\mathrm{Gal}(L/K), L^*)| = 1$. Hence $|\hat{H}^2(\mathrm{Gal}(L/K), L^*)| = n$. □

We need the following lemma.

Lemma 4.2.19. *Let G be a finite group and A be a G-module. Let $m, j \geq 0$ be nonnegative integers. We assume that*

(i) $\hat{H}^i(H, A) = 0$ for all $0 < i < j$ and all subgroups H of G;

(ii) if $H_1 \subset H_2 \subset G$, with H_1 normal in H_2 and H_2/H_1 is cyclic of prime order, then the order of $\hat{H}^j(H_2/H_1, A^{H_1})$ divides $[H_2 : H_1]^m$.

Then the order of $\hat{H}^j(G, A)$ divides $[G : 1]^m$.

Proof. For a prime p, let G_p be a Sylow p-subgroup of G. Corollary 2.7.15 says that the restriction map $\mathrm{Res} : \hat{H}^j(G, A) \to \hat{H}^j(G_p, A)$ is injective on the p-primary component of $\hat{H}^i(G, A)$. This allows us to reduce to the study of $\hat{H}^i(G_p, A)$, since we are interested in the order of $\hat{H}^j(G, A)$. Thus, we may assume that G is a p-group. The strategy for the proof is by induction on the order of G.

Assume that $|G| > 1$. Let H be a normal subgroup of G of order p. Apply the part (ii) of the hypothesis to $H_1 = H, H_2 = G$, and we obtain that the order of $\hat{H}^j(G/H, A^H)$ divides $[G : H]^m = p^m$ for all $j > 0$. By the induction hypothesis, we also obtain that the order of $\hat{H}^j(H, A)$ divides $[H : 1]^m$. Now part (i) of the hypothesis gives an exact sequence

$$0 \to \hat{H}^j(G/H, A^H) \overset{\mathrm{Inf}}{\to} \hat{H}^j(G, A) \overset{\mathrm{Res}}{\to} \hat{H}^j(H, A)$$

by Proposition 2.6.10. Thus the order of $\hat{H}^j(G, A)$ divides $|\hat{H}^j(G/H, A^H)| \cdot |\hat{H}^j(H, A)|$, which divides $[G : H]^m \cdot [H : 1]^m = [G : 1]^m$. This proves the case $j > 0$.

For $j = 0$, note that we have an exact sequence

$$\frac{A^H}{N_H(A)} \overset{\mathrm{Cor}}{\to} \frac{A^G}{N_G(A)} \to \frac{(A^H)^{G/H}}{N_{G/H}(A^H)}$$

where H is a normal subgroup of G of order p. Similarly, we have $|\hat{H}^0(G, A)|$ divides $|\hat{H}^0(H, A)| \cdot |\hat{H}^0(G/H, A^H)|$, where $|\hat{H}^0(H, A)|$ divides $[H : 1]^m$ and $|\hat{H}^0(G/H, A^H)|$ divides $[G : H]^m$ by hypothesis. Hence $|\hat{H}^0(G, A)|$ divides $[G : 1]^m$. This completes the proof. □

Theorem 4.2.20. *Let K be a nonarchimedean local field. Let L/K be a finite Galois extension of degree n with Galois group $\mathrm{Gal}(L/K)$. Then $\hat{H}^2(\mathrm{Gal}(L/K), L^*)$ is cyclic of order n. Moreover, there exists an element $u_{L/K} \in \hat{H}^2(K^{unr}/K, K^{unr*})$ generating $\hat{H}^2(\mathrm{Gal}(L/K), L^*)$ with $inv_K(u_{L/K}) = \frac{1}{n}$.*

Proof. We apply Lemma 4.2.19 to the case $G = \mathrm{Gal}(L/K)$, $A = L^*$, $m = 1$, $j = 2$. Note that part (i) of the hypothesis is satisfied by the Hilbert's Theorem 90, and part (ii) of the hypothesis is satisfied by Corollary 4.2.18. Hence the order of $\hat{H}^2(\mathrm{Gal}(L/K), L^*)$ divides n. However, by Corollary 4.2.13, $\hat{H}^2(\mathrm{Gal}(L/K), L^*)$ contains a subgroup of order n generated by $u_{L/K} \in \hat{H}^2(L^{\mathrm{unr}}/K, L^{\mathrm{unr}*})$ such that $\mathrm{inv}_K(u_{L/K}) = \frac{1}{n}$, namely $H^2(L/K)_{\mathrm{unr}} \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Therefore, $\hat{H}^2(\mathrm{Gal}(L/K), L^*)$ is cyclic of order n and generated by $u_{L/K}$. □

Remark 4.2.21. *The generator $u_{L/K}$ is usually called the fundamental class. It will be used to define the local reciprocity map.*

Corollary 4.2.22. *Let K be a nonarchimedean local field. Then we have*

$$H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^*) = H^2(\mathrm{Gal}(K^{unr}/K), K^{unr*}).$$

Proof. Note that $K^{\mathrm{unr}} \subset \overline{K}$, hence $H^2(\mathrm{Gal}(K^{\mathrm{unr}}/K, K^{\mathrm{unr}*}) \subset H^2(\mathrm{Gal}(\overline{K}/K, \overline{K}^*)$. For the other direction, Theorem 4.2.20 shows that for any finite Galois extension L/K of degree n, $\hat{H}^2(\mathrm{Gal}(L/K), L^*)$ is cyclic of order n. Hence $\hat{H}^2(\mathrm{Gal}(L/K), L^*) \subset H^2(\mathrm{Gal}(K^{\mathrm{unr}}/K), K^{\mathrm{unr}*})$. Since $H^2(\mathrm{Gal}(\overline{K}/K, \overline{K}^*)$ is the union of all such $\hat{H}^2(\mathrm{Gal}(L/K), L^*)$, $H^2(\mathrm{Gal}(\overline{K}/K, \overline{K}^*) \subset H^2(\mathrm{Gal}(K^{\mathrm{unr}}/K, K^{\mathrm{unr}*})$. □

Corollary 4.2.22 is important in the study of the Brauer groups. For now we use it (together with Corollary 4.2.13 and Theorem 4.2.20) to give the following theorem.

Theorem 4.2.23. *Let K be a nonarchimedean local field. There exists a canonical isomorphism*

$$inv_K : H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^*) \to \mathbb{Q}/\mathbb{Z}.$$

Moreover, if L/K is a finite Galois extension of degree n with Galois group $G = \mathrm{Gal}(L/K)$, then the following diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2(G, L^*) & \to & H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^*) & \xrightarrow{Res} & H^2(\mathrm{Gal}(\overline{K}/L), \overline{K}^*) \\ & & & & \downarrow{\scriptstyle inv_K} & & \downarrow{\scriptstyle inv_L} \\ 0 & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{\quad n \quad} & \mathbb{Q}/\mathbb{Z} \end{array}$$

is commutative, and therefore we recover the invariant map $inv_{L/K} : H^2(G, L^*) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$.

4.3 The local reciprocity map

First, we apply Tate's Theorem (Theorem 2.12.3) to obtain the following theorem.

Theorem 4.3.1. *Let K be a nonarchimedean local field. Let L/K be a finite Galois extension of degree n with Galois group $\mathrm{Gal}(L/K)$. Then cup product with $u_{L/K}$ defines an isomorphism*

$$\begin{aligned} \hat{H}^i(\mathrm{Gal}(L/K), \mathbb{Z}) &\to \hat{H}^{i+2}(\mathrm{Gal}(L/K), L^*) \\ \alpha &\mapsto \alpha \cup u_{L/K} \end{aligned}$$

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

Now we apply Theorem 4.3.1 to the case $i = -2$ to get the following theorem.

Theorem 4.3.2. *Let K be a nonarchimedean local field. Let L/K be a finite Galois extension of degree n with Galois group $\mathrm{Gal}(L/K)$. Then cup product with $u_{L/K}$ defines an isomorphism*

$$\mathrm{Gal}(L/K)^{ab} \to \frac{K^*}{N_{L/K}(L^*)}$$

where $G^{ab} = G/[G,G]$ is the abelianization of G.

Proof. Note that

$$\hat{H}^0(\mathrm{Gal}(L/K), L^*) = \frac{(L^*)^{\mathrm{Gal}(L/K)}}{N_{L/K}(L^*)} = \frac{K^*}{N_{L/K}(L^*)},$$

and

$$\begin{aligned}\hat{H}^{-2}(\mathrm{Gal}(L/K), \mathbb{Z}) &= H_1(\mathrm{Gal}(L/K), \mathbb{Z}) \\ &= \mathrm{Gal}(L/K)^{\mathrm{ab}} \quad \text{(by Proposition 2.5.7).}\end{aligned}$$

□

Remark 4.3.3. *If L/K is finite abelian, then $\mathrm{Gal}(L/K)^{ab} = \mathrm{Gal}(L/K)$ and hence we get an isomorphism*

$$\mathrm{Gal}(L/K) \cong \frac{K^*}{N_{L/K}(L^*)}.$$

Thus we prove part (ii) of Local Reciprocity Law (Theorem 4.1.1).

Definition 4.3.4. Let K be a nonarchimedean local field. Let L/K be a finite Galois extension. We define the *local reciprocity map* to be

$$\phi_{L/K} : \frac{K^*}{N_{L/K}(L^*)} \to \mathrm{Gal}(L/K)^{\mathrm{ab}}$$

as in Theorem 4.3.2, which is the inverse of cup product by $u_{L/K}$. Let $x \in K^*$, and let $\overline{x}$ be a representative of x in $\frac{K^*}{N_{L/K}(L^*)}$. We denote

$$(x, L/K) := \phi_{L/K}(\overline{x}).$$

Lemma 4.3.5. *Let K be a nonarchimedean local field. Let $K \subset E \subset L$ be a tower of finite Galois extensions. Then we have*

$$\begin{aligned}\mathit{Res}(u_{L/K}) &= u_{L/E}, \\ \mathit{Inf}(u_{E/K}) &= [L:E]u_{L/K}.\end{aligned}$$

Proof. Consider the following diagram

$$\begin{array}{ccccc} H^2(\mathrm{Gal}(\overline{K}/K),\overline{K}^*) & \xrightarrow{\mathrm{Res}} & H^2(\mathrm{Gal}(\overline{K}/E),\overline{K}^*) & \xrightarrow{\mathrm{Res}} & H^2(\mathrm{Gal}(\overline{K}/L),\overline{K}^*) \\ \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_E} & & \downarrow{\scriptstyle \mathrm{inv}_L} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{[E:K]} & \mathbb{Q}/\mathbb{Z} & \xrightarrow{[L:E]} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Note that all vertical maps are isomorphisms by Theorem 4.2.23. Applying the kernel-cokernel lemma and we get the following commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2(\mathrm{Gal}(E/K),E^*) & \xrightarrow{\mathrm{Inf}} & H^2(\mathrm{Gal}(L/K),L^*) & \xrightarrow{\mathrm{Res}} & H^2(\mathrm{Gal}(L/E),L^*) \\ & & \downarrow{\scriptstyle \mathrm{inv}_{E/K}} & & \downarrow{\scriptstyle \mathrm{inv}_{L/K}} & & \downarrow{\scriptstyle \mathrm{inv}_{L/E}} \\ 0 & \longrightarrow & \dfrac{1}{[E:K]}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \dfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} & \xrightarrow{[E:K]} & \dfrac{1}{[L:E]}\mathbb{Z}/\mathbb{Z}. \end{array}$$

The second square commutes, implying that

$$[E:K]\left(\mathrm{inv}_{L/K}(u_{L/K})\right) = [E:K]\frac{1}{[L:K]} = \frac{1}{[L:E]} = \mathrm{inv}_{L/E}(u_{L/E}) = \mathrm{inv}_{L/E}\left(\mathrm{Res}(u_{L/K})\right)$$

and hence

$$\mathrm{Res}(u_{L/K}) = u_{L/E}.$$

Similarly, the commutativity of the first square implies that

$$\mathrm{Inf}(u_{E/K}) = [L:E]u_{L/K}.$$

□

Proposition 4.3.6. *Let K be a nonarchimedean local field. Let $K \subset E \subset L$ be a tower of finite Galois extensions with $G = \mathrm{Gal}(L/K)$, $H = \mathrm{Gal}(L/E)$. Then the diagrams*

$$\begin{array}{ccc} \hat{H}^i(G,\mathbb{Z}) & \xrightarrow{u_{L/K}} & \hat{H}^{i+2}(G,L^*) \\ \downarrow{\scriptstyle Res} & & \downarrow{\scriptstyle Res} \\ \hat{H}^i(H,\mathbb{Z}) & \xrightarrow{u_{L/E}} & \hat{H}^{i+2}(H,L^*) \end{array}$$

and

$$\begin{array}{ccc} \hat{H}^i(G,\mathbb{Z}) & \xrightarrow{u_{L/K}} & \hat{H}^{i+2}(G,L^*) \\ \uparrow{\scriptstyle Cor} & & \uparrow{\scriptstyle Cor} \\ \hat{H}^i(H,\mathbb{Z}) & \xrightarrow{u_{L/E}} & \hat{H}^{i+2}(H,L^*) \end{array}$$

are commutative for all $i \in \mathbb{Z}$.

Proof. Let $a \in \hat{H}^i(G, \mathbb{Z})$. Then

$$\begin{aligned} u_{L/E} \cup \mathrm{Res}(a) &= \mathrm{Res}(u_{L/K}) \cup \mathrm{Res}(a) \quad \text{(by Lemma 4.3.5)} \\ &= \mathrm{Res}(u_{L/K} \cup a) \quad \text{(by Proposition 2.9.6).} \end{aligned}$$

Let $b \in \hat{H}^i(H, \mathbb{Z})$. Then

$$\begin{aligned} \mathrm{Cor}(u_{L/E} \cup b) &= \mathrm{Cor}(\mathrm{Res}(u_{L/K}) \cup b) \quad \text{(by Lemma 4.3.5)} \\ &= u_{L/K} \cup \mathrm{Cor}(b) \quad \text{(by Proposition 2.9.6).} \end{aligned}$$

□

Let L/K be a finite unramified extension of degree n with Galois group $G = \mathrm{Gal}(L/K)$. Let π be a prime element of K, then it is also a prime element of L, and defines a decomposition

$$L^* \cong U_L \times \pi^{\mathbb{Z}} \cong U_L \times \mathbb{Z}$$

of G-modules. Thus

$$\hat{H}^i(G, L^*) \cong \hat{H}^i(G, U_L) \oplus \hat{H}^i(G, \mathbb{Z})$$

for all $i \in \mathbb{Z}$. We already know that $\hat{H}^i(G, U_L) = 0$ by Corollary 4.2.7. Hence it remains to consider $\hat{H}^i(G, \mathbb{Z})$.

First we determine a cocycle representing $u_{L/K}$. Let $f \in \hat{H}^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ be the map such that $f(\mathrm{Frob}_{L/K}^i) = \frac{i}{n} \mod \mathbb{Z}$ for all $i \in \mathbb{Z}$. Then f generates $\hat{H}^1(G, \mathbb{Q}/\mathbb{Z})$ since $\mathrm{Frob}_{L/K}$ generates G. Recall that we have an isomorphism

$$\delta : \hat{H}^1(G, \mathbb{Q}/\mathbb{Z}) \cong \hat{H}^2(G, \mathbb{Z}).$$

Thus to determine the generator $u_{L/K}$ of $\hat{H}^2(G, L^*)$ it is enough to determine δf. We choose a lifting of f to 1-cochain $\tilde{f} : G \to \mathbb{Q}$. We choose the cochain $\tilde{f}$ to be the map $\mathrm{Frob}_{L/K}^i \mapsto \frac{i}{n}$ where $0 \leq i \leq n-1$. Then using formulas for the connecting homomorphism δ we obtain

$$\begin{aligned} \delta\tilde{f}(\mathrm{Frob}_{L/K}^i, \mathrm{Frob}_{L/K}^j) &= \mathrm{Frob}_{L/K}^i \tilde{f}(\mathrm{Frob}_{L/K}^j) - \tilde{f}(\mathrm{Frob}_{L/K}^{i+j}) + \tilde{f}(\mathrm{Frob}_{L/K}^i) \\ &= \begin{cases} 0 & \text{if } i + j \leq n - 1, \\ 1 & \text{if } i + j \geq n. \end{cases} \end{aligned}$$

Recall that we can identify $\mathbb{Z}$ with $\pi^{\mathbb{Z}} \subset L^*$, so $u_{L/K} \in \hat{H}^2(G, L^*)$ is represented by the cocycle φ given by

$$\varphi(\mathrm{Frob}_{L/K}^i, \mathrm{Frob}_{L/K}^j) = \begin{cases} 0 & \text{if } i + j \leq n - 1, \\ \pi & \text{if } i + j \geq n. \end{cases}$$

Note that since $\hat{H}^0(G, U_L) = 0$, we have $U_K \subset N_{L/K}(L^*)$ and so the class of π in $K^*/N_{L/K}(L^*)$ is well-defined.

Proposition 4.3.7. *Let K be a nonarchimedean local field. Let L/K be an unramified extension of degree n with Galois group $G = \mathrm{Gal}(L/K)$ generated by $Frob_{L/K}$. Let $x \in K^*, \overline{x} \in \frac{K^*}{N_{L/K}(L^*)} = \hat{H}^0(G, L^*)$ be a representative of x, $f \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) = \hat{H}^1(G, \mathbb{Q}/\mathbb{Z})$. Then*

$$f\left(\phi_{L/K}(\overline{x})\right) = inv_{L/K}(\overline{x} \cup \delta f).$$

Proof. Let $\overline{\phi}_{L/K}(\overline{x})$ be the image of $\phi_{L/K}(\overline{x})$ under the isomorphism $G = G^{\mathrm{ab}} \cong H_1(G, \mathbb{Z}) = \hat{H}^{-2}(G, \mathbb{Z})$. Then $\overline{\phi}_{L/K}(\overline{x}) \cup u_{L/K} = \overline{x} \in \hat{H}^0(G, L^*)$. So

$$\begin{aligned}
\overline{x} \cup \delta f &= u_{L/K} \cup \overline{\phi}_{L/K}(\overline{x}) \cup \delta f \\
&= u_{L/K} \cup \left(\overline{\phi}_{L/K}(\overline{x}) \cup \delta f\right) \quad \text{(by Proposition 2.9.4)} \\
&= u_{L/K} \cup \delta\left(\overline{\phi}_{L/K}(\overline{x}) \cup f\right) \quad \text{(by Theorem 2.9.7)}
\end{aligned}$$

where $\overline{\phi}_{L/K}(\overline{x}) \cup f$ is given by the cup product $\hat{H}^{-2}(G, \mathbb{Z}) \cup \hat{H}^1(G, \mathbb{Q}/\mathbb{Z}) \cong \hat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z})$, represented by i/n since $\hat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z}) \cong \hat{H}^0(G, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$ and $\delta : \hat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z}) \to \hat{H}^0(G, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$ is induced by the norm map, which is just multiplication by n since $\mathbb{Q}/\mathbb{Z}$ and $\mathbb{Z}$ are trivial G-modules. Hence

$$\begin{aligned}
\overline{x} \cup \delta f &= u_{L/K} \cup \delta\left(\overline{\phi}_{L/K}(\overline{x}) \cup f\right) \\
&= u_{L/K} \cup i.
\end{aligned}$$

Note that $f\left(\phi_{L/K}(\overline{x})\right) = \overline{\phi}_{L/K}(\overline{x}) \cup f = i/n$. Therefore,

$$\begin{aligned}
\mathrm{inv}_{L/K}(\overline{x} \cup \delta f) &= \mathrm{inv}_{L/K}(u_{L/K} \cup i) \\
&= \frac{i}{n} \\
&= f\left(\phi_{L/K}(\overline{x})\right).
\end{aligned}$$

□

Proposition 4.3.8. *Let K be a nonarchimedean local field. Let L/K be an unramified extension of degree n with Galois group $G = \mathrm{Gal}(L/K)$ generated by $Frob_{L/K}$. Then $\phi_{L/K}(\overline{x}) = (x, L/K) = Frob_{L/K}^{ord(x)}$ for all $x \in K^*$.*

Proof. The invariant map $\mathrm{inv}_{L/K} : \hat{H}^2(G, L^*) \to \mathbb{Q}/\mathbb{Z}$ is defined by the composition

$$\mathrm{inv}_{L/K} : \hat{H}^2(G, L^*) \xrightarrow[\cong]{\mathrm{ord}} \hat{H}^2(G, \mathbb{Z}) \xrightarrow[\cong]{\delta^{-1}} \hat{H}^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\gamma} \mathbb{Q}/\mathbb{Z}$$

where $\gamma(f) = f(\mathrm{Frob}_{L/K})$. Note that $\mathrm{ord}(\overline{x} \cup \delta f) = \mathrm{ord}(x) \cup \delta f$. Hence

$$\begin{aligned} f\left(\phi_{L/K}(\overline{x})\right) &= \mathrm{inv}_{L/K}(\overline{x} \cup \delta f) \quad \text{(by Proposition 4.3.7)} \\ &= \gamma \circ \delta^{-1} \circ \mathrm{ord}(\overline{x} \cup \delta f) \\ &= \gamma \circ \delta^{-1} \left(\mathrm{ord}(x) \cup \delta f\right) \\ &= \mathrm{ord}(x) \cup \left(\gamma \circ \delta^{-1}(\delta f)\right) \\ &= \mathrm{ord}(x) \cup \gamma(f) \\ &= \mathrm{ord}(x) f(\mathrm{Frob}_{L/K}) \\ &= f\left(\mathrm{Frob}_{L/K}^{\mathrm{ord}(x)}\right). \end{aligned}$$

Since f was arbitrary, we conclude that $\phi_{L/K}(\overline{x}) = \mathrm{Frob}_{L/K}^{\mathrm{ord}(x)}$. □

Remark 4.3.9. *Proposition 4.3.8 proves part (i) of Local Reciprocity Law (Theorem 4.1.1) since ord*$(\pi) = 1$.

4.4 Lubin-Tate formal group law

In this section we study formal group laws and Lubin-Tate theory, which provides tools for a straightforward construction of totally ramified abelian extensions of a nonarchimedean local field, and leads to a proof of the Local Existence Theorem.

Definition 4.4.1. Let A be a commutative ring with 1 and let $F \in A[[X, Y]]$. We say that F is a *commutative formal group law* if
(a) $F(X, F(Y, Z)) = F(F(X, Y), Z)$;
(b) $F(0, Y) = Y$ and $F(X, 0) = X$;
(c) there exists a unique $G(X)$ such that $F(X, G(X)) = 0$;
(d) $F(X, Y) = F(Y, X)$;
(e) $F(X, Y) \equiv X + Y \mod \deg 2$.

Remark 4.4.2. *(b) implies that $F(X, Y)$ is of the form $F(X, Y) = X + Y + XYG(X, Y)$, i.e., all the higher order terms are crossed terms.*

(e) implies that $F(X, Y)$ has no constant term.

Note that two formal power series are said to be *congruent* $\mod \deg n$ if and only if they coincide in all terms of degree strictly less than n.

Let K be a nonarchimedean local field. Let $A = \mathcal{O}_K$ and let $F(X, Y)$ be a commutative formal group law defined over $\mathcal{O}_K$. If $x, y \in \mathfrak{m}_K$, then $F(x, y)$ converges to an element in $\mathfrak{m}_K$. Under this composition $\mathfrak{m}_K$ becomes a group and we write $F(\mathfrak{m}_K)$ to denote this group. For example, if we set $F(X, Y) = X + Y$ then $F(\mathfrak{m}_K) = \mathfrak{m}_K$. If we set $F(X, Y) = X + Y + XY$ then we obtain the multiplicative group structure on $1 + \mathfrak{m}_K$.

Definition 4.4.3. Let $F(X,Y), G(X,Y)$ be two commutative formal group laws over a commutative ring A. A *homomorphism* $F \to G$ is a power series $h \in TA[[T]]$ such that

$$h(F(X,Y)) = G(h(X), h(Y)).$$

If h has an inverse, i.e., there exists a homomorphism $h' : G \to F$ such that

$$h \circ h' = T = h' \circ h,$$

then h is said to be an *isomorphism*. A homomorphism $f : F \to F$ is called an *endomorphism*.

Definition 4.4.4. Let F be a commutative formal group law over A. For any $f, g \in TA[[T]]$, we define

$$(f +_F g)(T) = F(f(T), g(T)).$$

Definition 4.4.5. Let K be a nonarchimedean local field, $q = |k|$ be the order of the residue field. Choose a prime element $\pi \in K$. We define $\mathcal{F}_\pi$ to be the set of formal power series $f \in \mathcal{O}_K[[X]]$ such that
(i) $f(X) \equiv \pi X \mod \deg 2$;
(ii) $f(X) \equiv X^q \mod \pi$.

Note that two formal power series are said to be *congruent* $\mod \pi$ if and only if the difference of coefficients of each degree is divisible by π.

Example 4.4.6. $K = \mathbb{Q}_p$, $\pi = p$, $f(X) = pX + \binom{p}{2}X^2 + \cdots pX^{p-1} + X^p$ is an example of such a power series.

Proposition 4.4.7. *Let $f, g \in \mathcal{F}_\pi$, let $n \in \mathbb{Z}$ and let $\phi_1(X_1, \cdots, X_n)$ be a linear form in $X_1, \cdots, X_n$ with coefficients in $\mathcal{O}_K$. Then there exists a unique $\phi \in \mathcal{O}_K[[X_1, \cdots, X_n]]$ such that*
(i) $\phi \equiv \phi_1 \mod \deg 2$;
(ii) $f(\phi(X_1, \cdots, X_n)) = \phi(g(X_1), \cdots, g(X_n))$.

Proof. Our approach is to construct such a ϕ by constructing a sequence $\{\phi_j\}$ with $\phi_j \in \mathcal{O}_K[[X_1, \cdots, X_n]]$ such that ϕ_j is unique $\mod \deg j + 1$ and satisfies (i) and (ii) $\mod \deg j + 1$. Then we set $\phi = \lim \phi_j$.

First we consider ϕ_1, which satisfies (i) and (ii) by assumption.

Now suppose we have constructed ϕ_j for some positive integer j. Because ϕ_j is unique $\mod \deg j+1$, we must have $\phi_i \equiv \phi_j \mod \deg j+1$ for all $i \geq j$. Thus $\phi_{j+1} - \phi_j$ contains only terms of degree $j + 1$. By assumption we have

$$f(\phi_j(X_1, \cdots, X_n)) = \phi_j(g(X_1), \cdots, g(X_n)) \mod \deg j + 1.$$

Let

$$E_{j+1} = f(\phi_j(X_1, \cdots, X_n)) - \phi_j(g(X_1), \cdots, g(X_n)) \mod \deg j + 2.$$

Let

$$\phi_{j+1} = \phi_j - \frac{E_{j+1}}{\pi(1-\pi^j)}.$$

We need to show that $\phi_{j+1} \in \mathcal{O}_K[[X_1, \cdots, X_n]]$. It suffices to show that $\pi | E_{j+1}$. To see this, note that $f(X) \equiv g(X) \equiv X^q \mod \pi$, so

$$\begin{aligned} E_{j+1} &\equiv f(\phi_j(X_1, \cdots, X_n)) - \phi_j(g(X_1), \cdots, g(X_n)) \\ &\equiv \phi_j(X_1, \cdots, X_n)^q - \phi_j(X_1^q, \cdots, X_n^q) \\ &\equiv 0 \mod \pi. \end{aligned}$$

Thus $\pi | E_{j+1}$ and hence $\phi_{j+1} \in \mathcal{O}_K[[X_1, \cdots, X_n]]$.

Since $\phi_j \equiv \phi_1 \mod \deg 2$ by assumption, and E_{j+1} has only terms of degree $j+1$, we have

$$\phi_{j+1} \equiv \phi_j \equiv \phi_1 \mod \deg 2.$$

We have to show that ϕ_{j+1} satisfies (ii) $\mod \deg j+2$. Note that

$$f(\phi_{j+1}) - \phi_{j+1}(g) \equiv f(\phi_{j+1}) - \phi_j(g) + \frac{E_{j+1}(g)}{\pi(1-\pi^j)} \mod \deg j+2.$$

By Taylor expansion, we have

$$\begin{aligned} f(\phi_{j+1}) &= f(\phi_j) + f'(\phi_j)(\phi_{j+1} - \phi_j) + \frac{f''(\phi_j)}{2!}(\phi_{j+1} - \phi_j)^2 + \cdots \\ &= f(\phi_j) + \pi\left(\frac{-E_{j+1}}{\pi(1-\pi^j)}\right) + \cdots \\ &\equiv f(\phi_j) - \pi\left(\frac{E_{j+1}}{\pi(1-\pi^j)}\right) \mod \deg j+2. \end{aligned}$$

Similarly, if we consider $E_{j+1}(g(X_1), \cdots, g(X_n))$, we have

$$\begin{aligned} E_{j+1}(g(X_1), \cdots, g(X_n)) &\equiv E_{j+1}(\pi X_1, \cdots, \pi X_n) \mod \deg j+2 \\ &\equiv \pi^{j+1} E_{j+1}(X_1, \cdots, X_n) \mod \deg j+2. \end{aligned}$$

Therefore,

$$\begin{aligned} f(\phi_{j+1}) - \phi_{j+1}(g) &\equiv f(\phi_{j+1}) - \phi_j(g) + \frac{E_{j+1}(g)}{\pi(1-\pi^j)} \mod \deg j+2 \\ &\equiv f(\phi_j) - \pi\left(\frac{E_{j+1}}{\pi(1-\pi^j)}\right) - \phi_j(g) + \pi^{j+1}\left(\frac{E_{j+1}}{\pi(1-\pi^j)}\right) \mod \deg j+2 \\ &\equiv E_{j+1} - E_{j+1} \mod \deg j+2 \\ &\equiv 0 \mod \deg j+2. \end{aligned}$$

It only remains to show the uniqueness of ϕ_{j+1}. We write $\phi_{j+1} = \phi_j + \phi^{j+1}$ and suppose

$$f(\phi_{j+1}) - \phi_{j+1}(g) \equiv 0 \mod \deg j + 2.$$

We will show that $\phi^{j+1} = -\frac{E_{j+1}}{\pi(1-\pi^j)}$. As above, we use Taylor expansions to get

$$f(\phi_{j+1}) \equiv f(\phi_j) + \pi\phi^{j+1} \mod \deg j + 2$$

and the fact that ϕ^{j+1} only has terms of degree $j+1$ to get

$$\phi_{j+1}(g(X_1), \cdots, g(X_n)) \equiv \pi^{j+1}\phi^{j+1}(X_1, \cdots, X_n) \mod \deg j + 1.$$

Thus

$$\begin{aligned} 0 &\equiv f(\phi_{j+1}) - \phi_{j+1}(g) \mod \deg j + 2 \\ &\equiv f(\phi_j) + \pi\phi^{j+1} - \phi_j(g) - \phi^{j+1}(g) \mod \deg j + 2 \\ &\equiv E_{j+1} + \pi(1-\pi^j)\phi^{j+1} \mod \deg j + 2. \end{aligned}$$

Therefore, $\phi^{j+1} = -\frac{E_{j+1}}{\pi(1-\pi^j)}$. By induction, we are done. □

Proposition 4.4.8. *For every $f \in \mathcal{F}_\pi$, there is a unique commutative formal group law F_f with coefficients in $\mathcal{O}_K$ such that*

$$f(F_f(X,Y)) = F_f(f(X), f(Y)),$$

i.e., f is an endomorphism.

Proof. Let F_f be the unique solution to

$$\begin{cases} F_f(X,Y) \equiv X + Y \mod \deg 2 \\ f(F_f(X,Y)) = F_f(f(X), f(Y)) \end{cases}$$

given by Proposition 4.4.7. We only need to check that F_f is a commutative formal group law. We can do this by uniqueness in Proposition4.4.7.

Note that

$$\begin{aligned} F_f(X, F_f(Y,Z)) &\equiv X + F_f(Y,Z) \equiv X + Y + Z \mod \deg 2, \\ F_f(F_f(X,Y), Z) &\equiv F_f(X,Y) + Z \equiv X + Y + Z \mod \deg 2, \\ f(F_f(X, F_f(Y,Z))) &= F_f(f(X), f(F_f(Y,Z))) = F_f(f(X), F_f(f(Y), f(Z))), \\ f(F_f(F_f(X,Y), Z)) &= F_f(f(F_f(X,Y)), f(Z)) = F_f(F_f(f(X), f(Y)), f(Z)). \end{aligned}$$

Hence $F_f(X, F_f(Y,Z))$ and $F_f(F_f(X,Y),Z)$ are both solutions to

$$\begin{cases} H(X,Y,Z) \equiv X + Y + Z \mod \deg 2 \\ f(H(X,Y,Z)) = H(f(X), f(Y), f(Z)). \end{cases}$$

By the uniqueness we have

$$F_f(X, F_f(Y, Z)) = F_f(F_f(X, Y), Z).$$

$F_f(0, Y)$ and Y are both solutions to

$$\begin{cases} H(X, Y) \equiv Y \mod \deg 2 \\ f(H(X, Y)) = H(f(X), f(Y)). \end{cases}$$

Hence $F_f(0, Y) = Y$. $F_f(X, 0)$ and X are both solutions to

$$\begin{cases} H(X, Y) \equiv X \mod \deg 2 \\ f(H(X, Y)) = H(f(X), f(Y)). \end{cases}$$

Hence $F_f(X, 0) = X$. Similarly, we can verify that F_f is indeed a commutative formal group law. □

Remark 4.4.9. *The formal group laws F_f defined by Proposition 4.4.8 are the Lubin-Tate formal group laws.*

Proposition 4.4.10. *Let $f \in \mathcal{F}_\pi$ and F_f be the Lubin-Tate formal group law given by Proposition 4.4.8. Then for any $a \in A = \mathcal{O}_K$ there exists a unique $[a]_f \in \mathcal{O}_K[[X]]$ such that*
(i) $[a]_f$ commutes with f;
(ii) $[a]_f \equiv aX \mod \deg 2$.
Moreover, $[a]_f$ is an endomorphism of the group law F_f.

Proof. For any $a \in \mathcal{O}_K$ and any $f, g \in \mathcal{F}_\pi$, let $[a]_{f,g}(T)$ be the unique solution to

$$\begin{cases} [a]_{f,g}(T) \equiv aT \mod \deg 2 \\ f([a]_{f,g}(T)) = [a]_{f,g}(g(T)) \end{cases}$$

given by Proposition 4.4.7. Note that

$$F_f([a]_{f,g}(X), [a]_{f,g}(Y)) \equiv [a]_{f,g}(X) + [a]_{f,g}(Y) \equiv aX + aY \mod \deg 2,$$

$$[a]_{f,g}(F_g(X, Y)) \equiv aF_g(X, Y) \equiv aX + aY \mod \deg 2,$$

$$F_f([a]_{f,g}(g(X)), [a]_{f,g}(g(Y))) = F_f\left(f([a]_{f,g}(X)), f([a]_{f,g}(Y))\right) = f\left(F_f([a]_{f,g}(X), [a]_{f,g}(Y))\right),$$

$$[a]_{f,g}(F_g(g(X), g(Y))) = [a]_{f,g}\left(g(F_g(X, Y)) = f\left([a]_{f,g}(F_g(X, Y))\right)\right).$$

Hence both $F_f([a]_{f,g}(X), [a]_{f,g}(Y))$ and $[a]_{f,g}(F_g(X, Y))$ are solutions to

$$\begin{cases} H(X, Y) \equiv aX + aY \mod \deg 2 \\ f(H(X, Y)) = H(g(X), g(Y)). \end{cases}$$

By Proposition 4.4.7, we must have

$$F_f([a]_{f,g}(X), [a]_{f,g}(Y)) = [a]_{f,g}(F_g(X,Y)).$$

Now let $f = g$, and $[a]_f = [a]_{f,f}$, then we are done. □

Remark 4.4.11. *Using uniqueness of $[a]_f$ in Proposition 4.4.10, we have*

$$[\pi]_f(T) = f(T)$$

and

$$[1]_f(T) = T.$$

Proposition 4.4.12. *Let $f \in \mathcal{F}_\pi$, $a \in \mathcal{O}_K$. The map $a \mapsto [a]_f := [a]_{f,f}$ is an injective ring homomorphism of $A = \mathcal{O}_K$ to the ring $End_{\mathcal{O}_K}(F_f)$.*

Proof. We first show that $[a]_f \in \mathrm{End}_{\mathcal{O}_K}(F_f)$. Note that

$$[a]_f\left(F_f(X,Y)\right) \equiv aF_f(X,Y) \equiv aX + aY \mod \deg 2,$$

and

$$F_f\left([a]_f(X), [a]_f(Y)\right) \equiv [a]_f(X) + [a]_f(Y) \equiv aX + aY \mod \deg 2.$$

Also, since both $[a]_f$ and F_f commutes with f, we have

$$f\left([a]_f(F_f(X,Y))\right) = [a]_f\left(f(F_f(X,Y))\right) = [a]_f(F_f(f(X), f(Y))),$$

and similarly

$$f\left(F_f([a]_f(X), [a]_f(Y))\right) = F_f\left(f([a]_f(X)), f([a]_f(Y))\right) = F_f\left([a]_f(f(X)), [a]_f(f(Y))\right).$$

By the uniqueness in Proposition 4.4.7 applied to $g = f$, $\phi_1(X,Y) = aX + aY$, we have

$$[a]_f\left(F_f(X,Y)\right) = F_f\left([a]_f(X), [a]_f(Y)\right).$$

Hence $[a]_f \in \mathrm{End}_{\mathcal{O}_K}(F_f)$.

We also need to check the necessary properties for a ring homomorphism. The binary operations in the ring $\mathrm{End}_{\mathcal{O}_K}(F_f)$ are $+_{F_f}$ and composition. So we need to verify that $[a]_f +_{F_f} [b]_f = [a+b]_f$ and $[ab]_f = [a]_f \circ [b]_f$. Both $[a]_f + [b]_f$ and $[a+b]_f$ commute with f. Also,

$$[a]_f +_{F_f} [b]_f \equiv aX + bX \equiv [a+b]_f \mod \deg 2.$$

By the uniqueness in Proposition 4.4.10, we must have $[a]_f +_{F_f} [b]_f = [a+b]_f$. A similar argument shows that $[ab]_f = [a]_f \circ [b]_f$.

Finally, the homomorphism is injective because $[a]_f \equiv aX \mod \deg 2$, so a can be recovered as the coefficient of the term of degree 1. Also note that $[a]_f$ has no constant term by Remark 4.4.2. Hence the map $a \mapsto [a]_f := [a]_{f,f}$ is injective.

□

Proposition 4.4.13. *Let $f, g \in \mathcal{F}_\pi$. Then $F_f \cong F_g$.*

Proof. Let $u \in U_K$. Then $[u]_{f,g} : F_g \to F_f$ has an inverse $[u^{-1}]_{g,f} : F_f \to F_g$. Hence $F_f \cong F_g$. □

Let K be a nonarchimedean local field, $q = |k|$ be the order of the residue field. We fix a prime element π of K. For $f \in \mathcal{F}_\pi$, let F_f be the corresponding Lubin-Tate formal group law given in Proposition 4.4.8. We write M_f for the group of points in $\mathfrak{m}_{\overline{K}}$ equipped with the formal group law defined by F_f, i.e.,

$$M_f = F_f(\mathfrak{m}_{\overline{K}}).$$

Then M_f has an $\mathcal{O}_K$-module structure given by

$$\begin{aligned} x +_{F_f} y &= F_f(x, y), \\ ax &= [a]_f(x). \end{aligned}$$

for any $x, y \in M_f$ and $a \in \mathcal{O}_K$. Let

$$E_f^n = \ker([\pi^n]_f)$$

and

$$E_f = \bigcup_{n \geq 1} E_f^n.$$

Then E_f is exactly the torsion submodule of M_f. Let

$$K_\pi^n = K(E_f^n),$$

$$K_\pi = \bigcup_{n \geq 1} K(E_f^n),$$

and denote

$$G_{\pi,n} = \mathrm{Gal}(K_\pi^n / K),$$

then we have

$$\mathrm{Gal}(K_\pi / K) = \varprojlim_n G_{\pi,n}.$$

Proposition 4.4.14. *The $\mathcal{O}_K$-module E_f is isomorphic to $K/\mathcal{O}_K$. Hence $End_{\mathcal{O}_K}(E_f^n) \cong \mathcal{O}_K/(\pi^n)$ and $Aut_{\mathcal{O}_K}(E_f^n) \cong (\mathcal{O}_K/(\pi^n))^*$.*

Proof. (i) Proposition 4.4.13 implies that the choice of $f \in \mathcal{F}_\pi$ is unimportant since the Lubin-Tate formal group laws are isomorphic for all elements of $\mathcal{F}_\pi$. Hence we may choose $f(X) = X^q + \pi X$. Let $a \in \mathfrak{m}_{\overline{K}}$. Then $f(X) - a = 0$ has solutions in $\overline{K}$, and in fact they belong to $\mathfrak{m}_{\overline{K}}$ (we can prove this by using properties of nonarchimedean absolute values). Note that $[\pi]_f(T) = f(T)$, hence the map $[\pi]_f : M_f \to M_f$ is surjective (given $a \in M_f$,

there exists $x \in M_f$ such that $f(x) = a$, hence $[\pi]_f(x) = f(x) = a$). This implies that M_f is a divisible $\mathcal{O}_K$-module and hence a direct sum of copies of $K/\mathcal{O}_K$.

Now consider

$$E_f^1 = \ker([\pi_f]) = \{a \in M_f : [\pi]_f(a) = 0 = f(a)\}.$$

Hence E_f^1 is exactly the set of roots of f, so $|E_f^1| = q$ and hence $E_f^1 \cong \mathcal{O}_K/(\pi)$. Since $[\pi]_f$ is surjective, the sequence

$$0 \longrightarrow E_f^1 \longrightarrow E_f^n \xrightarrow{[\pi]_f} E_f^{n-1} \to 0$$

is exact. By induction, E_f^n has q^n elements. Moreover, since E_f^1 is cyclic, E_f^n must be cyclic. Therefore, E_f^n is cyclic of order q^n, and hence $E_f^n \cong \mathcal{O}_K/(\pi^n)$. Since $E_f = \cup_{n\geq 1} E_f^n$, it follows that $E_f \cong K/\mathcal{O}_K$. Also, the action of $\mathcal{O}_K$ on E_f^n induces an isomorphism $\mathcal{O}_K/(\pi^n) \cong \mathrm{End}_{\mathcal{O}_K}(E_f^n)$. □

Theorem 4.4.15. *(i) For each $n \geq 1$, K_π^n/K is totally ramified of degree $(q-1)q^{n-1}$.*

(ii) The action of $\mathcal{O}_K$ on E_f^n defines an isomorphism

$$(\mathcal{O}_K/(\pi^n))^* \to \mathrm{Gal}(K_\pi^n/K).$$

In particular, K_π^n/K is abelian.

(iii) For each $n \geq 1$, π is a norm from K_π^n to K.

Proof. (i)-(ii) Again we choose $f(X) = X^q + \pi X$. Let x_1 be a root of $f(X)$, and define x_n inductively by choosing x_n to be a root of $f(X) - x_{n-1}$. Consider the tower of Eisenstein extensions

$$K \subset K(x_1) \subset K(x_2) \subset \cdots \subset K(x_n) \subset K_\pi^n$$

where $[K(x_1) : K] = q - 1$ and $[K(x_n) : K(x_{n-1})] = q$ for all $n \geq 2$. This shows that $K(x_n)$ is totally ramified over K of degree $(q-1)q^{n-1}$.

E_f^n is the kernel of $[\pi^n]_f$, i.e., the set of roots of $f \circ \cdots \circ f = f^{(n)}$. Hence K_π^n is precisely the splitting field of $f^{(n)}$. So $\mathrm{Gal}(K_\pi^n/K)$ can be identified with a subgroup of the group of permutations of the set E_f^n, this subgroup is contained in $\mathrm{Aut}_{\mathcal{O}_K}(E_f^n) \cong (\mathcal{O}_K/\pi^n)^*$, which has order $(q-1)q^{n-1}$. So

$$(q-1)q^{n-1} \geq |\mathrm{Gal}(K_\pi^n/K)| = [K_\pi^n : K] \geq [K(x_n) : K] = (q-1)q^{n-1}.$$

This shows that $K_\pi^n = K(x_n)$ and $\mathrm{Gal}(K_\pi^n/K) \cong \mathrm{Aut}_{\mathcal{O}_K}(E_f^n) \cong (\mathcal{O}_K/(\pi^n))^*$.

(iii) By construction, x_n is a root of the polynomial

$$(f(X)/X) \circ f^{(n-1)} = X^{(q-1)q^{n-1}} + \cdots + \pi.$$

Since $K(x_n)/K = (q-1)q^{n-1}$, this polynomial must be the minimal polynomial of x_n. Thus

$$N_{K_\pi^n/K}(x_n) = (-1)^{(q-1)q^{n-1}}\pi = \pi.$$

□

The fact that K_π is the union of totally ramified extensions of K and K^{unr} is the union of unramified extensions of K implies that $K_\pi \cap K^{\mathrm{unr}} = K$. We define a homomorphism

$$\phi_\pi : K^* \to \mathrm{Gal}(K_\pi \cdot K^{\mathrm{unr}}/K)$$

by defining the restrictions of $\phi_\pi(a)$ to K_π and K^{unr} for each $a \in K^*$. Let $a = u\pi^m \in K^*$. Define

$$\phi_\pi(a)|_{K^{\mathrm{unr}}} = \mathrm{Frob}^m$$

and

$$\phi_\pi(a)|_{K_\pi} = [u^{-1}]_f$$

where Frob is the Frobenius element $\mathrm{Frob}_{K^{\mathrm{unr}}/K}$. Although K is complete, K^{unr} is not complete, and we write $\widehat{K^{\mathrm{unr}}}$ for the completion of K^{unr} with respect to the unique extension of the valuation of K to K^{unr}. We also write Frob for the Frobenius element $\mathrm{Frob}_{\widehat{K^{\mathrm{unr}}}/K}$.

Remark 4.4.16. *We use u^{-1} instead of u in the definition of the map ϕ_π so that both $K_\pi \cdot K^{unr}$ and ϕ_π are independent of the choice of the prime element π, as we will see in Theorem 4.4.20.*

Lemma 4.4.17. *The homomorphisms*

$$\begin{aligned} \mathcal{O}_{\widehat{K^{unr}}} &\to \mathcal{O}_{\widehat{K^{unr}}} \\ x &\mapsto \mathit{Frob}(x) - x \end{aligned}$$

and

$$\begin{aligned} \mathcal{O}_{\widehat{K^{unr}}} &\to \mathcal{O}_{\widehat{K^{unr}}} \\ x &\mapsto \mathit{Frob}(x)/x \end{aligned}$$

are surjective with kernels $\mathcal{O}_K$ and U_K respectively.

Proposition 4.4.18. *Let K be a nonarchimedan local field. Let $\pi, \pi' = u\pi$ be two different primes of K. Let F_f and F_g be the Lubin-Tate formal group laws defined by $f \in \mathcal{F}_\pi, g \in \mathcal{F}_{\pi'}$. Then there exists $\varepsilon \in U_{\widehat{K^{unr}}}$ such that $\mathit{Frob}(\varepsilon) = \varepsilon u$ and a power series $h(T) \in \mathcal{O}_{\widehat{K^{unr}}}[[T]]$ such that*
(i) $h(T) \equiv \varepsilon T \mod \deg 2$;
(ii) $\mathit{Frob}(h) = h \circ [u]_f$;
(iii) $h(F_f(X,Y)) = F_g(h(X), h(Y))$;
(iv) $h \circ [a]_f = [a]_g \circ h$ for all $a \in \mathcal{O}_K$.

Proof. We first show that there exists a $h(T) \in \mathcal{O}_{\widehat{K^{\mathrm{unr}}}}[[T]]$ that satisfies (i) and (ii). Let $\varepsilon \in U_{\widehat{K^{\mathrm{unr}}}}$ such that $\mathrm{Frob}(\varepsilon) = \varepsilon u$ (such ε exists by Lemma 4.4.17). Let $h_1(T) = \varepsilon T$, and we construct a sequence of polynomials h_r such that

$$h_r(T) = h_{r-1}(T) + xT^r,$$

$$\mathrm{Frob}(h_r) \equiv h_r \circ [u]_f \mod \deg r + 1$$

for some $x \in \mathcal{O}_{\widehat{K^{\mathrm{unr}}}}$. Note that $h_1(T)$ satisfies (i) and (ii). Suppose that $h_r(T)$ satisfies (i) and (ii). Let $a \in \mathcal{O}_{\widehat{K^{\mathrm{unr}}}}$ such that $\mathrm{Frob}(a) - a = c(\varepsilon u)^{-r-1}$ where c is the coefficient of T^{r+1} in $h_r \circ [u]_f - \mathrm{Frob}(h_r)$. Note that such a exists by Lemma 4.4.17. Let $b = a\varepsilon^{r+1}$, and we claim that $h_{r+1}(T) = h_r(T) + bT^{r+1}$ satisfies (ii). Well,

$$\begin{aligned}
\mathrm{Frob}(h_{r+1}(T)) &= \mathrm{Frob}(h_r(T)) + \mathrm{Frob}(a\varepsilon^{r+1}T^{r+1}) \\
&= \mathrm{Frob}(h_r(T)) + \mathrm{Frob}(a)\mathrm{Frob}(\varepsilon T)^{r+1} \\
&= \mathrm{Frob}(h_r(T)) + \left(a + \frac{c}{(\varepsilon u)^{r+1}}\right)\mathrm{Frob}(\varepsilon T)^{r+1} \\
&\equiv \mathrm{Frob}(h_r(T)) + \left(a + \frac{c}{(\varepsilon u)^{r+1}}\right)(\mathrm{Frob}(\varepsilon))^{r+1}T^{r+1} \mod \deg r + 2 \\
&\equiv \mathrm{Frob}(h_r(T)) + a(\mathrm{Frob}(\varepsilon))^{r+1}T^{r+1} + cT^{r+1} \mod \deg r + 2 \\
&\equiv h_r \circ [u]_f(T) - cT^{r+1} + a(\mathrm{Frob}(\varepsilon))^{r+1}T^{r+1} + cT^{r+1} \mod \deg r + 2 \\
&\equiv h_r \circ [u]_f(T) + a(\mathrm{Frob}(\varepsilon))^{r+1}T^{r+1} \mod \deg r + 2 \\
&\equiv h_r \circ [u]_f(T) + a(\varepsilon u)^{r+1}T^{r+1} \mod \deg r + 2 \\
&\equiv h_r \circ [u]_f(T) + a\varepsilon^{r+1}T^{r+1} \circ [u]_f(T) \mod \deg r + 2 \\
&\equiv h_r \circ [u]_f(T) + bT^{r+1} \circ [u]_f(T) \mod \deg r + 2 \\
&\equiv h_{r+1} \circ [u]_f(T) \mod \deg r + 2.
\end{aligned}$$

Now take the limit of these h_r to get the desired h so that it satisfies (i) and (ii).

Next, we will show that h can be chosen so that $g = \mathrm{Frob}\ h \circ f \circ h^{-1}$. Define $\theta = \mathrm{Frob}\ h \circ f \circ h^{-1}$. Note that

$$\theta = \mathrm{Frob}\ h \circ f \circ h^{-1} = h \circ [u]_f \circ f \circ h^{-1} = h \circ f \circ [u]_f \circ h^{-1}.$$

By (ii) we have $T = h \circ [u]_f \circ (\mathrm{Frob}\ h)^{-1}(T)$, hence

$$h^{-1} = [u]_f \circ (\mathrm{Frob}\ h)^{-1}.$$

Since f and $[u]_f$ have coefficients in $\mathcal{O}_K$, we have

$$\begin{aligned}
\mathrm{Frob}\ \theta &= \mathrm{Frob}\ h \circ f \circ [u]_f \circ (\mathrm{Frob}\ h)^{-1} \\
&= \mathrm{Frob}\ h \circ f \circ h^{-1} \\
&= \theta
\end{aligned}$$

and so $\theta \in \mathcal{O}_K[[T]]$. Moreover,

$$\begin{aligned}
\theta(T) &= \mathrm{Frob}\ h \circ f \circ h^{-1}(T) \\
&\equiv \mathrm{Frob}\ \varepsilon\pi\varepsilon^{-1}T \mod T^2 \\
&\equiv \varepsilon u\pi\varepsilon^{-1}T \mod T^2 \\
&\equiv \pi' T \mod T^2,
\end{aligned}$$

and

$$\begin{aligned}\theta(T) &= \text{Frob } h \circ f \circ h^{-1}(T) \\ &\equiv \text{Frob } h \circ (h^{-1})^q(T) \mod \mathfrak{m}_K \\ &\equiv \text{Frob } h \ (\text{Frob } h^{-1}(T^q)) \mod \mathfrak{m}_K \\ &\equiv T^q \mod \mathfrak{m}_K.\end{aligned}$$

Therefore, $\theta \in \mathcal{F}_{\pi'}$. Now let $\theta' = [1]_{g,\theta} \circ h$. Then θ' still satisfies (i) and (ii), and

$$\text{Frob } \theta' \circ f \circ (\theta')^{-1} = [1]_{g,\theta} \circ \theta \circ [1]_{g,\theta}^{-1} = g.$$

(iii) and (iv) follows from Proposition 4.4.7. □

Lemma 4.4.19. *Let K be a nonarchimedean local field, L/K be an algebraic extension, and $x \in \hat{L}$. If x is separable and algebraic over L, then $x \in L$.*

Proof. Let $L' = \hat{L} \cap \overline{K}$. Let $\sigma \in \text{Gal}(\overline{K}/L)$. We know that σ is continuous and it is the identity on L. Let $x \in L'$. Then x is the limit of elements in L and so the action of σ is trivial on x as well. Thus $\text{Gal}(\overline{K}/L) = \text{Gal}(\overline{K}/L')$. Then by Galois theory, we obtain $L' = L$. □

Theorem 4.4.20. *The field $K_\pi \cdot K^{unr}$ and the map ϕ_π are independent of the choice of π.*

Proof. Let π and $\pi' = u\pi$ be two different prime elements of K. Let $f \in \mathcal{F}_\pi$, $g \in \mathcal{F}_{\pi'}$, and define h as in Proposition 4.4.18. Then

$$\begin{aligned}\text{Frob} \circ h \circ [\pi]_f &= (h \circ [u]_f) \circ [\pi]_f \\ &= h \circ [u\pi]_f \\ &= h \circ [u']_f \\ &= [\pi']_g \circ h,\end{aligned}$$

i.e., $\text{Frob} \circ h(f(T)) = g(h(T))$. Therefore, for any $a \in \overline{K}$, if $a \in E_f^1$, then $f(a) = 0$, so $g(h(a)) = 0$, and hence $h(a) \in E_g^1$. Similarly, if $b \in E_g^1$, then $g(b) = 0$, so $f(h^{-1}(b)) = 0$, and hence $h^{-1}(b) \in E_f^1$. So h defines an isomorphism $E_f^1 \to E_g^1$. Thus

$$\begin{aligned}\widehat{K^{\text{unr}}}(E_g^1) &= \widehat{K^{\text{unr}}}(h(E_f^1)) \\ &\subset \widehat{K^{\text{unr}}}(E_f^1) \\ &= \widehat{K^{\text{unr}}}(h^{-1}(E_g^1)) \\ &\subset \widehat{K^{\text{unr}}}(E_g^1).\end{aligned}$$

Thus $\widehat{K^{\text{unr}}}(E_g^1) = \widehat{K^{\text{unr}}}(E_f^1)$. Now combine Lemma 4.4.19 and we get $K^{\text{unr}}(E_f^1) = K^{\text{unr}}(E_g^1)$. Similarly, $K^{\text{unr}}(E_f^n) = K^{\text{unr}}(E_g^n)$ for all $n \geq 1$. Thus $K_\pi \cdot K^{\text{unr}} = K_{\pi'} \cdot K^{\text{unr}}$.

We need to show that $\phi_\pi = \phi_{\pi'}$ as well. Note that both $\phi_\pi(\pi)$ and $\phi_{\pi'}(\pi)$ act as Frob on K^{unr}. Thus they agree on K^{unr}. On K_π, $\phi_\pi(\pi)$ is the identity map. Our first goal is to show that $\phi_{\pi'}(\pi)$ is also the identity map on K_π. Note that K_π^n is generated by E_f^n over K, and h gives an isomorphism $E_f^n \to E_g^n$. It suffices that show that for all $n \geq 1$ and $x \in E_f^n$, we have $\phi_{\pi'}(\pi)(h(x)) = h(x)$. Since $\pi = u^{-1}\pi'$, we have

$$\phi_{\pi'}(\pi) = \phi_{\pi'}(u^{-1})\phi_{\pi'}(\pi') = \sigma_1\sigma_2$$

where

$$\sigma_1 = \begin{cases} \text{Frob} & \text{on } K^{\mathrm{unr}} \\ 1 & \text{on } E_f^n \end{cases}$$

and

$$\sigma_2 = \begin{cases} 1 & \text{on } K^{\mathrm{unr}} \\ [u]_f & \text{on } E_f^n. \end{cases}$$

Since h has coefficients in $\widehat{K^{\mathrm{unr}}}$, we have

$$\begin{aligned} \phi_{\pi'}(\pi)(h(x)) &= \sigma_1\sigma_2(h(x)) \\ &= \sigma_1(h(\sigma_2(x))) \\ &= \sigma_1(h([u]_f(x))) \\ &= h(x). \end{aligned}$$

Hence $\phi_{\pi'}(\pi)$ is identity on K_π. Since π was arbitrary and prime elements generate K^*, we conclude that ϕ_π does not depend on π. □

Lemma 4.4.21. *Let $n, m \geq 1$. Let K_m be the unique unramified extension of degree m over K. Let $H_{n,m}$ be the subgroup of K^* generated by $U_K^{(n)}$ and π^m. Then $\phi_\pi(a)|_{K_\pi^n \cdot K_m} = 1$ for all $a \in H_{n,m}$.*

Lemma 4.4.22. *Let $a \in K^*$. Then $\phi_K(a)|_{K_\pi \cdot K^{unr}} = \phi_\pi(a)$.*

Proof. We know that both $\phi_K(\pi)$ and $\phi_\pi(\pi)$ act as Frob on K^{unr}. Hence they agree on K^{unr}. By part (iii) of Theorem 4.4.15, π is a norm from K_π^n to K for every $n \geq 1$. Hence $\phi_K(\pi)$ acts trivially on K_π^n for every $n \geq 1$. Apply Lemma 4.4.21 with $m = 1$, then we get that $\phi_\pi(\pi)$ acts trivially on K_π^n for every $n \geq 1$. So ϕ_K and ϕ_π agree on $K_\pi^n \cdot K^{\mathrm{unr}}$ for all $n \geq 1$, so they must agree on the union $\bigcup_{n\geq 1} K_\pi^n \cdot K^{\mathrm{unr}} = K_\pi \cdot K^{\mathrm{unr}}$. We are done since prime elements of K generate K^* (every $a \in K^*$ can be written as $a = u\pi^i$, and $u = (u\pi)\pi^{-1}$). □

Lemma 4.4.23. *Let $n, m \geq 1$. Let $K_{n,m} = K_\pi^n \cdot K_m$. Then $N_{K_{n,m}/K}(K_{n,m}^*) = U_K^{(n)} \langle \pi^m \rangle = H_{n,m}$.*

Proof. By Lemma 4.4.21, $H_{n,m}$ is contained in the kernel of the local reciprocity map, i.e., $H_{n,m} \subset N_{K_{n,m}/K}(K_{n,m}^*)$ by part (ii) of Theorem 4.1.1. On the other hand, we have

$$\begin{aligned}[K : H_{n,m}] &= [U_K : U_K^{(n)}][\langle \pi \rangle : \langle \pi^m \rangle] \\ &= (q-1)q^n m \\ &= [K_\pi^n : K][K_m : K] \\ &= [K_{n,m} : K].\end{aligned}$$

By part (ii) of Theorem 4.1.1 we know that ϕ_K induces an isomorphism

$$\phi_{K_{n,m}/K} : K^*/N_{K_{n,m}/K}(K_{n,m}^*) \to \mathrm{Gal}(K_{n,m}/K).$$

Therefore,

$$H_{n,m} = N_{K_{n,m}/K}(K_{n,m}^*).$$

□

Theorem 4.4.24. *$K^{ab} = K_\pi \cdot K^{unr}$ and $\phi_\pi = \phi_K$.*

Now we are ready to prove the Local Existence Theorem.

Proposition 4.4.25. *Let K be a nonarchimedean local field. Let L/K be a finite abelian extension. Then $N_{L/K}(L^*)$ is open subgroup of K^* of finite index.*

Proof. The local reciprocity map gives an isomorphism $\phi_{L/K} : K^*/N_{L/K}(L^*) \cong \mathrm{Gal}(L/K)$, hence $N_{L/K}(L^*)$ is of finite index. Now we need to show that $N_{L/K}(L^*)$ is open. Note that U_K is compact, hence $N_{L/K}(U_L)$ is closed in U_K (since U_K is Hausdorff, and $N_{L/K}$ is continuous). U_K is open in K^*, so $N_{L/K}(U_K)$ is open in K^* as well. Therefore, $N_{L/K}(L^*)$ is open in K^* too, because it contains an open subgroup $N_{L/K}(U_K)$ of K^*. □

Proposition 4.4.26. *Let K be a nonarchimedean local field. Suppose H is an open subgroup of K^* with finite index, then H is a norm subgroup.*

Proof. Because H is open, there is some $n \geq 1$ such that $U_K^n \subset H$ (since $\{U_K^i\}$ forms a neighborhood basis for the identity in K^*). Because H is of finite index in K^*, there are only a finite number of cosets of the form $\pi^j H$, hence there exists some $m \geq 1$ such that $\pi^m \in H$. Hence H contains the subgroup $H_{n,m}$ generated by $U_K^{(n)}$ and π^m. Let K_m be the unique unramified extension of degree m over K, and consider the subfield $K_{n,m} = K_\pi^n \cdot K_m$ of K^{ab}. By Lemma 4.4.23, we have $H_{n,m} = N_{K_{n,m}/K}(K_{n,m}^*)$. Let L be the subfield of $K_{n,m}$ that is fixed by $\phi_{K_{n,m}/K}(H)$. Then H is the kernel of the map $\phi_K : K^* \to \mathrm{Gal}(L/K)$, and by Theorem 4.1.1, we must have

$$H = N_{L/K}(L^*).$$

□

Remark 4.4.27. *Proposition 4.4.25 and Proposition 4.4.26 complete the proof of Local Existence Theorem (Theorem 4.1.6).*

References

[ANT] *Algebraic Number Theory* lecture notes. Available at `http://math.okstate.edu/people/pyan/AlgebraicNumberTheory.pdf`.

[Cas86] Cassels, J.W.S., *Local Fields*, Cambridge University Press, Cambridge, 1986.

[CF67] Cassels, J.W.S., Fröhlich, A., *Algebraic Number Theory*, Washington DC, 1967.

[FT91] Fröhlich, A., Taylor, M., *Algebraic Number Theory*, Cambridge University Press, 1991.

[LT65] Lubin, J., Tate, J., *Formal complex multiplication in local fields*, Annals of Mathematics (1965): 380-387.

[Mil13] Milne J.S., *Class Field Theory (v4.02)*, 2013. Available at `http://www.jmilne.org/math/`.

[Neu86] Neukirch, J., *Class Field Theory*, Springer, 1986.

[Ser80] Serre, J.P., *Local Fields*, Springer-Verlag, 1980.

[Sha] Sharifi, R., *An Introduction to Group Cohomology*, Lecture notes, available at `http://math.arizona.edu/~sharifi/groupcoh.pdf`.

[Wat73] Waterhouse, W.C., *Profinite groups are Galois groups*, Proceedings of the American Mathematical Society 42 (1973), 639-640.